

NOTE TO USERS

This reproduction is the best copy available.

UMI[®]

**Balancing Information Access and Security (BIAS):
Explaining Three Decades of
United States Encryption Policymaking**

**A Dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy at George Mason University**

By

**Mark L. DeVirgilio
Masters of Science
University of Hawaii, 1980**

**Chair: E. H. Sibley, Professor
School of Public Policy**

**Summer Semester 2005
George Mason University
Fairfax, Virginia 22030-4444**

UMI Number: 3175608

INFORMATION TO USERS

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleed-through, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

UMI[®]

UMI Microform 3175608

Copyright 2005 by ProQuest Information and Learning Company.

All rights reserved. This microform edition is protected against unauthorized copying under Title 17, United States Code.

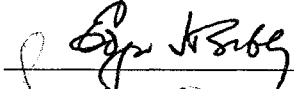
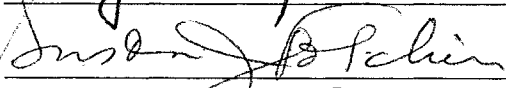
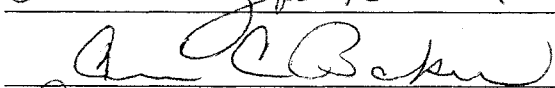
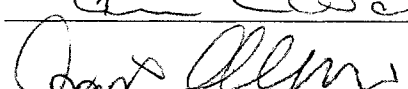

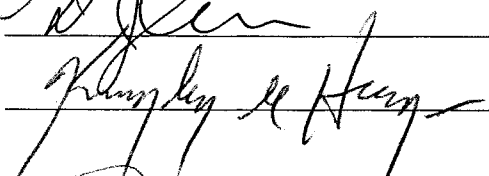
ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

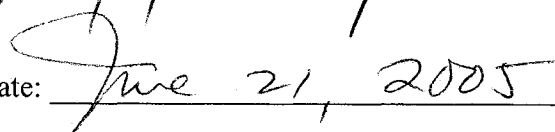
BALANCING INFORMATION
ACCESS AND SECURITY (BIAS):
EXPLAINING THREE DECADES OF
UNITED STATES ENCRYPTION POLICYMAKING

by

Mark L. DeVirgilio
A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree of
Doctor of Philosophy
Public Policy

Committee:

	Chair
	Member
	Member
	External Reader
	Program Director
	Dean, School of Public Policy

Date:  June 21, 2005

Summer Semester 2005
George Mason University
Fairfax, Virginia

Table of Contents

	Page
List of Tables	iv
List of Figures	v
List of Abbreviations/Symbols	vi
Abstract	xi
Chapter One: Introduction	1
Digital Encryption as an Information Control Policy Paradigm	7
Policy Processes to Balance Information Access and Security.....	16
Purpose, Thesis, and Research Questions	22
Outline of Dissertation	26
Chapter Two: Foundation and Theory	27
Encryption Laws and Regulations.....	29
Prior Studies and Research.....	43
Allison's Decision Models.....	57
Policy Dilemma and the Need to Extend Theory.....	69
Chapter Three: Methodology	73
Case Study Design	74
Analysis Units and Data Handling.....	77
Pattern Matching	79
Research Displays	88
Chapter Four: Data and Results	91
First Mover Period: 1973-1986.....	91
Congressional Group.....	94
Encryption Technology Group.....	118
Executive Group	139
Government Agencies Group.....	161
First Mover Period Summary.....	182
Competitive Period: 1987-1997	184

Congressional Group.....	188
Encryption Technology Group.....	223
Executive Group	256
Government Agencies Group.....	287
Competitive Period Summary	316
Status Quo Period: 1998-2004	319
Congressional Group.....	322
Encryption Technology Group.....	359
Executive Group	397
Government Agencies Group.....	432
Status Quo Period Summary	464
Chapter Five: Explanation and Discussion	468
Congressional Group.....	468
Encryption Technology Group.....	477
Executive Group.....	486
Government Agencies Group.....	497
Interactions	507
Chapter Six: Conclusion	522
Bibliography.....	537
Curriculum Vitae.....	555

List of Tables

	Page
Table 2-1 Important Laws Shaping Encryption Policy.....	31
Table 2-2 Modified Rational Actor Model	61
Table 2-3 Modified Organizational Behavior Model.....	64
Table 2-4 Modified Governmental Politics Model	68
Table 3-1 List of Groups, Actors, and Data Sources	79
Table 3-2 Criteria and Valances.....	87
Table 3-3 Analytical Periods.....	90
Table 4-1 First Mover Period Summary	182
Table 4-2 Competitive Period Summary.....	317
Table 4-3 Status Quo Period Summary.....	466

List of Figures

	Page
Figure 1-1 Hebern's cryptographic machine.....	9
Figure 1-2 Encryption system containing secret and public key subsystems	14
Figure 4-1 Timeline of IBM activities leading up to the publication of DES.....	135
Figure 4-2 Public key encryption activities and the wait for computer power	137
Figure 4-3 Author's rendition of a digital encryption standard test device	165
Figure 4-4 Timeline of NBS and IBM activities.....	178
Figure 4-5 Timeline of executive branch activities.....	282
Figure 4-6 Internet credit card transaction showing the use of electronic signatures.....	346
Figure 4-7 Timeline of Encryption Technology Group activities.....	390
Figure 4-8 Timeline of executive branch activities.....	424
Figure 4-9 Timeline for DSS FIPS Pub 186-2 and AES FIPS Pub 197	458
Figure 4-10 Author's private FORTEZZA card	461
Figure 5-1 Congressional Group valances over three periods	469
Figure 5-2 Encryption Technology Group valances over three periods	478
Figure 5-3 Executive Group valances over three periods	487
Figure 5-4 Government Agencies Group valances over three periods	498
Figure 5-5 Actor group decision behaviors.....	508

List of Abbreviations/Symbols

ACM	Association of Computing Machinery
<i>AECA</i>	<i>Arms Export Control Act</i>
AES	Advanced Encryption Standard
ADPE	Automated Data Processing Equipment
BIS	Bureau of Industry and Security
BSA	Business Software Alliance
BXA	Bureau of Export Administration
CA	Certificate Authority
CCEP	Commercial COMSEC Endorsement Program
CCIA	Computer and Communications Industry Association
CCL	Commerce Control List
CDT	Center for Democracy and Technology
CFR	Code of Federal Regulations
CI	Counterintelligence
COCOM	Coordinating Committee on Multilateral Export Controls
COMSEC	Communications Security
CPSR	Computer Professionals for Social Responsibility
CRS	Congressional Research Service
DCI	Director of Central Intelligence
DES	Data Encryption Standard

<i>DMCA</i>	<i>Digital Millennium Copyright Act</i>
DOD	Department of Defense
DOJ	Department of Justice
DRM	Digital Rights Management
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAR	Export Administration Regulations
EES	Escrowed Encryption Standard
EFF	Electronic Frontier Foundation
EPA	Environmental Protection Agency
EPIC	Electronic Privacy Information Center
<i>E-SIGN Act</i>	<i>Electronic Signatures in Global and National Commerce Act</i>
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standard
<i>FISA</i>	<i>Foreign Intelligence Surveillance Act of 1978</i>
FR	<i>Federal Register</i>
GPM	Governmental Politics Model
H.R. 145	<i>Computer Security Act of 1987</i>
HSPD	Homeland Security Presidential Directive
IBM	International Business Machines Corporation
<i>IEEPA</i>	<i>International Emergency Economic Powers Act</i>
INFOSEC	Information Security

ICT	Information and Communication Technology
ISO	International Standards Organization
ISP	Internet Service Provider
ITAA	Information Technology Association of America
ITAR	International Traffic in Arms Regulations
KEA	Key Exchange Algorithm
KMI	Key Management Infrastructure
LEAF	Law Enforcement Access Field
MIT	Massachusetts Institute of Technology
MPEG	Motion Picture Experts Group
NBS	National Bureau of Standards
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NRC	National Research Council
NSA	National Security Agency
NSC	National Security Council
NSCS	National Security Council System
NSD	National Security Directive – G. H. W. Bush Era terminology
NSDD	National Security Decision Directive – Reagan Era terminology
NSS	National Security Strategy of the United States
NTISSC	National Telecommunications and Information Systems Security Committee

OBM	Organizational Behavior Model
OECD	Organization for Economic Cooperation and Development
OG	<i>Official Gazette</i>
OMB	Office of Management and Budget
OSP	Online Service Provider
OTA	Office of Technology Assessment
PDD	Presidential Decision Directive – Clinton Era terminology
PKI	Public Key Infrastructure
PKP	Public Key Partners
<i>PROTECT Act</i>	<i>Promote Reliable On-line Transactions to Encourage Commerce and Trade Act</i>
R&D	Research and Development
RAM	Rational Actor Model
RIAA	Recording Industry Association of America
RSA	Rivest, Adleman, and Shamir public key encryption subsystem
<i>SAFE Act</i>	<i>Security and Freedom through Encryption Act</i>
SCM	Security countermeasures
SIGINT	Signals Intelligence
SSA	Social Security Administration
TDEA	Triple Data Encryption Algorithm or Triple DES
USACM	United States Association of Computing Machinery
<i>USA PATRIOT Act</i>	<i>Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act</i>

U.S.C.	United States Code
USPTO	United States Patent and Trademark Office
USSS	United States SIGINT System
WIPO	World Intellectual Property Organization

Abstract

BALANCING INFORMATION ACCESS AND SECURITY (BIAS): EXPLAINING THREE DECADES OF UNITED STATES ENCRYPTION POLICYMAKING

Mark L. DeVirgilio, Ph.D.

George Mason University, 2005

Chair: Dr. E. H. Sibley

The United States leads the world in developing and employing encryption technology, but has problems in deciding a balance between information access and security requirements. Encryption use is both a powerful enabler of global information economies and global networks of criminals, spies, and terrorists. This dissertation explains how three decades of decisions and actions have produced a de facto encryption policy. By analyzing decisions and actions according to metrics derived from Graham T. Allison's decision models, I found that groups of actors exhibited convergent decision behaviors described by the Rational Actor Model and by a mix of the Organizational Behavior and Governmental Politics Models. Currently, an encryption policy status quo is the result of decisions and actions made according to the Rational Actor Model and by organizations changing their governing variables. As a policy forecast, I believe that a successful encryption policy should be market-based, but the government must be proactive with public policies when information security failures occur.

Chapter One: Introduction

Examining three decades of United States encryption policymaking events according to policy actor groups, their perceptions of the information control problem, their favored alternatives or solutions, and their decision timings may further illuminate the general field of technology policymaking. In the information age, a common supposition supported by the Internet experience is that technology evolves too rapidly for groups of actors to make effective and predictable policy decisions. This dissertation on encryption policymaking suggests that this supposition of happenstance policymaking is wrong and will show that decision-making patterns exist. Understanding these patterns may have predictive value and may be useful in creating future policy designs. The goal of my dissertation is to analyze historical evidence in order to produce new knowledge that will advance United States and global encryption policy designs. My dissertation explores groups of encryption policy actors, provides explanations for past decisions and actions, and suggests a trajectory for future policy decisions.

While the United States leads the world in the development and use of digital encryption, its public policies that promote encryption benefits and reduce the negative externalities of encryption use have not met international and domestic expectations on the broader problem of balancing information access and security requirements. For my research, I define public policies as plans of action resulting from predictable and

repeatable decision processes that distribute benefits, costs, responsibilities, and trust throughout the private and government sectors. During the past three decades, groups of actors have made decisions on how to satisfy information access and security requirements by developing and controlling information tools based on encryption technology. Some of these decisions have kept pace with technology and market advancements, while other decisions have locked advancements into a government-directed technology progression. Such a spectrum of decisions often juxtaposes the relationships between information access and security requirements and controlling or liberalizing encryption use. One way to keep these relationships in context is to explore how information and encryption control decisions affect technology leadership, economic, privacy, trust, national security, and public safety requirements in the United States. Over time, policy decisions on encryption control may become congruent with requirements on information access and security. When this happens, a national and global policy will have matured.

Although some believe that market control of digital encryption technology may be optimal in the information age, a mature public policy may still be required to deter or prevent users of personal computers and other electronic information devices from criminally exploiting, maliciously hiding, or accidentally losing critical information. No market-based policy can guarantee access to critical information required for the functioning of the market and civil society, ensuring personal safety and privacy, and the survival of the state. A smart public policy design should find the right level of information access, by government and private sector actors, to critical information and

should preserve the strength and trust of encryption tools used to maintain information security. Thus, policymakers must seek to balance the benefits of digital encryption in facilitating e-commerce, ensuring trust, protecting privacy, and securing valuable information against the costs of hostile use, espionage, criminal exploitation, and unrecoverable loss of information. This balance has been an elusive goal because groups of actors have different perceptions on the problem, on favored alternatives or solutions, and on when to act.

The United States government believes that e-commerce will be a multi-trillion dollar activity specifically enabled by digital encryption and that encryption will be an essential tool for information security and privacy. However, members of the National Security Council System (NSCS) and governmental departments caution that encryption tools may provide too much information security. Uncontrolled encryption use may allow criminals, spies, and terrorists to shield their activities from surveillance, and the careless or malicious use of encryption may result in the permanent loss of critical information. A balanced solution may require that information owners sacrifice a degree of information security by granting a trusted authority a degree of information access. Information access, especially by the government, is viewed as a form of socio-political submission that has been an anathema to the culture of the United States. In the United States, the rights of individuals and the right to privacy generally trump responsibilities to society and the state. Thus, individuals believe that liberalized encryption use is a right that limits the power of a historically aggressive national security state. With encryption use posing such socio-political and cultural hurdles, policymakers are at an impasse with

respect to constructing encryption policy designs that will achieve a balance between information access and security.

In the past three decades, groups of policy actors have followed different decision paths in the development of solutions to their perceptions of the problem. Policy designers should analyze these past policy decisions in order to create new policy choices that use information technology advances to ensure privacy, to participate fairly in the global information economy, and to protect the United States from attack. This analysis should be done and policy choices developed if future information and encryption control policies are to lead, or at least be congruent with, the rest of the world. Policy leadership in this area may be forfeited to contenders, such as the Europeans, that favor state regulation of technology and have less compunction for individual rights. Such a consequence will unduly harm the United States, as this country has a unique “American Creed” of individualism, a love of technology leadership, a greater global security burden because of its intense moralist views, and a more polarized perception of information access and security requirements.¹ The terrorist attack on September 11, 2001 highlighted a schism in these requirements that was known since the Nixon administration. The United States did not have adequate information access to prevent this attack and still does not have sufficient information security to prevent a future cyber-attack.

¹ I attribute the notions of an American Creed and moralistic bent to Professor Seymour Martin Lipset.

My research uses a case analysis study to investigate groups of actors and to explain the decision-making processes used in past information and encryption control actions. Although the United States Congress is a primary policy actor by virtue of its law-making function, Congress has yet to codify a policy that directly balances information access and security requirements by determining the right level of encryption control. My research may show why Congress has been reluctant to pass laws that favor or specify technology solutions. For over three decades, other groups of actors have influenced policy designs and have made de facto policy by taking rational actions, by following organizational behaviors, and by advancing political agendas. All the while, a market-based encryption policy has emerged, which by definition does not consider encryption's externalities. Externalities include positive outcomes such as the widespread use of standardized encryption systems and negative outcomes such as the fostering of illegal activities. If the United States had not been attacked, then explaining the emergence of a market-based encryption policy that was tolerated by all actor groups would have been the final product of my research.

My research also analyzes groups of actors outside of Congress that continue to make information and encryption control policies. The attack on September 11, 2001 has created a government agenda that seeks to increase the level of public safety in the United States and aggressively pursues vital national security interests on a global scale. This government agenda comes at great expense, as measured in dollars and lives, and at a socio-political cost of reduced American freedoms and diminished American innovative spirit. Civil libertarians, privacy rights advocates, and technologists from businesses and

academia believe that recent laws, such as the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (*USA PATRIOT Act*), have gone too far in sacrificing civil liberties, privacy, and technology leadership advantages for narrow increases in national security and public safety. Thus, actors in this group seek to influence policy design by expanding encryption usage to counteract the *USA PATRIOT Act*.

When actor groups believe that encryption is an essential “tool of democracy” and is required for limiting the power of an untrustworthy and intrusive government, then such groups are motivated to take actions that make policy. Past successful actions, such as the promotion of encryption to negate the domestic eavesdropping activities allowed by the *Foreign Intelligence Surveillance Act of 1987*, motivate these groups to fight for further encryption liberalization. This fight entails using media demonstrations, sponsoring legal challenges in the federal court system, testifying before Congress, and developing encryption tools for use on a global scale to convince other actor groups that unrestricted encryption use is an inevitable part of the information age.

Other actor groups normally associated with national security and public safety functions, such as an executive branch group and a quasi-independent federal government agencies group, believe that encryption control policies are required to enhance the effectiveness of surveillance activities permitted by the *USA PATRIOT Act*. In passing this act without addressing encryption use, Congress has postponed the decision on the balance between information access and security. Thus, the executive branch and

government agencies continue to influence the encryption policy debate by taking independent or loosely coupled actions. Often the executive branch will take the leadership initiative, act according to its perception of the problem, and apply its own solution without specific legislative authority. One result of such executive branch actions is the generation of political animosity with Congress. With politically distracted legislative and executive branches, government agencies are often left alone to make their own decisions on information and encryption control policies. The actions and interactions of groups of actors making information and encryption control policy decisions form the investigative basis for this dissertation.

Digital Encryption as an Information Control Policy Paradigm

Following Thomas Kuhn's ideas on scientific revolutions, digital encryption may represent a technology paradigm that will force changes in linear and sequential policy design processes.² In the past, information access and security have been controlled by physical means such as using locks and keys. The nature of information has changed as much of the valuable information is now in electronic form. Information control policies that determine information access and security requirements should also change. Encryption technology serves as the "lock and key" for electronic information and is the focus of an ongoing information control debate. At the beginning of the twentieth

² Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed. (Chicago: University of Chicago Press, 1996), 92-110.

century, control of encryption was easier and involved physical control of electromechanical encryption hardware and keys. A paradigm shift may have occurred when both information and encryption took digital forms. Now policymakers cannot rely upon physical control of information and electromechanical encryption devices that had worked before for over fifty years. Policymakers must now decide on how the government will control intangible digital information and encryption technologies, while maintaining the benefits of marked-based technology developments and preserving a fragile public trust with thoughtful government intervention.

Since the early 1900s, the United States has been an encryption technology leader and has now fostered encryption usage on a global scale. David Kahn, an expert on the history of cryptography, noted that American inventor Hugh Hebern developed one of the first electromechanical cipher machines for business use around 1917. Figure 1-1 shows Hebern's machine with its typewriter-styled body and prominent cylindrical rotors that contained the electrical contacts used for the encryption process. By typing information as a message, the rotors would change position with each key stroke, thereby altering the electrical circuits and scrambling the plaintext into cipher text. In an early demonstration of United States government policy toward this combined civilian and military or "dual-

use” encryption technology, the government conscripted a version of Hebern’s machine for use in World War II and did not adequately compensate its inventor.³

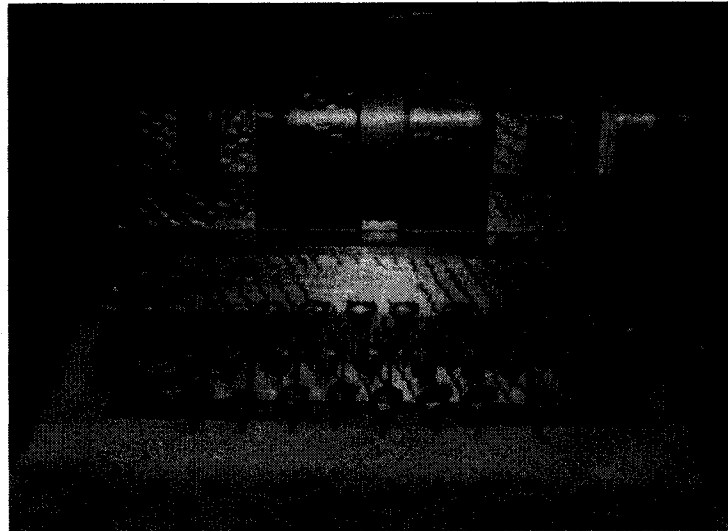


Figure 1-1 Hebern’s cryptographic machine at the National Cryptologic Museum, Fort Meade, Maryland

The word “encryption” has a World War II etymology and refers to the process of selectively protecting information by the “diffusion and confusion” or the rearrangement and substitution of the symbols used to represent the information. Strong encryption is done in such a way that it “confuses” code breakers by “diffusing” a change in one symbol of the input into a change in many symbols of the output.⁴ Policies to control

³ David Kahn, *The Code Breakers: The Story of Secret Writing* (New York: Scribner 1996), 394-434.

⁴ Merriam-Webster Collegiate Dictionary, 2004, < <http://www.m-w.com/cgi-bin/dictionary> >, accessed December 2004.

dual-use encryption technology are now problematic, as software algorithms and alphanumeric encryption keys have replaced tangible electromechanical devices and physical keys. Adding to the policy paradigm, digital encryption has fundamentally changed the nature of encryption technology by being itself an intangible information product that is inherently difficult to control. Encryption can be both the protector of digital information and a form of digital information, which is subject to policies on information control.

The relationships between information access and security requirements and encryption control and liberalization policies may be non-linear and complex. Encryption liberalization permits users to have an unprecedented level of information security and privacy. Modern digital encryption allows near perfect and unbreakable protection of information, which is a capability that has never before existed. However, encryption users can misuse or lose information, thus making information permanently inaccessible for national security purposes, public safety actions, or personal health contingencies. Despite this dilemma posed by encryption use, United States federal agencies have pushed the use of encryption technology onto the government and private sectors.

The United States government developed the Data Encryption Standard (DES) in the mid-1970s by modifying an encryption algorithm designed by industry. Although

Claude. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal* 28 (October 1949): 656-715. Shannon uses communication theory concepts throughout his paper, which now have taken the analogous meanings of diffusion and confusion.

originally developed for government use, DES has become the worldwide digital encryption standard. Digital encryption works by using digital logic circuits or computer algorithms to rearrange and substitute the binary ones and zeros underlying the “plain text” information to produce “cipher text.” For example, the plain text message “I have a secret” is transformed into the cipher text message of “Û@Û” %o’Yí ”öb%”gÑò:ÓBôï ” by using the DES encryption algorithm with a hexadecimal key of “DC 6B FB 1C 52 B9 07 76.” DES fits in a category called secret key encryption, because using DES is analogous to the use of a lock and key to secure valuable property. To satisfy information access and security requirements, encryption policy often focuses on controlling the strength of encryption algorithms and on managing encryption keys. Encryption policy, following the lock and key analogy, decides on how strong the lock should be and who will hold the keys. In my research, an examination of encryption technology development serves as one source of evidence on policy decisions.

Safeguarding and maintaining encryption keys have been the historical weakness of secret key encryption, and a solution to this problem would enable the use of easy and powerful encryption by the public. All copies of a person’s secret key, legitimate and otherwise, allow access to the protected information. Public key encryption fixes this weakness, but complicates encryption policy design by further entangling information control requirements with the control of encryption, which is itself an information technology product. The 1976 invention of public key encryption by Stanford University engineers Whitfield Diffie and Martin Hellman, in collaboration with Ralph Merkel, is

arguably the most important information and encryption technology advancement of the twentieth century. Diffie and Hellman realized that the handling and exchanging of encryption keys limited the practical uses of digital encryption. They disclosed the motivation behind their discovery in a journal article: "A private conversation between two people with no prior acquaintance is a common occurrence in business, however it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means."⁵ Unfortunately, their solution would also enable criminals, spies, and terrorists to overcome the same problems and to deny information access to national security and law enforcement officials.

Public key encryption solved the key distribution problem of secret key encryption in a revolutionary manner. Diffie and Hellman proposed the use of special mathematical functions and specially selected numbers to generate a mathematical lock-box that uses two different types of encryption keys. Once these two keys are generated and sent electronically to different locations, the selected numbers can be deleted to increase the security of the system. One of these keys is called the "public key" and is stored openly. In a very different paradigm from secret key encryption, the public key can be used to "one-way" encrypt information. Once employed in this fashion, the public key cannot be used to unlock or decrypt the information. In addition, no manipulation of the public key will produce a key to unlock the information. The recipient of the encrypted information uses the other mathematically generated key or "private key" for decryption. The

⁵ Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* IT-22, no. 6 (November 1976): 644.

paradigm change instituted by public key encryption allows users to access libraries of public keys and to encrypt information with the public keys of the intended recipients. This can be done without waiting for a courier to deliver a secret key or having to guard and maintain the public key once used. The enabling effect of public key encryption is analogous to a large supply of impervious and transportable information lockboxes that are normally free, but may range in cost up to twenty-five dollars per year.⁶

While the public key encryption paradigm may be essential to an Internet shopper performing a transaction through a secure “https://” server, the same paradigm allows criminals, spies, and terrorists to communicate with impunity. The minimal requirement for users of public key encryption is a personal computer with communications capability. In the 1970s, few citizens had computers and this lack of access to computing power severely limited the usefulness of public key encryption. Thirty years later, computers and Internet access are available to most people in the United States, which now makes control of public key encryption paramount. Controlling public key encryption’s benefits and negative externalities presents a challenge to policymakers trying to decide on how to protect mathematical algorithms generated by encryption researchers, how to regulate software applications that use these algorithms, and how to control encryption key libraries. The development of public key encryption has further intertwined information and encryption control problems and solutions.

⁶ The author’s military Common Access Card enables public key encryption and is free. The author’s Verisign public key encryption service costs \$15.00 per year.

Encryption policy actors face complex decisions as modern encryption systems use both secret key and public key encryption technologies in a synergistic fashion. Policy designs constructed incrementally for each emerging encryption technology may lack the required coherency to control more powerful and complex encryption products. Coherent policy should address both secret and public key encryption subsystems and should account for the evolving capabilities and uses of these subsystems. Figure 1-2 shows one such use of these two subsystems.

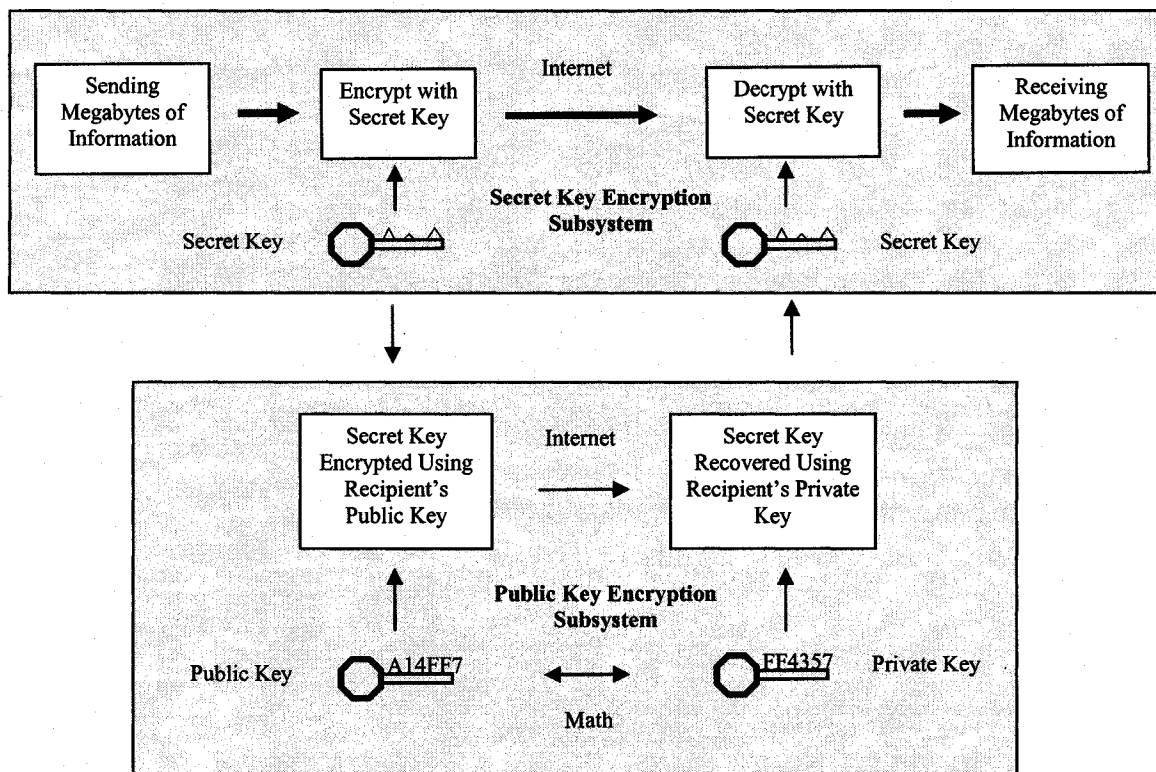


Figure 1-2 Encryption system containing secret and public key subsystems and used for sending encrypted information over the Internet

The secret key encryption subsystem does the bulk of the information protection work, as this subsystem is very efficient in terms of encryption and decryption speeds. For example, a one million byte (megabyte) file took 3.6 seconds to encrypt with a secret key algorithm. The same file took 83 seconds to encrypt with a public key algorithm.⁷ Being around twenty times less efficient, the public key encryption subsystem is not suitable for everyday encryption usage, but is essential in solving the key distribution problem. In addition, Figure 1-2 shows how these two subsystems work together to create an efficient encryption system. Users employ public key encryption to send a secret key to a recipient. The recipient then uses this secret key to decrypt information sent separately through the Internet. This secret key or “session key” is normally destroyed after the communication is completed.

As the session key allows access to the protected information, national security and law enforcement officials must intercept and maintain the session key in order to access encrypted information. Often the session key is used only once and a new session key is generated for each subsequent transaction. Because of this complexity, effective encryption control policies should account for secret key encryption algorithms; each session’s secret encryption key and encrypted message; and certificates that contain the digital identities, signatures, public keys, and private keys of users. Developing an encryption control policy may be possible if the international community, the United

⁷ I ran DES secret key and RSA public key encryption tests using a one-megabyte draft of this dissertation. I used a dual 300 MHz Pentium II Dell server as the test platform. Software came from Dr. Krzysztof Gaj’s encryption technology class at George Mason University.

States government, industry, and individuals can agree on a set of rules and can trust each other to follow these rules. Past encryption policy debates and encryption policy designs have focused on the following aspects of the encryption system:

- Determining the strengths of secret key encryption subsystems
- Determining the capabilities of public key encryption subsystems
- Regulating the geopolitical distribution of encryption systems
- Obtaining, managing, and archiving session keys and encrypted messages
- Establishing trust relationships among users, vendors, and government
- Regulating the market to control the externalities of encryption use

Policy Processes to Balance Information Access and Security

Ensuring national security and maintaining public safety are primary concerns of public policy, as market forces and ethical concerns are often inadequate. Development of public policies may follow the notional phases of agenda setting, formulation, implementation, and evaluation.⁸ This sequence of policy phases, collectively called “policy design” by political scientists Anne Schneider and Helen Ingram, implies a rational and linear policymaking process.⁹ The initial phase of this linear process involves coupling perceived problems to policy alternatives or solutions. If perceived problems have no solutions, then policy design may stand idle at the policy formulation

⁸ Randall B. Ripley, “Stages of the Policy Process,” in *Public Policies Theories, Models and Concepts: An Anthology*, ed. Daniel C. McCool (Englewood Cliffs, New Jersey: Prentice Hall, 1995), 157-162.

⁹ Anne Larason Schneider and Helen Ingram, *Policy Design for Democracy* (Lawrence, Kansas: University Press of Kansas, 1997), 2-3.

stage. However, policymakers can sometimes solve composite problems incrementally, as partial solutions become available. More often, policymakers wait to produce several alternative solutions, thereby creating a decision agenda that packages a problem with its potential solutions. Policy design moves forward to the policy implementation phase when a decision-making process selects the optimum solution. Political scientist Graham T. Allison, in his seminal article analyzing the Cuban Missile Crisis, described this type of decision-making process as one that follows a conceptual “Rational Policy Model.”¹⁰ In subsequent texts, Allison renamed this model to the “Rational Actor Model” or RAM.¹¹ According to this model, policy results from a rational choice of the optimum solution from a list of alternatives.

The digital encryption paradigm may hinder policy design by creating conflicting perceptions of information control problems and by reducing the quality and quantity of alternatives. Political scientist John W. Kingdon notes that problem ownership occurs when policymakers transform “conditions” into problems that are “appropriate for government action.”¹² Policy actors that perceive information and encryption control as tolerable conditions instead of problems may favor inaction or incremental actions that forestall the policy decision. Inaction and incremental actions often result in a de facto or conglomerate encryption policy. Competing actors that perceive their own versions of

¹⁰ Graham T. Allison, “Conceptual Models and the Cuban Missile Crisis,” *American Political Science Review* 63, no. 3 (September 1969): 690.

¹¹ Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* 2d ed. (New York: Longman, 1999), 13-75.

¹² John W. Kingdon, *Agendas, Alternatives, and Public Policies*, 2d ed. (New York: HarperCollins College Publishers, 1995), 110-111.

information and encryption control problems may formulate policy alternatives commensurate with their organizational or political objectives. Kingdon uses a “Policy Window” metaphor to describe this less structured and often happenstance policy process. Kingdon’s metaphor depicts a policy process where “parallel” problem, policy, and political streams converge into a “decision agenda.”¹³

A problem that reaches the decision agenda in this manner may follow patterns described by Allison’s alternative decision models. In his Organizational Behavior Model (OBM), Allison describes a pattern where organizational actors make decisions based on “factored” problems and organizational culture.¹⁴ This model suggests that organizations are likely to set a decision agenda with part of a composite problem and to formulate alternatives consistent with their organizational culture. Allison’s Governmental Politics Model (GPM) describes a pattern where politically motivated actors make decisions based upon increasing their political power or leadership stature.¹⁵ This model suggests that political actors set the decision agenda by appearing to solve economic, military, and political crises faced by the nation. When treated as a set, Allison’s decision models provide three contrasting analytical perspectives that researchers can use to investigate and explain actions and decisions.

¹³ *Ibid.*, 2-4 and 71-89. Kingdon advances Cohen, March and Olsen’s Garbage Can Model and discusses incrementalism.

¹⁴ Allison and Zelikow, *Essence of Decision*, 143-196.

¹⁵ *Ibid.*, 255-324.

Conflicting requirements on government access to information and on information security to protect privacy may polarize encryption policy actors in the United States. Over time, conflicting requirements may create decision-making patterns unique to the American public policy process. Sociologist Seymour M. Lipset developed the idea of an evolved American “creed” that differentiates Americans from Canadians and Western Europeans.¹⁶ Supporting Lipset’s idea, United States encryption policymaking is dramatically different from the Canadian process. For example, Canada’s *Personal Information Protection and Electronic Documents Act* went through a normal legislative process and became law in April 2000. A corresponding United States bill, the *Security and Freedom through Encryption Act of 1999*, failed to reach a floor vote in the House.¹⁷ Americans and their representatives in Congress appear reluctant to make decisions on solutions that interfere with personal freedoms and choices.

A cyclical favoring by the government for information access or for information security requirements has a basis in United States history. Law professor Mary Ann Glendon believes that overarching individual rights, such as the right to privacy, interfere with policymaking. Glendon, in *Rights Talk*, describes how early American property rights evolved into modern privacy rights, with each individual American now becoming

¹⁶ Seymour Martin Lipset, *Continental Divide: The Value and Institutions of the United States and Canada* (New York: Routledge, Chapman and Hall, Inc., 1990), 212-227.

¹⁷ *Personal Information Protection and Electronic Documents Act*, Second Session, Thirty-Sixth Parliament, 48-49 Elizabeth II, 1999-2000. Bill C-6, Royal Assent or passage on 13 April 2000. U.S. House, H.R. 850, 106th Congress, 1st sess., 1999, Report No. 106-117, Parts I, II, II, IV, and V.

a “lone rights-bearer.”¹⁸ The uncompromising nature of privacy rights and the loose connection between rights-empowered individuals and their representative institutions may prevent the achievement of political consensus required by policymakers. A spectrum of policy actors should agree on the problem and should generate consensual alternatives that solve the problem. Glendon believes that strong privacy rights may hinder the consensus forging abilities of “the intermediate institutions that stand between the individual and the state.”¹⁹ These institutions are comprised of non-lawmaking policy actors representing electronic rights advocates, government agencies, industries, professional organizations, and universities. A lack of consensual policy alternatives from a myriad of policy actors weakens the rational decision-making process and may encourage organizational and political solutions to the information and encryption control problems.

Securing information against unauthorized access both helps and hurts national security. During the first 75 years of the twentieth century, the United States preferred policies that preserved national security, which in turn, expedited a crisis action styled decision-making process. The events of World War I and World War II favored public policies that satisfied national security objectives and discouraged free-market policies. Political scientist David M. Hart describes this decision-making alignment as the policies

¹⁸ Mary Ann Glendon, *Rights Talk: The Impoverishment of Political Discourse* (New York: The Free Press, 1991), 47-75.

¹⁹ *Ibid.*, 75.

of a “national security state.”²⁰ The conscription of Hebern’s cryptographic machine was a good example of encryption policymaking by direct government intervention to help national security. According to Hart, satisfying the requirements of the national security state would dominate science and technology decision-making until the energy crisis in 1973 and the end of the Vietnam War changed the decision-making environment.²¹

Digital encryption development occurred in a new policymaking era. The post-Vietnam War Era saw the convergence of several changes in the United States policy environment. Technology, economic, and social requirements challenged the primacy of national security requirements. Public policies, as expressed through government actions, regulations, and laws would now face mounting commercial influences and social pressures. The 1970s development of the Data Encryption Standard and the invention of public key encryption created new opportunities and responsibilities in society and new worries for the state. Information technology companies, some formed by encryption technology pioneers, perceived the commercial value of encryption and advanced company policies on the role of encryption in satisfying societal and state requirements. Technology companies that formed during the Reagan Era flourished in a period of an empowered commercial sector and relaxed government regulatory controls.

²⁰ David M. Hart, *Forged Consensus: Science, Technology, and Economic Policy in the United States, 1921-1953* (Princeton: Princeton University Press, 1998), 175-205.

²¹ *Ibid.*, 221-231.

In this era, societal requirements challenged state requirements to the extent of threatening national security and public safety.²²

Renewed social activism at the start of the Information Age continued the challenge to policy decisions that previously favored national security requirements. Such decisions were under continual attack by activists and proved to be problematic in enforcement. For example in 1992, MIT professor Phil Zimmermann released public key encryption software on the Internet against the warnings of the United States government. Electronic rights advocates would see encryption as a “vital tool of freedom,” and the United States Department of Justice would look for ways to harass and prosecute Zimmermann.²³ Over time, fluctuating perceptions on information access and security requirements would modulate encryption policy designs according to the prejudices of various actor groups.

Purpose, Thesis, and Research Questions

The purpose of my research is to develop a case study that describes to policymakers the historical relationships among groups of encryption policy actors and explains how group actions influenced encryption policy designs. Policymakers may use

²² Bruce L. R. Smith, *American Science Policy since WWII* (Washington D.C.: The Brookings Institution, 1990), 145-158.

²³ Phil Zimmermann, “Interview with Author of PGP (Pretty Good Privacy),” *High Tech Today Hosted by Russell Hoffman*, 5 February 1996, < <http://www.animatedsoftware.com/hightech/philspgp.htm> >, accessed 10 October 2004.

this information to assess past policy actions and decisions and to advance a more coherent encryption policy. Specific goals for my research are as follows:

- Expand the body of knowledge in the area of technology policy decision-making.
- Generate a research product that categorizes encryption policy actors and explains their decisions and actions over several decades.
- Explain and suggest improvements to the decision-making process in order to produce better encryption policy designs.

If encryption policy design always followed from rational decision-making, then my research would be a documentary on historical cost and benefit decisions. However, encryption policy actors in the United States often use alternative decision-making processes that produce a conglomeration of public policies. The use of alternative decision-making processes confounds rational actors with organizational policies that are incremental by design and are difficult to integrate. In addition, alternative decision-making processes may sacrifice rationality for contests of political power. Thus, rational actors may face a decision-making environment with a loose policy baseline and without the benefits of having to develop alternatives and of choosing the optimum solution.

My thesis is that the United States has great difficulties in producing comprehensive information and encryption control policies and may have future difficulties for three reasons:

- Each group of competitive policy actors will tend to behave in accordance with a favored decision model.

- Groups of competitive policy actors that interact may behave in accordance with common decision models.
- Over time, groups favoring alternative decision-making processes will exhibit complicated organizational learning and political behaviors and will balance groups favoring rational decision-making processes.

My thesis makes important claims about rational and alternative decision-making processes that balance national security and public safety gains against privacy and economic losses. In my research, I examine how policy actor groups using rational and alternative decision-making processes produce public policies that are a conglomeration of rational, procedural, and political policy fragments. In one extreme, fragmented information and encryption control policies may not only perpetuate hostile and criminal activities, but also may create moral hazards among users by encouraging widespread encryption use without commensurate responsibilities and liabilities. In the other extreme, fragmented policies may encourage a healthy competition among groups of actors that may not agree on an optimal policy, but can agree on satisficing policies. Over time, an encryption policy conglomerate may be desirable to groups of policy actors with stable decision behaviors. If these groups have unstable decision behaviors, then an apparent status quo may be a hiatus before the eruption of future policy conflict. My research investigates the likelihoods of both outcomes.

To guide data collection and analysis, I separated my research questions into descriptive and explanatory questions. Answering my descriptive questions provides part of the analytical breadth for my research:

- Who are the major encryption control policy actors?
- What conceptual groups of actors emerge when major encryption events occur?

I will answer my explanatory questions by analyzing the decision-making patterns of these conceptual groups over several periods. I will match the observed patterns with the patterns suggested by Allison's Rational Actor, Organizational Behavior, and Governmental Politics Models. Although Allison developed his models for episodic decision events, encryption events over the past three decades provide a unique opportunity to compare data from long-term observations with the patterns suggested by his models. Answering explanatory questions provides additional analytical breadth and longitudinal depth to my research:

- How strongly do the actions of these conceptual groups correspond with the patterns suggested by Allison's decision models?
- Why do competitive and interactive groups show convergence toward common decision models?
- How stable are these interactions among decision models when projecting future policy decisions?

I will use the answers to these descriptive and explanatory questions to support my hypothesized existence of stable long-term decision behaviors and to suggest better policy designs that will anticipate failures and maintain stability.

Outline of Dissertation

I have organized my dissertation into six chapters with Chapter 1 being the "Introduction." Chapter 2, "Foundation and Theory," examines the spectrum of encryption laws and regulations, reviews relevant studies and scholarly works, and relates decision-making theory to the public policy process. Chapter 3, "Methodology," presents the design of the case study, details the data coding and valance assignment tasks, and discusses the presentation of results in research displays. Chapter 4, "Data and Results," presents the categorized groups of policy actors, the valances of their actions, and a pattern match of their decision-making processes to Allison's models. Chapter 5, "Explanation and Discussion," examines changes in the longitudinal patterns of decision-making events and explains the interactions of policy actor groups and these patterns. Chapter 6, "Conclusion," provides a summary of the research, suggests extensions to the literature on technology policymaking theory, and predicts the requirement for a future information and encryption control policy design.

Chapter Two: Foundation and Theory

The United States Congress is a primary policymaking institution by virtue of its law-making powers. Over the past three decades, Congress has passed laws that both directly and indirectly control encryption use. An examination of these laws provides the chronological context for encryption policymaking. At the heart of successful legislation is a decision-making process that considers the influences of groups of related actors, but does not subordinate policy design to any one of these groups. However, if Congress has problems and is slow in making decisions, then these groups may take actions to make their own individual policies.

Groups of actors outside of the legislative branch are also active in the policymaking process. The executive branch often takes action to fix legislative lapses. Government agencies take routine actions to satisfy regulatory and standardization requirements. A more active judicial branch can take action to balance free speech and privacy rights against public safety and national security requirements, especially when prodded by electronic rights advocates seeking to limit government power. In addition, universities and information technology industries that develop and market encryption technology products are powerful advocates for free-market control of information and encryption technologies. The totality of actions by these groups can substitute for legislative progress, and thus, can become part of the information and encryption policy conglomerate.

Prior researchers have investigated cases of encryption policy development in order to find policy actors and their modes of participation in the policymaking process. These researchers have found that encryption policies trend toward the middle of a policy spectrum that is bounded by voluntary standards at the lower end and by specific laws at the higher end. I will extend this area of research by analyzing the long-term activities of policy actors and by determining how these activities influence decision-making processes. My goal is to explain how short-term actions and policy segments shape long-term decision-making processes, and thus, overall policies.

In the late 1960s, Graham T. Allison developed models to explain why policymakers produce fragmented policies, even when they know that integrated policies normally require rational decisions. Allison's alternative decision-making models, which are the Organizational Behavior Model and the Governmental Politics Model, may explain the trend away from relying on rational decisions to make policies.²⁴ An understanding of how well Allison's decision models explain encryption policymaking requires an examination of the theoretical foundation, assumptions, and mechanisms of action behind these models.

As noted earlier, the *Security and Freedom through Encryption Act of 1999 (SAFE Act)* was the latest and best attempt at a comprehensive encryption law. The failure of the *SAFE Act* to culminate three decades of information and encryption policy activities,

²⁴ Graham T. Allison, "Conceptual Models and the Cuban Missile Crisis," *American Political Science Review* 63, no. 3 (September 1969): 689-718. Allison did not use OBM or GPM in his article, but settled upon these names by the time of his 1999 book *Essence of Decision*.

presents a policy dilemma for the United States that has global consequences. As the world relies on United States encryption standards and generally follows United States policy precedents, the United States is now at the center of a global encryption policy impasse.²⁵ Allison's decision models, being episodic or crisis oriented, were not originally intended to explain long-term interactions among the decision processes that produced this policy dilemma. Since Allison based his models on a synthesis, I will extend his theoretical foundation and synthesis to explain decision-making processes that span decades.

Encryption Laws and Regulations

President Clinton's 2000 National Security Strategy of the United States called for the start of an information technology control program by proposing a balanced encryption technology export policy. However, for the past three decades, Congress has passed over a dozen laws that only partially address the information and encryption control problems.²⁶ None of these laws have succinctly addressed the proposed starting point. Political scientist Walter J. Oleszek believes that Congress may not have the flexibility to make timely and supportive information control policy decisions: "Any decision-making body, Congress included, needs a set of rules, procedures, and

²⁵ World rankings on encryption policy indicate that the U.S. is not an encryption policy leader, despite being the encryption technology leader. See the Electronic Privacy Information Center's, *Cryptography & Liberty 2000 an International Survey of Encryption Policy* (Washington, D.C.: Electronic Privacy Information Center, 2000).

²⁶ The White House, *A National Security Strategy for a Global Age* (Washington, D.C.: GPO, December 2000), 33-34.

conventions, formal and informal, in order to function.”²⁷ In particular, a procedurally bound Congress may be stymied by the rapid actions of competitive policy actor groups seeking to influence the decision process. An examination of the debates behind successful and unsuccessful laws may reveal the information and encryption control areas that have congressional involvement.

Since 1965, more than dozen laws have formed part of the current information and encryption control policy conglomerate. Table 2-1 lists these laws and gives a cursory assessment of their policy focus in terms of supporting economic, international, national security, privacy, and public safety goals. Several of these laws balance multiple and conflicting goals, making them of particular interest to my research. The information contained in these laws and their respective law-making processes are documented in the *Congressional Record* and in congressional hearings and reports. Examinations of the record, hearings, and reports may help identify groups of policy actors and their perspectives on the information and encryption policy designs.

²⁷ Walter J. Oleszek, *Congressional Procedures and the Policy Process*, 4th ed. (Washington, D.C.: CQ Press, 1996), 5.

Table 2-1 Important Laws Shaping Encryption Policy

Year	Common Name	Policy Directions	Notes
1965	<i>Brooks Act</i>	Administrative	Law directs common technology standards
1968	<i>The Foreign Military Sales Act. Changed in 1976 to the Arms Export Control Act</i>	Economic, International, and National Security	Law regulates encryption exports and imports
1969	<i>Export Administration Act of 1969. Renewed in 1979</i>	Economic, International, and National Security	Law regulates encryption exports and imports
1974	<i>The Privacy Act of 1974</i>	Privacy and Public Safety	Law recognizes the threat of gleaned computer data
1978	<i>Foreign Intelligence Surveillance Act of 1978</i>	National Security and Privacy	Domestic surveillance law
1986	<i>Electronic Communications Privacy Act of 1986</i>	Economic, National Security, Privacy, and Public Safety	Use of encryption to protect privacy and economic value
1987	<i>Computer Security Act of 1987</i>	National Security and Economic	Law controls technology through federal standards
1994	<i>Communications Assistance for Law Enforcement Act</i>	Public Safety and Privacy	First law to mention the externalities of encryption use
1996	<i>Economic Espionage Act of 1996</i>	Economic and National Security	Criminal penalties for illegal encryption use
1998	<i>Digital Millennium Copyright Act</i>	Economic and International	Encryption to protect intellectual property
2000	<i>Electronic Signatures in Global and National Commerce Act</i>	Economic and International	Legalizes encryption-based digital signatures
2001	<i>Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act</i>	Public Safety and National Security	Law expands <i>FISA</i> to include surveillance of U.S. citizens
2002	<i>Cyber Security Research and Development Act</i>	Economic, National Security, Privacy, and Public Safety	Basic research and development funding

The 1965 Public Law 89-306, the *Brooks Act*, amended the *Federal Property and Administrative Services Act of 1949* to force the development of “uniform Federal automatic data processing standards” by the Department of Commerce.²⁸ The *Brooks Act* was the basis for the development of Federal Information Processing Standards (FIPS). Under the Department of Commerce, the National Bureau of Standards (NBS) developed a FIPS to cover the original secret key encryption algorithm used by the federal government and subsequently by the private sector. NBS continued to develop standards on the use of encryption to satisfy confidentiality, authenticity, integrity, and non-repudiation requirements. In a controversial move, NBS did not develop a public key encryption standard either to avoid patent infringement issues or to limit federal support of this encryption subsystem.

In 1968, Congress passed Public Law 90-629, the *Foreign Military Sales Act* to amend the *Foreign Assistance Act of 1961*. These laws are contentious in that Congress has modified them more than three dozen times. Congress retroactively changed the name of the 1968 law to the *Arms Export Control Act* in a 1976 amendment.²⁹ The *Arms Export Control Act* balances economic, foreign policy, and national security issues and affects domestic information technology and encryption companies and their customers. The *Arms Export Control Act* extends the reach of Congress into foreign policy affairs and tasks the State Department to regulate the import and export of arms and dual-use

²⁸ *Brooks Act*, U.S. Statutes at Large 79 (1965): 1127-1129.

²⁹ Edward Thompson Company and West Publishing Company staff editors, *United States Code Annotated: 2003 Popular Name Table*, (St. Paul: West Group, 2003), 81.

technologies.³⁰ The *Arms Export Control Act* provides a legal basis for the International Traffic in Arms Regulations (ITAR). The ITAR contains the United States Munitions List that specifically mentions encryption technology.³¹ The ITAR limits the import and export of encryption products, thus affecting both the global encryption market and the domestic availability of encryption products. The national security benefits and economic consequences of regulating encryption are topics of recurring debate among policymakers.

The expiration of Public Law 91-185, the *Export Administration Act of 1969* and the periodic failures to renew its successor, Public Law 96-72, the *Export Administration Act of 1979*, demonstrate the disagreements between the executive and legislative branches on the extent of their regulatory powers.³² Both these laws tasked the Department of Commerce to control exports that affect the national security and economic well-being of the United States. The *Export Administration Act of 1979* directly affects domestic encryption use by limiting the free-flow of encryption products between the domestic and international markets. Since Congress routinely fails to reauthorize this law on time, the executive branch has issued several frenzied executive orders to support the applicable regulations.³³ These actions by the executive branch

³⁰ *Arms Export Control Act, U.S. Code*, vol. 22, sec. 2778 (2001).

³¹ U.S. Department of State, United States Munitions List, *Code of Federal Regulations*, vol. 22, sec. 121 (Washington, D.C.: GPO, 2001): 425. Microfiche.

³² *Export Administration Act of 1969, U.S. Statutes at Large* 83 (1969): 841-847.
Export Administration Act of 1979, U.S. Statutes at Large 93 (1979): 503-536.

³³ One recent failure was in the *Export Administration Act of 2001*, S. 149. *Congressional Record*, 107th Congress, 1st sess., 2001, 147, pt. 8:S459-S479. An example of frenzied activity was the back-to-back executive orders needed to support federal regulations while the *Export Administration Act*

have allowed the Department of Commerce to use the Export Administration Regulations (EAR) as an uninterrupted method of encryption control, even to the extent of subsuming most of the ITAR encryption controls.³⁴

Under the Department of Commerce, the newly named Bureau of Industry and Security (BIS) has replaced the Bureau of Export Administration and now controls information and encryption technology exports and imports. BIS forces compliance with the EAR and with the 1996 Wassenaar Arrangement, which is a supranational agreement that controls the international flow of dual-use technologies. BIS has a complex task in administering layers of overlapping regulations to include the ITAR and EAR. Currently, the EAR contains the most extensive set of federal regulations that control the flow of encryption products and technologies.

Public Law 93-579, the *Privacy Act of 1974*, sought to limit the power of the federal government in collecting, using, maintaining, and disseminating personal information.³⁵ In passing this law, Congress made the following finding: “[T]he increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of

temporarily lapsed. See these two executive orders: President, Executive Order 12923, "Continuation of Export Control Regulations," 30 June 1994, *Federal Register* 59, no. 127 (5 July 1994): 34551-2 and President, Executive Order 12924, "Continuation of Export Control Regulations," 19 August 1994, *Federal Register* 59, no. 162 (23 August 1994): 51747-8.

³⁴ U.S. Department of Commerce, Export Administration Regulations, *Code of Federal Regulations*, vol. 15, secs. 730-744 (Washington, D.C.: GPO, 2001), 185-327. Microfiche.

³⁵ *Privacy Act of 1974*, *U.S. Code*, vol. 5, sec. 552a (2001).

personal information.”³⁶ While protecting individuals from the harmful use of information, the *Privacy Act of 1974* also made exceptions for information collected to satisfy national security and public safety requirements. Perhaps the most important limitation of this law was that it did not provide the means for individuals to secure personal information through such measures as using encryption. Since the *Privacy Act of 1974* places the federal government in charge of protecting computerized personal information, privacy advocates contend that the federal government’s information access requirements often trump privacy rights. This contention is a primary part of the current encryption policy debate.

Public Law 95-511, the *Foreign Intelligence and Surveillance Act of 1978 (FISA)*, codified the concept of domestic intelligence gathering on suspected foreign operatives. *FISA* in its implementation in several sections under Title 50 of the United States Code calls for expanded domestic surveillance, creates an annual report to Congress on domestic surveillance activities, and establishes a “FISA Court” to decide on which activities to approve or disapprove. The application of *FISA* to monitor Internet communications, as being a subset of “wired” communications, causes electronic rights advocates great concern. Since the passage of *FISA* came before the widespread availability of digital encryption, the law does not mention the problems caused by encryption.³⁷ Both foreign operatives and law-abiding citizens using encryption lower the effectiveness of *FISA* authorized surveillance. Recent anti-terrorism laws have

³⁶ *Privacy Act of 1974, U.S. Statutes at Large* 88 (1974): 1896-1910.

³⁷ *Foreign Intelligence and Surveillance Act of 1978, U.S. Code*, vol. 50, secs. 1801-1811 (2001).

strengthened and expanded *FISA*, while electronic rights advocates continue to weaken and constrain *FISA*.

Public Law 99-508, the *Electronic Communications Privacy Act of 1986* was the first law that gave legal weight to the practice of using encryption to protect information. Users of encryption gained legal protection for their information by preventing communications from being “readily accessible to the general public.”³⁸ Thus, users who protect their privacy or their commercially valuable information, no matter how weak or strong such protections are, can have the federal government go after violators and can seek civil damages for relief. In part, this law satisfied satellite video operators who petitioned Congress for a law that protected their encrypted or scrambled signals from non-paying interlopers. This law did not protect users of encryption in the government sector, as the government could “intercept encrypted or other official communications of the United States executive branch entities or United States Government contractors for communication security purposes.”³⁹ This law also protected a computer user from a “computer trespasser,” and this new legal right would have large public policy implications as the numbers of personal computers grew.⁴⁰

Public Law 100-235, the *Computer Security Act of 1987*, as modified by Public Law 104-113, the *National Technology Transfer and Advancement Act of 1995* and by Public Law 104-106, the *Clinger-Cohen Act of 1996*, is the current basis for the

³⁸ *Electronic Communications Privacy Act of 1986, U.S. Code*, vol. 18, secs. 2510-2521 (2004).

³⁹ *Electronic Communications Privacy Act of 1986, U.S. Statutes at Large* 100 (1986): 1848-1873.

⁴⁰ *Ibid.*

production of Federal Information Processing Standards (FIPS) for computer systems used by the federal government.⁴¹ Although originally intended for United States federal government purposes, many FIPS have become standards that support the international community. The *Computer Security Act of 1987* tasked the National Bureau of Standards (NBS), now the National Institute of Standards and Technology, to develop security standards and guidelines for federal computer systems. Specifically, this act gave the NBS the “responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate.”⁴² The link between the National Security Agency (NSA), a Department of Defense organization, and global encryption standards is a matter of controversy in Congress, industry, and among electronic rights advocates.

Public Law 103-414, the 1994 *Communications Assistance for Law Enforcement Act (CALEA)* was the first law to discuss the problem of encryption use by stating requirements for private sector assistance in circumventing encryption. This law directs communication providers to use technical means to recover court-ordered wiretap information if the service provider also supplied the encryption service.⁴³ Congress was not very demanding on the subject of encryption assistance: “A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to

⁴¹ *Computer Security Act of 1987, U.S. Code*, vol. 15, secs. 271-278h and vol. 40, sec. 759d (2003).
National Technology Transfer and Advancement Act of 1995, U.S. Code, vol. 15, sec. 272 (2003).
Clinger-Cohen Act of 1996, U.S. Code, vol. 15, sec. 272 (2003).

⁴² *Computer Security Act of 1987, U.S. Statutes at Large* 102 (1988): 1724-1730.

⁴³ *Communications Assistance for Law Enforcement Act of 1994, U.S. Code*, vol. 18, sec. 2519 (2003).

decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.”⁴⁴ *CALEA* offers no assistance in the likely event of the government having to decrypt an intercepted communication when the telecommunications company does not possess the encryption key. *CALEA* is a policy milestone in that it ended the assumption that the government could break or “crack” encrypted information to satisfy public safety and national security requirements. Government access to encryption keys appears to be the only solution. Congress did not know the extent of illegal encryption use and solved this lack of knowledge with another law.

Public Law 104-294, the *Economic Espionage Act of 1996*, protects trade secrets and industrial information that are vital to the competitiveness and security of the United States.⁴⁵ This law affects encryption policy in three new areas. One area is in the information gathering section of this law that specifies an annual “report to the Congress on the nature and extent of the use of encryption or scrambling technology to facilitate or conceal criminal conduct.”⁴⁶ The requirement for such information implied that Congress did not know the extent of encryption’s negative externalities. The second area is in the control of information or “intangible goods” section of the law. While the *Economic Espionage Act of 1996* does not directly discuss encryption technology, this law protects the intellectual property and software implementations of encryption

⁴⁴ *Communications Assistance for Law Enforcement Act of 1994, U.S. Statutes at Large* 108 (1994): 4279-4298.

⁴⁵ *Economic Espionage Act of 1996, U.S. Code*, vol. 18, secs. 271-278h (2003).

⁴⁶ *Economic Espionage Act of 1996, U.S. Statutes at Large* 110 (1997): 3487-3513.

algorithms developed in the United States. As much of the world's software originates in the United States and as modern software normally has embedded encryption, the *Economic Espionage Act of 1996* provides the government with an additional control mechanism on encryption technology. The third area is the protection of the information infrastructure of the United States. Such a large responsibility instigated political battles in the government over definitions, resources, and jurisdiction.

The *Economic Espionage Act of 1996* in combination with the *Arms Export Control Act* and the *Export Administration Act of 1979* allows for the coercion and prosecution of individuals and companies that release encryption software or source code on the Internet. However, the First Amendment permits the printing of the disputed source code in a book. With such inconsistent encryption controls, electronic rights advocates have defeated government attempts to successfully prosecute individuals who release encryption technology.⁴⁷

Public Law 105-304, the 1998 *Digital Millennium Copyright Act (DMCA)*, relies upon encryption technology to protect copyrighted materials from illegal access and duplication. This law addresses claims from the publishing and entertainment industries that theft of their intellectual property causes severe economic damage to the United States. This law is unique in that it uses the word "encryption" over 20 times. Another important feature of this law is its enforcement of an international agreement

⁴⁷ *Bernstein v United States Department of Justice*, 176 F.3d 1145 (9th Cir. 1999). See the Concluding comments paragraph.

administered by the United Nation's World Intellectual Property Organization (WIPO).⁴⁸

Two notable and related shortfalls of *DMCA* are its contradiction of the reverse engineering principle and its allowance of "legal low-curb" encryption technology for protection of valuable property. Allowing reverse engineering prevents companies from gaining monopolies using obvious technologies, and a legal low-curb entices violators to bypass trivial copy protection schemes and thus break the law. A good example of the problematic enforcement of *DMCA* is the protection of copyrighted digital versatile disks (DVD). The decryption algorithm found in DVD players is simplistic, and the encryption keys are stored on the header area of a DVD. It is illegal to read the keys off this header area without using a licensed DVD player or playback software. In a now famous case, Norwegian teenager Jon Johansen was brought to trial for "cracking" his own DVD by writing software to read and use these keys.⁴⁹

Congress passed the *DMCA*, in large-part, to assist video and music industries in the United States. These industries see *DMCA* as a legal remedy for the lack of an effective encryption system that they could use to protect copyrighted material. However, this legal remedy cannot cure weak engineering. For example, in the *Universal City Studios v. Reimerdes* case, Federal District Judge Lewis A. Kaplan ordered, in accordance with the *DMCA*, that information on the Content Scrambling System (CSS) used to protect

⁴⁸ *Digital Millennium Copyright Act, U.S. Statutes at Large* 112 (1999): 2859-2918.

⁴⁹ Morten Overbye, "Teenager Cleared in Landmark DVD Case," *CNN.com/Technology*, 7 January 2003 < <http://www.cnn.com/2003/TECH/01/07/dvd.johansen/> >, accessed October 2004.

DVDs could not be released on the Internet.⁵⁰ Electronic rights advocates mocked this restriction by printing the information on t-shirts and neckties. *DMCA* enforcement problems show that industry must rely on strong encryption and an effective key management system or digital rights management (DRM) to protect copyrighted material. Government enforcement alone does not work.

The 2000 Public Law 106-229, the *Electronic Signatures in Global and National Commerce Act*, authorizes the use of electronic signatures for many business and government transactions.⁵¹ In a media event, President Clinton signed the law conventionally and electronically. The law focuses on the authenticity, integrity, and non-repudiation capabilities provided by technologies such as public key encryption. Authenticity proves the identity of the person signing the document, while integrity proves the signed document is genuine and not an alteration. Non-repudiation prevents a person from denying that he or she signed the document. Authenticity and non-repudiation may help satisfy law enforcement and national security surveillance activities by removing much of the anonymity behind Internet transactions. In a controversial omission, the law does not address the confidentiality capabilities made possible by the use of public key encryption. Industry and electronic rights advocates suspect that the *Electronic Signatures in Global and National Commerce Act* decoupled confidentiality capabilities from digital signatures to avoid making the encryption control issue into a

⁵⁰ *Universal City Studios et al. v. Reimerdes et al.*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

⁵¹ *Electronic Signatures in Global and National Commerce Act*, *U.S. Statutes at Large* 114 (2001): 464-476.

problem. Another interpretation is that Congress did not want technical specificity in a law that would bias the market toward politically favored solutions.

Public Law 107-56, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)*, reinforces Kingdon's notion of a policy window in which a crisis forces the convergence of problem, policy, and political streams. For the purposes of encryption control policy, the *USA PATRIOT Act* greatly expands *FISA*. For example, Title II of the *USA PATRIOT Act* labeled "Enhanced Surveillance Procedures" expands the surveillance scope from foreign agents to "United States persons."⁵² As *FISA* surveillance activities and procedures now apply to citizens, the American Civil Liberties Union envisions that this law will cause great harm to privacy rights. "Just six weeks after the September 11 attacks, a panicked Congress passed the 'USA PATRIOT Act,' an overnight revision of the nation's surveillance laws that vastly expanded the government's authority to spy on its own citizens and reduced checks and balances on those powers, such as judicial oversight."⁵³ Increased encryption use by law-abiding citizens, criminals, spies, and terrorists may be an unintended consequence of the *USA PATRIOT Act*. Problematically, this law has no provisions to address legitimate and illegitimate encryption use.

⁵² *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, U.S. Statutes at Large* 115 (2001): 272-402.

⁵³ Jay Stanley and Barry Steinhardt, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society," *ACLU Technology and Liberty Program*, 9 January 2003 <<http://www.aclu.org/SafeandFree/SafeandFreeMain.cfm>>, accessed October 2004.

The 2002 Public Law 107-305, the *Cyber Security and Development Act* authorizes funding for research and development of encryption technology to enhance computer security. This law is specifically concerned about protecting the economic, privacy, and public safety aspects of digital information. Congress stipulated that the National Science Foundation (NSF) administer much of the authorized funding and that institutions of higher learning receive millions of dollars to pursue research in areas such as encryption security and circumvention.⁵⁴ The *Cyber Security and Development Act* is typical of laws that seek a technology solution to the encryption policy dilemma. Research on encryption technology that is secure enough to protect privacy and valuable information, while being amenable to government surveillance requirements, may provide policymakers with solutions to end the policy impasse.

Prior Studies and Research

Individuals, government organizations, professional associations, and electronic rights advocates have studied and researched information and encryption control policies. Their findings have not stimulated the production of coherent policy, because many of these researchers have not identified the decision process as being integral to the policy problem. For the purposes of review, I have separated prior encryption studies and research into policy studies, engineering demonstrations, and scholarly research

⁵⁴ *Cyber Security Research and Development Act, U.S. Statutes at Large* 116 (2002): 2367-2382.

categories. In each category, I identified policy actors, isolated the policy issue, or used the findings and ideas to shape my research design.

Policy Studies

The Association of Computing Machinery (ACM) conducted an early encryption policy study in 1993. The ACM is a professional organization with a membership largely comprised of technically skilled individuals. The ACM published their study as a report titled "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy." The ACM study focused on the federal Escrowed Encryption Standard (EES) and the potential benefits and likely repercussions of using this standard. EES forces users to escrow or place their encryption keys in a government facility. When authorized by a court order, a key escrow system allows the government to decipher encrypted communications and information. The ACM found that government encryption solutions, which by satisfying divergent information access and security requirements, caused policy problems. While the ACM avoided hard decisions by recommending a neutral and conflicting encryption policy, the ACM did acknowledge the global effects of United States encryption policy decisions:

The United States can legislate policy only within its borders, but the global impact of our domestic political decisions should not be underestimated. The choices the United States makes about escrowed encryption, confidentiality of

communications, and government access to encrypted communications will reverberate across the globe.⁵⁵

The ACM study suggested that United States decision-making processes may have to consider global issues along with the domestic encryption policy agenda.

A 1994 report by Congress' Office of Technology Assessment (OTA) documented the encryption policy debate, but did not make a policy recommendation. The OTA report, titled "Information Security and Privacy in Network Environments," documented three important characteristics of United States encryption policy. The first characteristic was defining the encryption control problem in terms of a tension between opposing goals:

The federal government faces a fundamental tension between two important policy objectives: 1) fostering the development and widespread use of cost-effective information safeguards, and 2) controlling the proliferation of safeguard technologies that can impair U.S. signals-intelligence and law-enforcement capabilities.⁵⁶

Like the ACM study, OTA believed that opposing goals or "objectives" were likely to cause problems with the decision-making process.

The second characteristic was the use of Federal Information Processing Standards (FIPS) to control technology. OTA concluded that the use of government standards, such

⁵⁵ Susan Landau, et al., *Codes, Keys and Conflict: Issues in U.S. Crypto Policy: Report of a Special Panel of the ACM U.S. Public Policy Committee* (New York: Association for Computing Machinery, June 1994), 64-66.

⁵⁶ U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC: GPO, September 1994), 8-9.

as the Escrowed Encryption Standard, caused problems with the private sector: "In OTA's view, both the EES and the DSS [Digital Signature Standard] are federal standards that are part of a long-term control strategy intended to retard the general availability of 'unbreakable' or 'hard to break' cryptography within the United States. The reasons are to meet national security and law enforcement requirements."⁵⁷ OTA's opinion is the first official acknowledgement that government standards can control encryption technology with or without legislative approval. Allowing government agencies to make encryption policy through organizational actions may threaten the abilities of the executive and legislative branches to make complementary policy decisions.

The third characteristic noted by OTA was the problem of having different domestic and international encryption policies. In their report, the OTA questioned the rationality and ability of the United States to follow two policies. OTA discussed the conflict among congressional committees trying to liberalize software and encryption export laws to satisfy economic requirements and other committees trying to tighten laws to satisfy national security requirements.⁵⁸ In the case of divergent policy views, decision makers may have to formulate satisficing alternatives in order to facilitate a rational decision-making process or accept organizational and political decisions.

⁵⁷ *Ibid.*, 10-11.

⁵⁸ *Ibid.*, 12-13.

The National Research Council (NRC) studied encryption policy at the request of Congress. The NRC is the operational arm of the National Academy of Sciences (NAS). Congress chartered the NAS in 1863 to provide advice on research and development policy and to compensate for the lack of a federal department dealing exclusively with science and technology policy.⁵⁹ NRC published their findings in a 1996 report titled “Cryptography’s Role in Securing the Information Society.” The NRC report contained over 700 pages and produced five major and many more secondary recommendations.

The NRC recommendations were broad and polar, thereby avoiding the hard task of combining and tailoring recommendations to produce satisficing alternatives. The first recommendation of the NRC was as follows: “No law should bar the manufacture, sale, or use of any form of encryption within the United States.”⁶⁰ The second recommendation was that the executive and legislative branches should formulate encryption policy. The third recommendation was that policy affecting commercial encryption “should be more closely aligned with market forces.”⁶¹ This recommendation runs counter to the second recommendation in that the control of encryption’s externalities requires public policy. The fourth recommendation was as follows: “Export controls on cryptography should be progressively relaxed but not eliminated.”⁶² The fifth recommendation suggested that “law enforcement and national security” should face the

⁵⁹ A. Hunter Dupree, *Science in the Federal Government: A History of Policies and Activities* (Baltimore: Johns Hopkins University Press, 1985), 135-148.

⁶⁰ Kenneth W. Dam, and Herbert S. Lin, eds., *Cryptography’s Role in Securing the Information Society* (Washington, D.C.: National Academy Press, 1996), 303.

⁶¹ *Ibid.*, 304.

⁶² *Ibid.*, 305.

“new technical realities of the information age.”⁶³ However, the fifth recommendation was a capitulation to the encryption liberalizing first and third recommendations. By not reconciling conflicting recommendations, the NRC report implied that policymakers would face encryption control decisions without the help of technology solutions from sponsored research and development efforts. This may not be the case, as new encryption technologies may make encryption control easier by requiring a common level of trust among the government, encryption service providers, and encryption users.

In 2000, the Congressional Research Service (CRS) produced an issue brief titled “Encryption Technology: Congressional Issues.” In this brief, CRS recapped encryption policy events that happened between 1994 and 2000 and covered encryption related bills of the 105th and 106th Congresses. CRS noted a gradual shift in administration policy toward loosening export restrictions on encryption technology. An important caveat was that the Clinton administration favored using mandatory escrowed-key encryption technology for exported products. CRS also noted a disagreement between FBI Director Louis Freeh and the administration over escrowed-key encryption for domestic use.⁶⁴ The CRS brief highlighted the difficulties in achieving a policy consensus, even within a single branch of government.

⁶³ *Ibid.*, 322.

⁶⁴ Richard M. Nunno, *Encryption Technology: Congressional Issues*, CRS Issue Brief for Congress, IB96039, 14 July 2000. Available from the National Council for Science and the Environment (NCSE) server at < <http://www.ncseonline.org/NLE/CRSreports/Science/st-40.cfm?&CFID=13501874&CFTOKEN=58518647> >, accessed April 2004.

Encryption key recovery was a recurring theme identified by the CRS. The decision on how to implement key recovery or a key management infrastructure (KMI) may be the centerpiece of future policy decisions. One solution favored by CRS was market control of encryption: “Many opponents of encryption controls agree that key recovery has advantages for recovering a lost, stolen, or corrupted key, but believe market forces will drive the development of a KMI for stored computer data without government involvement.”⁶⁵ The CRS brief documented for the first time a satisficing policy alternative that proposes market-controlled encryption with a key recovery feature. However, CRS did not produce cost and benefit information to support this alternative. In addition, CRS did not explain how the market would handle encryption externalities that affect national security and public safety requirements.

Engineering Demonstrations

Brute-force “cracking” tries all the possible encryption keys to find the decryption key. The cost of and time for cracking are measures of encryption strength, and both measures grow exponentially as the number of bits in the encryption key increases. Satisfying national security and public safety requirements for information access may mean the expenditure of millions of dollars and may take weeks or years of cracking time. Little unclassified data exists on the costs of cracking, but the data is critical for making rational decisions on key-length restrictions. Until recently, only speculative data for cracking costs existed. One estimate from journalist James Bamford, who researched

⁶⁵ *Ibid.*

the NSA for his book *The Puzzle Palace*, was “septillions of dollars.”⁶⁶ An engineering demonstration would produce a more accurate estimate.

The Electronic Frontier Foundation (EFF) sponsored a 56-bit Data Encryption Standard (DES) code-breaking project to demonstrate the obsolescence of DES and to document the cracking cost.⁶⁷ Anecdotal evidence suggested that NIST and NSA tinkered with the 1970s vintage DES key length of 56-bits to allow for cracking.⁶⁸ In 1998, EFF built a DES cracker for \$210,000. This cracker could exhaustively searched through the entire 56-bit key space or 72 quadrillion (72×10^{15}) keys in order to find the single decryption key. An opportunity to use the DES cracker came in 1999 when RSA Security sponsored a DES code-breaking contest on the Internet.⁶⁹ The DES cracker, along with thousands of Internet computer participants orchestrated through a consortium called “Distributed.net,” searched for and found the decryption key in 22 hours.

EFF used the relative ease of cracking DES as a reason to suspect government encryption standards and to question the supposed high costs of cracking. EFF concluded the following in their study: “It appears that highly credible people were either deliberately lying to Congress and to the public in order to advance their own harmful agendas, or were advocating serious infringements on civil liberties based on their own

⁶⁶ James Bamford, *The Puzzle Palace: A report on America's Most Secret Agency* (Boston: Houghton Mifflin Company, 1982), 348.

⁶⁷ Electronic Frontier Foundation, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (Sebastopol, C.A.: O'Reilly & Associates, 1998), 1-1 to 1-18.

⁶⁸ Bruce Schneier, *Applied Cryptography*, 2d ed. (New York: John Wiley & Sons, Inc., 1996), 265-301.

⁶⁹ RSA Security, “RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF),” 19 January 1999 < http://www.rsasecurity.com/company/news/releases/pr.asp?doc_id=462 >, accessed April 2004.

ignorance of the underlying issues.”⁷⁰ This insinuation by EFF has some merit in that the government, purposefully or inadvertently, achieved encryption control by limiting the encryption key size of DES.

In 2002, Distributed.net completed a four-year effort to crack a version of the commercial RC5 encryption system that uses a 64-bit key. Their press statement shows that cracking time has increased exponentially from the 22 hours required for DES:

So, after 1,757 days and 58,747,597,657 work units tested the winning key was found! While it's debatable that the duration of this project does much to devalue the security of a 64-bit RC5 key by much, we can say with confidence that RC5-64 is not an appropriate algorithm to use for data that will still be sensitive in more than several years' time.⁷¹

Distributed.net does bring up a concern that the selected encryption key length should guarantee confidentiality for many years after the time of encryption. However, national security and public safety cracking efforts are likely to incur exponentially growing costs and cracking times, if encryption technology is solely driven by requirements to protect data for years after the original use of encryption. Although there is a market desire for encryption systems with key lengths above 64-bits, policymakers must determine the trade-offs with national security and public safety requirements. The 64-bit encryption threshold, which was the mainstay of the Export Administration Regulations in the 1990s, may still be a viable policy alternative.

⁷⁰ Electronic Frontier Foundation, *Cracking DES*, 1-6.

⁷¹ Distributed.net, Distributed.net completes RC5-64 project, 25 September 2002, <<http://www.distributed.net/pressroom/news-20020926.txt>>, accessed April 2004.

Scholarly Research

Three recent dissertations used historical information about encryption policy development to support theories on information technology policymaking. All three used textual data on encryption events and policy actors to support their theories on government control of information and communication technology (ICT). I present a review of these dissertations in order of their publication dates.

The first dissertation I reviewed was by Jeffery W. Seifert from Syracuse University. He wrote a dissertation titled “Who(se) Rules (for) the Internet: Regime Formation and Global Public Policy for the Information Age.” Seifert explored failures in the CLIPPER Chip policy and concluded that ICT policies trend toward the center of a rule system continuum. The CLIPPER Chip was a hardware implementation of a similar system to the one specified by the Escrowed Encryption Standard. CLIPPER would have controlled the negative externalities of encryption by allowing the government to reconstruct a user’s encryption key. CLIPPER technology relied on trusted United States government escrows, each holding a copy of the key or information required to reconstruct the encryption key. Only government authorization or a court order would allow key release or reconstruction to take place. In theory, this would reduce the potential for government abuse.

Seifert developed a rule system continuum with points labeled “Market or Low Government Involvement,” “Self Regulation,” “Epistemic Communities,” “Mixed Regimes,” and “National Laws or High Government Involvement” to explain ICT policy

development.⁷² Seifert manually coded 391 pieces of textual material by categorical areas, such as authorship and audience, and by rule areas, such as key length and key escrow. Additionally, the rule area used a “-, 0, +” valance coding system to assist with the analysis.⁷³

Seifert found that governmental actors favored Mixed Regimes that used regulations, while non-governmental actors favored Mixed Regimes that used instructions. Regulations specify enforceable encryption control parameters, while instructions are more trusting by allowing the use of voluntary encryption control parameters. Seifert also found that no actor groups favored the low end of control, which was his Market approach. In addition, no actor groups favored the high end of control, which was his National Law approach. Seifert’s detailed analysis of the individual actors within the government group showed a difference between the executive and legislative branches. He found that the executive branch was more likely to specify regulations, while the legislative branch was less likely to do so.⁷⁴

I believe that Seifert’s narrow selection of the escrowed encryption case limited his findings and that a longitudinal examination of encryption actors and policies may reveal a greater spectrum of policy preferences. I agree with Seifert’s level of analysis that separated the large government actor group into smaller groups, such as the executive

⁷² Jeffery W. Seifert, “Who(se) Rules (for) the Internet: Regime Formation and Global Public Policy for the Information Age” (Ph.D. diss., Syracuse University, 2000), 10-39.

⁷³ *Ibid.*, 165-168.

⁷⁴ *Ibid.*, 100-113.

branch and the legislative branch. In the area of methodology, Seifert manually manipulated his data, but he believes that digital textual material “can be used for enhanced analysis in the future using computer-based techniques.”⁷⁵ I will follow Seifert’s original manual methodology, as the lack of digital texts before 1990 would create digitizing work and would bias my research toward data found in recent digital texts.

The second dissertation I reviewed was by Vandana Pednekar-Magal from Bowling Green State University. She wrote a dissertation titled “State Surveillance and the Telecommunication Policy Process: The Politics of US Encryption Policy.” She also used the Escrowed Encryption Standard case to support her thesis. Pednekar-Magal found that current telecommunications policymaking theories were inadequate for contentious policies. She used a case study methodology developed by qualitative research expert Robert C. Yin to find pattern matches against pluralist, managerialist, and neo-Marxist perspectives of state policymaking.⁷⁶ In her dissertation, she used the ideas found in Alford and Friedland’s *Powers of Theory: Capitalism, the State and Democracy* to produce these contrasting perspectives.⁷⁷ She defined the pluralist perspective as one that maximizes political consensus through “the actions of individuals and groups in specific political situations.”⁷⁸ In contrast, the managerialist perspective “asserts that bureaucratic executives tend to dominate the policy process and implement policy inside

⁷⁵ *Ibid.*, 69-70.

⁷⁶ Vandana Pednekar-Magal, “State surveillance and the telecommunication policy process: The politics of United States encryption policy” (Ph.D. diss., Bowling Green State University, 2000), 10-12.

⁷⁷ *Ibid.*, 7.

⁷⁸ *Ibid.*, 27-29.

and outside the state through cooperation with private organizations.”⁷⁹ She defined the Neo-Marxist perspective as the policymaking efforts required to maintain the interrelations among the state, capitalism, and classes.⁸⁰

Pednekar-Magal used these perspectives in her research as Yin’s propositions or theories of action. In determining the fit of the Escrowed Encryption Standard case to her propositions, Pednekar-Magal found that each proposition explained some policymaking attributes of the case. While she found that no proposition was completely adequate in explaining the broader account of policymaking, she concluded that the “managerial perspective of the state resonates best with the findings of the case study.” She also concluded the following: “[The Escrowed Encryption Standard] policy was geared toward maintaining the state’s monopoly in the development of encryption standards.”⁸¹

In my research, I extend Pednekar-Magal’s idea that technology standards are important control mechanisms that do not require authoritative laws or regulations to be effective. I will challenge Pednekar-Magal’s conclusion that the state has a monopoly in creating standards with the idea that other actors, such as encryption vendors and professional organizations, also create competitive encryption standards. Pednekar-Magal’s use of Yin’s methodology and three propositions reinforced my decision to use a similar methodology. However, I will use data that spans a much longer period in order to gain more longitudinal depth.

⁷⁹ *Ibid.*, 29-33.

⁸⁰ *Ibid.*, 33-39.

⁸¹ *Ibid.*, 152-156.

The third dissertation I reviewed was by Glenda Nadine Morgan from the University of Minnesota. Morgan wrote a dissertation titled “The message and the medium: Electronic communications technologies and global policy change in copyright, privacy and encryption.” She used three technology cases to explain the existence of “virtual epistemic communities.” According to Morgan, virtual epistemic communities use a combination of organizations and interpreters as policy actors in an international policy environment. Morgan found that older theories, such as technological determinism where technology drives changes, various forms of realism where state power drives changes, and constructivism where shared meaning drives changes, were unable to account for changes in an electronically networked world.⁸²

Morgan used a qualitative methodology to show policymaking parallels among three electronic communication policy cases. Morgan’s third case considered global encryption policy. She used information on the Escrowed Encryption Standard and the activities of the Bureau of Export Administration to demonstrate that government power controls encryption. Morgan then used the reactions of interpreters and organizations to support her idea of a virtual epistemic community that tempers government control. Her examples of interpreters included privacy rights activists such as Marc Rotenberg from the Electronic Privacy Information Center (EPIC) and Alan Davidson from the Center for Democracy and Technology (CDT). Her examples of organizations included the

⁸² Glenda Nadine Morgan, “The message and the medium: Electronic communications technologies and global policy change in copyright, privacy and encryption” (Ph.D. diss., University of Minnesota, 2001), 18-41.

American Civil Liberties Union and the Global Internet Liberty Campaign.⁸³ After examining the activities of interpreters and organizations, Morgan concluded that the “global epistemic community organized around encryption showed the potential of electronic communication technology to challenge government authority.”⁸⁴

In my research, I will investigate how electronic rights advocates, such as CDT and EPIC, influence encryption policy decisions. Morgan’s research indicated that this influence is significant and is global in nature. I also will expand on Morgan’s idea of international actors affecting United States domestic encryption policy. International encryption policy actors may include the International Standards Organization (ISO), Organization for Economic Cooperation and Development (OECD), the Wassenaar Arrangement, and the World Intellectual Property Organization (WIPO).

Allison’s Decision Models

Decision models use historical evidence to determine the likelihood of future public policy decisions. United States public policies are government decisions to provide broad societal benefits that individuals ultimately pay for. While policy actors are normally government decision makers, peripheral actors outside of government can also become decision makers by influencing policy design or by taking direct action. Researchers can use Allison’s decision models to explain how policy actors, such as

⁸³ *Ibid.*, 300-311.

⁸⁴ *Ibid.*, 322.

electronic rights advocates, encryption vendors, governmental branches and agencies, international organizations, professional organizations, and research and development entities, make encryption policy. Allison's decision models are the Rational Actor Model (RAM), the Organizational Behavior Model (OBM), and the Governmental Politics Model (GPM). Allison, a professor at Harvard University, used earlier versions of these models in his famous paper on the Cuban Missile Crisis published in 1969.⁸⁵

Subsequently, Allison published two books on the use of his models, one in 1971 and one in 1999. In his most recent book titled *Essence of Decision: Explaining the Cuban Missile Crisis*, Allison expanded the applicability of his models beyond national security issues. Allison and his coauthor Philip Zelikow applied these models to general decision-making events found in public policies and business practices. Although the new and expanded models have a coauthor, I will refer to them as Allison's decision models.⁸⁶

Allison's decision models have five components that overlap by varying degrees. I reduced these overlaps to increase the precision of his models. The first component or "Basic Units of Analysis" are the decision events in question. The second component or "Organizing Concepts" are the relationships between actors and actions. The third component or "Dominant Inference Pattern" covers the motivating force or logic in selecting a course of action. The fourth component or "General and Specific

⁸⁵ Graham T. Allison, "Conceptual Models and the Cuban Missile Crisis," *American Political Science Review* 63, no. 3 (September 1969): 689-718. I used Allison's most recent names for these models.

⁸⁶ Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown and Company, 1971).

Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* 2d ed. (New York: Longman, 1999), 13-75, 143-196 and 255-324.

Propositions” are the actions and events predicted by the selected model. The fifth component or “Evidence” is an explanatory story built from the evidence.⁸⁷ I will develop and sharpen the first four components for each of Allison’s decision models.

Rational Actor Model

Allison’s Rational Actor Model posits that actors make utility maximizing decisions based principally on cost and benefit information. His Rational Actor Model thus serves as a predictable baseline to compare and contrast his alternative decision models. Allison believes that making rational decisions is a human proclivity that can solve economic, political, and social problems. Allison cited various scholars, ranging from sociologist Seymour Martin Lipset to economist Herbert Simon, in order to demonstrate the widespread use of rational decision-making theory. Allison tailored rational decision-making theory for use in practical situations by incorporating Simon’s idea of “bounded rationality” and Robert Axelrod’s game theory “win-win” outcomes. In practical situations faced by rational actors, the right decision may not be utility maximizing for an individual actor. If reaching consensus is important, such as in an iterative policy game, then the right decision may be the one that produces higher payoffs for multiple actors.⁸⁸

I accept Allison’s derivation of his Rational Actor Model with one modification. Expanding on Herbert Simon’s “satisficing” idea, policymakers in a pluralistic

⁸⁷ Allison and Zelikow, *Essence of Decision*, 24-26, 163-185, and 294-313.

⁸⁸ *Ibid.*, 13-23.

democracy reach consensus by going through the process of formulating satisficing policy alternatives, ranking these alternatives, and choosing the best alternative.⁸⁹ The requirement for producing satisficing alternatives may be more difficult to achieve in the United States. As I noted earlier, Canada had no problems in passing a law that specifies the rights and responsibilities of Canadians to use electronically protected information. The unitary actor concept is organic to parliamentary decision-making, as the ministers in the executive branch are also part of the legislative branch. The shared power arrangement in the United States may require more effort to pass legislation, especially technology legislation that is perishable. A large part of policy effort in the United States is often expended on political maneuvering among the executive, legislative, and judicial branches of government, while the generation of alternatives lacks emphasis.

In the United States, the process of formulating satisficing alternatives may train multiple actors to behave as a unitary actor. Multiple policy actors, so trained, may speed-up policy design by efficiently formulating, ranking, and choosing policy alternatives. When feedback from the policy implementation phase becomes available, these trained policy actors can use this feedback and the knowledge gained from making past decisions to formulate even better policy alternatives. A consequence of waiting for information to produce better alternatives is having a lethargic process. To fix the lethargy associated with rational decision-making, the speed of the alternative formulation process may have to match the rate of technology advancement.

⁸⁹ Herbert A. Simon, "Rational Decision Making in Business Organizations," *The American Economic Review* 69, no. 4 (September 1979): 493-513.

Table 2-2 shows the Rational Actor Model components and examples applicable to my research. The examples incorporate modifications to handle the satisficing alternative concept.

Table 2-2 Modified Rational Actor Model⁹⁰

Rational Actor Model Components	Examples
Basic Unit of Analysis	<ul style="list-style-type: none"> • Cost and benefit considerations determine the decision agenda • Satisficing alternatives allow pluralistic actors to make choices as if they were a unitary actor
Organizing Concepts	<ul style="list-style-type: none"> • A unitary actor or a group of actors is the decision maker • Defining the problem and finding alternatives or solutions set the decision agenda • Developing satisficing alternatives fosters unified action
Dominant Inference Patterns	<ul style="list-style-type: none"> • Actions or policies result from value maximizing decisions • Satisficing alternatives are value maximizing to a group of actors and not to any individual actor
General and Specific Propositions	<ul style="list-style-type: none"> • Cases that show quantification of the problem and selection of the best alternative • Cases that show generation of satisficing alternatives and consensus building in the selection of the alternative that is optimum to the group

⁹⁰ Rational Actor Model adapted from Allison and Zelikow, *Essence of Decision*, 24-26.

Organizational Behavior Model

Allison's Organizational Behavior Model posits that decisions are the products of organizational actions. Allison created the Organizational Behavior Model as an alternative model that does not rely on rational actor decisions for explanations. In this model, he believes that decisions are the resultant of organizational structures and processes. Policy experts use the phrase "following standard operation procedures" to describe the effects of organizational culture and learning on making routine decisions. Allison cited the older works of Adam Smith and Max Weber and the more modern works of Richard Cyert, James March, Johan Olsen, and James Q. Wilson to show that specialized organizations are more efficient problem solvers than are groups of individuals.⁹¹ The organization exists, in large part, to solve problems. A question not fully answered by Allison is the relative contributions of the "organization" as an entity and the organization's internal "organizing" processes to this noted problem solving efficiency.

Allison explained organizational behavior through its relationships with organizational logic and culture. However, Allison did not make a required distinction between organizations and organizing. While the structure of an organization may affect its short-term decision-making abilities, I believe that the longer-term decision-making patterns of an organization or its "organizing" abilities result from adaptive organizational learning processes. These adaptive processes allow for the internal

⁹¹ Allison and Zelikow, *Essence of Decision*, 143-160.

modification of the organization's structure and processes in response to changes in the decision-making environment. Organizations may follow standard operating procedures for short-term control of technology advancements. Over time, "hard" problems caused by technological advancements may induce organizational changes.

Organizational learning expert Chris Argyris used the idea of double-loop learning to explain how organizations function and adapt when confronted by hard problems. Single-loop learning occurs when an organization uses trial and error guesses, often based on what worked before, to select a solution from a list of alternatives. Double-loop learning adds the ability of the organization to change its "governing variables."⁹² Argyris defined governing variables as the actions of individuals that "drive and guide" the organization. Argyris believes that single loop learning is more "appropriate for the routine, repetitive issue." This belief matches Allison's idea of organizations following standard operating procedures in order to solve problems. Argyris' substantial contribution to organizational learning is that double-loop learning can solve "complex, non-programmable issues" and ensures "that there will be another day in the future of the organization."⁹³ In the short-term, the appearance of actions that follow standard operating procedures may mask changes in organizational processes or "organizing" brought about by leaders internal to the organization. Over time, pattern matching the actions of an organization against the Organizational Behavior Model may reveal the

⁹² Chris Argyris, *On Organizational Learning*, 2d ed. (Malden, Massachusetts: Blackwell Publishers, 1999), 65-71.

⁹³ *Ibid.*, 68-69.

effects of this organizing process. One anticipated effect is the creation of a highly efficient problem solving organization that may lure policymakers away from using rational actor or political decision processes.

Table 2-3 Modified Organizational Behavior Model⁹⁴

Organizational Behavior Model Components	Examples
Basic Unit of Analysis	<ul style="list-style-type: none"> • “Organizational outputs” determine the decision agenda • Organizational behavior changes over time in response to governing variables
Organizing Concepts	<ul style="list-style-type: none"> • Organizations as actors • Problems are “fractionated” according to organizational abilities and initial solutions follow “standard operating procedures” • Failed solutions are important in changing governing variables
Dominant Inference Patterns	<ul style="list-style-type: none"> • Actions or policies result from organizational processes • Actions or policies change over time as individuals in the organization react to the problem environment
General and Specific Propositions	<ul style="list-style-type: none"> • Cases that show the use of organizational actions to incrementally solve pieces of a problem • Cases that show the relationship between organizing adaptations and new solutions to hard problems

Table 2-3 shows the Organizational Behavior Model components and examples applicable to my research. The examples incorporate modifications to handle Argyris’

⁹⁴ Governmental Politics Model adapted from Allison and Zelikow, *Essence of Decision*, 164-185.

idea of governing variables that may account for long-term changes in organizational behavior.

Governmental Politics Model

The Governmental Politics Model posits that actors make politically motivated decisions in order to solve problems. Allison created the Governmental Politics Model as an alternative decision model that does not rely on rational actor decisions or organizational behaviors for explanations. Allison cited the works of political scientists Richard Neustadt on presidential power and John Kingdon on government agenda setting to demonstrate how political power affects decision-making processes. In addition, Allison introduced the idea of an “action channel” or problem solver in his GPM. The action channel can be a person or a group that a political leader selects to solve a particular issue.⁹⁵ The action channel is similar to Kingdon’s idea of policy entrepreneur. The actions of a policy entrepreneur often lead to the metaphoric coupling of problem, policy, and political streams into Kingdon’s “policy window.”⁹⁶

The identification of an action channel and the determination of the political role in decision-making are major aspects of the Governmental Politics Model. As researchers uncover new evidence on action channels and political roles, they often find that politics plays a larger role in decision-making than was previously reported. For example, researchers have reevaluated Allison’s original case study on the Cuban Missile Crisis

⁹⁵ Allison and Zelikow, *Essence of Decision*, 255- 294.

⁹⁶ Kingdon, *Agendas, Alternatives, and Public Policies*, 165-195.

and have found greater support for the Governmental Politics Model.⁹⁷ To expand the search for action channels in encryption policymaking, the dynamics of political power in Congress and the political power wielded by the federal courts require further investigation.

Politics can affect congressional processes that determine policy. Encryption policymaking in the House of Representatives may be especially vulnerable to political effects. Congressional scholar Walter Oleszek notes that, when compared to the Senate, power in the House is more unevenly distributed, political affiliations are more important, and rule following is more stringent.⁹⁸ By virtue of its size, the House introduces more bills than the Senate and has more committee members to orchestrate in the passage of these bills. Committee chairs use politics and consensus in moving bills through their committee processes. In the case of encryption policy, several committees may have to approve the proposed bill, and committees often “mark-up” a bill to suit the agendas of their committee chairs. The chairs of important and powerful committees usually determine the political content of proposed legislation by competing to be the final committee to mark-up a bill. Committee processes and bill sequencing thus serve as indicators of political influence. In addition, committee chairs may be the action channels for actors inside and outside of Congress.

⁹⁷ The recent releases of papers and recordings from the President Kennedy and President Johnson periods have led to reinvestigations of the Cuban Missile Crisis. See Timothy J. McKeown, “The Cuban Missile Crisis and Politics as Usual,” *The Journal of Politics* 62, no. 1 (February 2000): 70-87.

⁹⁸ Walter J. Oleszek, *Congressional Procedures and the Policy Process*, 4th ed. (Washington, D.C.: CQ Press, 1996), 25-38.

The lengthy and political process for selecting federal court justices invites politics into the judicial system. Over time, these judges may turn to judicial activism and in effect become action channels for policies that are not specified in laws or are contrary to existing laws. Privacy rights advocates often dispute the claim that judicial activism is a recent political occurrence by citing the 1928 wiretapping case *Olmstead v. United States* as proof of the early and supposedly less political origin of privacy rights.⁹⁹ In writing the dissent to this case, Supreme Court Justice Brandeis used a late nineteenth century idea on the “right to be left alone” and applied it to a wire-tapping case: “They [authors of the Constitution] conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men.”¹⁰⁰ However, judicial scholar Robert Bork supports a more recent political origin of the right to privacy by showing that the politicization of the 1953-1969 Warren Court affected subsequent major Supreme Court decisions.¹⁰¹ In politically sensitized courts, actors elevating the importance of free speech and privacy rights over national security and public safety requirements can influence encryption policy.

Table 2-4 shows the Governmental Politics Model components and examples applicable to my research. Allison’s original model generally covers the effects of political influence on the executive branch and government agencies. The examples in

⁹⁹ *Olmstead v. United States*, 277 U.S. 438 (1928).

¹⁰⁰ The U.S. Supreme Court case has Justice Brandeis’ dissent. See *Olmstead et. al. v. United States*, 277 US 438-488 (1928).

The “right to be left alone” idea dates back to the mid-1800s. See Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy,” *Harvard Law Review* IV, no. 5 (December 15, 1890): 193-220.

¹⁰¹ Robert H. Bork, *The Tempting of America: The Political Seduction of the Law* (New York: The Free Press, 1990), 69-100.

table 2-4 incorporate modifications to handle the effects of political influence on the legislative branch and the federal judicial system. To simplify my research and to avoid a detailed analysis of the federal judicial system, I used information and encryption control cases found in the popular media.

Table 2-4 Modified Governmental Politics Model¹⁰²

Governmental Politics Model Components	Examples
Basic Unit of Analysis	<ul style="list-style-type: none"> • “Political bargaining” by the executive, legislative, and judicial branches determines the decision agenda
Organizing Concepts	<ul style="list-style-type: none"> • Players and their positions as part of a political game • “Perceptions and parochial priorities” are important in deciding between conditions and problems • “Action channels” in all three branches of government
Dominant Inference Patterns	<ul style="list-style-type: none"> • Actions or policies result from political bargaining games • Political “pulling and hauling” as the ultimate arbitrator among the three branches of government
General and Specific Propositions	<ul style="list-style-type: none"> • Cases that show a political demarcation between conditions and problems • Cases that show a reliance on actions channels from the three branches of government to solve problems

¹⁰² Allison and Zelikow, *Essence of Decision*, 294-313.

Policy Dilemma and the Need to Extend Theory

What has been a simple encryption policy decision in other countries has become a policy dilemma in the United States. The proposed *Security and Freedom Through Encryption Act (SAFE Act)* originated in the second session of the 104th Congress. Representative Robert Goodlatte (R-Virginia) introduced the bill on March 5, 1996, as H.R. 3011. The main point of this encryption-liberalizing bill was as follows:

It shall be lawful for any person within any State, and for any United States person in a foreign country, to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.¹⁰³

Representative Goodlatte reintroduced the SAFE Act in the 105th Congress as H.R. 695 and in the 106th Congress as H.R. 850.¹⁰⁴ The last attempt at passage occurred in 1999 when H.R. 850 had over 250 co-sponsors. Explaining why this encryption-liberalizing bill failed to reach a floor vote, despite a good economy and lowered national security and public safety concerns, remains a mystery to policymakers. My extensions to Allison's decision models may explain this event, its long-term policymaking effects, and a possible policy trajectory.

The terrorist attack on September 11, 2001 has elevated the tensions between actors supporting information access for national security and public safety purposes and actors

¹⁰³ *Congressional Record*, 104th Congress, 2nd sess., 1996, 142, pt. 28: H1715 and E276.

¹⁰⁴ *Congressional Record*, 105th Congress, 1st sess., 1997, 143, pt. 11: E245-E247.

Congressional Record, 106th Congress, 1st sess., 1999, 145, pt. 30: H814.

Congressional Record, 106th Congress, 1st sess., 1999, 145, pt. 31: E297.

supporting information security for economic and privacy purposes. In response to this attack, the 107th Congress passed the surveillance minded *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)*.¹⁰⁵ This law dramatically increases government surveillance powers allowed by *FISA*. The government can now target United States citizens, in addition to foreign agents, with electronic surveillance. Increased surveillance is likely to increase the use of encryption as a countermeasure. However, the *USA PATRIOT Act* does not restrict this anticipated use of encryption. My extensions to Allison's decision models may better explain why crisis action policymaking did not address this root problem.

In the international encryption policy area, the Organization for Economic Cooperation and Development (OECD) has a current policy document titled "Guidelines for Cryptography Policy." In this document, OECD lists a broad array of policy alternatives that range from government control to market control of encryption. What is missing from the OECD guidelines is a policy decision on an alternative that is agreeable to all parties.¹⁰⁶ This continuing failure to decide on encryption policy affects supra-national agreements such as the Wassenaar Arrangement that controls dual-use technologies. Wassenaar member countries have already eroded encryption controls on

¹⁰⁵ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, U.S. Statutes at Large*, 115 (2001): 272-402.

¹⁰⁶ Organization for Economic Cooperation and Development, Science, Industry and Technology Directorate, "Guidelines for Cryptography Policy", <
http://www.oecd.org/document/11/0,2340,en_2649_34255_1814731_1_1_1_1,00.html >, accessed April 2004.

the allowed strength of exportable encryption algorithms. Without a decision on allowable secret key encryption strength, competitive pressures have moved the official baseline from 56 bits to 64 bits and beyond. The unofficial baseline set by the globally available Advanced Encryption Standard is now an unbreakable 128 bits.

Without laws or regulations for mandatory key management, current encryption technology is not under control from the perspective of satisfying public safety and national security requirements. A metric of encryption technology control is the International Standards Organization's (ISO) list of approved encryption standards. The list is currently empty, as the ISO has avoided the politically charged area of encryption control by placing all submitted encryption standards in a holding registry. Foreign policy actors are waiting for the United States to show its leadership and to produce an encryption policy design with globally acceptable encryption standards.

Policymakers have a requirement to extend decision-making theory to handle hard technology policy problems. My extension of Allison's decision models may better explain the long-term actions of policy actors in the United States and may explain how these actions created a conglomerate encryption policy. My modifications to Allison's decision models take a short-term decision model and extend it to cover three decades of encryption policymaking. I have modified the Rational Actor Model to explain how the generation of alternatives produces group interactions required for policy decisions. I have modified the Organizational Behavior Model to explain how double-loop learning produces organizational adaptations that keep pace with encryption technology

advancements. I have modified the Governmental Politics Model to explain how specific individuals and groups from the three branches of government create policies based on balancing political power.

My research uses these modified models in a case study design to pattern-match the actions and decisions of groups of actors and engineering evidence against metrics derived from each model. Groups of policy actors provide the research breadth and three decades of evidence provide the required research depth. The next chapter presents the details on the research methodology.

Chapter Three: Methodology

Qualitative methods can answer research questions about policy designs by organizing and explaining the historical record of information and encryption control events and decisions. A qualitative approach also eliminates the requirement for an experimental design that isolates variables and controls for environmental influences, both of which are difficult tasks in a case study of policy actions. Another important factor supporting the choice to use a qualitative approach is that quantitative experiments tend to perturb the environment or context in which causal relationships occur. Research experts Denzin and Lincoln, editors of the *Handbook of Qualitative Research*, believe that the interactions of the observed variables and the “unreduced environment” contain the answers to qualitative research questions. Denzin and Lincoln highlight the different objectives of qualitative and quantitative research with the following statements:

“Qualitative researchers believe that rich descriptions of the social world are valuable ... Quantitative researchers are deliberately unconcerned with rich descriptions because such detail interrupts the process of developing generalizations.”¹⁰⁷ When properly accomplished, a qualitative methodology can characterize policy groups and can match events and decisions against the relationships suggested by theoretical models.

¹⁰⁷ Norman K. Denzin and Yvonna S. Lincoln, eds., *Handbook of Qualitative Research*, 2d ed. (Thousand Oaks, California: Sage Publications, 2000), 1-28.

Case Study Design

My research involves analyzing the relationships among groups of encryption actors over a three-decade time span. Although my research is largely qualitative, I still rely on quantitative constructions to help with the pattern matching tasks. Qualitative research experts Miles and Huberman call this combination a “qualitative-quantitative linkage” and believe that such linkages can improve the efficiency of a case study.¹⁰⁸ I use Robert K. Yin’s well-known case study research design as a framework to achieve these linkages. In his book *Case Study Research*, Yin suggests the following components of qualitative research design:

- Specifying research questions
- Producing propositions
- Creating and using analysis units
- Linking the data to the propositions
- Using criteria to interpret the findings¹⁰⁹

I have previously stated my descriptive and explanatory research questions. The next component of my research design is a set of propositions that will serve as theories of action to explain the relationships among events, actors, alternatives considered, and decisions. In 1969, Graham T. Allison proposed three decision models, each of which

¹⁰⁸ Mathew B. Miles, and A. Michael Huberman, *An Expanded Sourcebook: Qualitative Data Analysis* (Thousand Oaks, California: Sage Publications, 1994), 40-43.

¹⁰⁹ Robert K. Yin, *Case Study Research: Design and Methods*, 2d ed. (Thousand Oaks, California: Sage Publications, 1994), 1-17.

having a set of propositions.¹¹⁰ Allison's decision models are the Rational Actor Model, the Organizational Behavior Model, and the Governmental Politics Model. The latter two models account for influences that go beyond rational actor or utility maximizing logic by considering the behavior of organizations and the role of politics in influencing the decision-making process.¹¹¹

- The Rational Actor Model may dominate if policy actors can generate alternatives and rank these alternatives according to perceived cost and benefit information. Policymakers can then select the optimum solution, which becomes policy.
- The Organizational Behavior Model may dominate when organizations make decisions by following "standard operating procedures."¹¹² Different organizations may solve their own pieces of the problem and may efficiently choose solutions from their own lists of alternatives. In this case, environmental factors, organizational culture, and organizational learning considerations may influence actor groups to choose different solutions when facing the same problem.
- The Governmental Politics Model may dominate when "action channels" working for politically motivated leaders take policy actions based on

¹¹⁰ Graham T. Allison, "Conceptual Models and the Cuban Missile Crisis," *American Political Science Review* 63, no. 3 (September 1969): 689-718.

¹¹¹ Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* 2d ed. (New York: Longman, 1999), 13-75, 143-196 and 255-324.

¹¹² *Ibid.*, 143-196.

maintaining political power and supporting constituents.¹¹³ In this case, actors may see the favored solution as increasing their political power and not as selecting an optimum cost and benefit solution.

Corresponding to each of Allison's decision models, I created a proposition applicable to my encryption policy case study:

- Proposition 1. Unified actors determine encryption policy by choosing the optimum solution. If alternatives and cost and benefit information are available on the policy issue in question, then policymakers are more likely to follow the Rational Actor Model in making decisions.
- Proposition 2. Organizations and organizing processes produce actions that determine encryption policy. If technical expertise, authority, or past solutions are associated with particular organizations, then these organizations are more likely to follow the Organizational Behavior Model in making the next decision.
- Proposition 3. Actors who influence the balance of political power among the branches of government determine encryption policy. If an actual or perceived technology crisis occurs, then policymakers may compete for political leadership and are more likely to follow the Governmental Politics Model in making decisions.

¹¹³ *Ibid.*, 255-324.

I developed a fourth proposition to extend Allison's models to account for multi-year interactions between policy actors and their decisions:

- Proposition 4. Actor groups that experience failures are more likely to change decision models. In addition, actor groups that experience failures may change the decision-making environment through double-loop learning instead of adopting behaviors suggested by a single decision model.

I used these propositions as candidate hypotheses to organize and pattern-match the textual, graphical, and engineering data. This data was first collated according to analysis units, which serve as actor groups in my research.

Analysis Units and Data Handling

I aggregated individual policy actors into four groups to serve as my analysis units. In order to preserve these groups through the longitudinal aspect of my research, I maintained a consistent definition of each analysis unit through three analytical periods. An analysis unit is a group of encryption actors that have similar functions in developing encryption technology, are in the same branch of government, or share a similar philosophy on information and encryption control. Table 3-1 lists the four groups and their constituent policy actors. The Congressional Group creates the laws that govern information and encryption control policies. The Executive Group contains the president,

cabinet, and members in the Executive Office of the President. The Encryption Technology Group has actors from academia, electronic rights advocates, encryption vendors, professional organizations, and research and development entities. While the Executive Group establishes encryption policies and activities that satisfy federal government and international relations requirements, the Government Agencies Group contains the government organizations that develop, use, and regulate information and encryption technologies.

Table 3-1 also lists data associated with the actions of each analysis unit. Often data clusters around an encryption event, such as the development of a new form of encryption or a change in a regulatory policy regime. Data from important encryption events, such as the federal government's development of the Data Encryption Standard, often supported analyses for several groups. Because the selection of encryption events acts as a data filter that introduces data bias, I used important encryption events covered by the news media, newspapers, common magazines, and books as flags for analysis candidates. Popular coverage of an encryption event created an unbiased significance threshold for important encryption technology advancements and ensuing policy issues, while filtering less significant events that did not have policy implications and would have encumber my analysis.

Table 3-1 List of Groups, Actors, and Data Sources

Analysis Unit	Policy Actors in the Unit	Types of Data
Congressional Group	Congressional Research Service Office of Technology Assessment House Committees Senate Committees Sponsors of legislation	Committee reports Enacted legislation Proposed legislation Public statements Studies
Encryption Technology Group	Association for Computing Machinery American National Standards Institute Center for Democracy and Technology, Electronic Frontier Foundation, and Electronic Privacy Information Center Institute for Electrical and Electronic Engineers IBM, Network Associates, RSA Security and VeriSign MIT and Stanford University	Activism Court cases Magazines and newspapers Market strategies Patents Policy recommendations Publications Official testimony Reports and studies Standards
Executive Group	Attorney General Office of Management and Budget Secretary of Commerce Secretary of Defense Secretary of State Secretary of the Treasury	Agreements Executive orders Policy directives Policy statements Vetoes
Government Agencies Group	Bureau of Industry and Security National Institute of Standards and Technology National Security Agency	Publications Policy statements Regulations Standards

Pattern Matching

The process of examining and characterizing the actions of each analysis unit and exploring the relationships among analysis units is a procedure Yin calls “pattern

matching.” According to Yin, pattern matching is the most difficult part of the case study.¹¹⁴ I accomplished pattern matching by using standardized criteria to relate the actions of each analysis unit to my propositions. Earlier, I developed propositions based on Allison’s decision models. Next, I will develop four criteria or valances that will be used to examine and characterize actions. My “Lead Actor” and “Problem Perception” valances are closely related to Allison’s “Organizing Concepts” category that he used to describe the actors and the nature of the problem. These two valances also answer who and what questions, respectively. My “Favored Alternative” (solutions) and “Decision Timing” valances are closely related to Allison’s “General Propositions” category that he used to describe the outputs of decision processes.¹¹⁵ These two valances answer how and when questions.

A. Lead Actor – Who

The first criterion is the perception of a lead actor that will transform the condition associated with information security of digital data into a problem with possible statutory or technology solutions. Often lead actors will self-emerge in accordance with their power, expertise, or function within their respective institutions or organizations. Some lead actors may arise sequentially to fulfill their functions when called upon. Other lead actors may arise in parallel to compete for ownership of the problem.

¹¹⁴ Yin, *Case Study Research*, 20-27.

¹¹⁵ Allison and Zelikow, *Essence of Decision*, 13-75, 143-196 and 255-324.

- I assign a valance of two for groups that favor the government as the lead actor. The government is more likely to be the lead actor when a new technology, such as encryption, jeopardizes national security and public safety or when there is a lack of economic incentive in the private sector to find a solution. A group of actors may follow the Governmental Politics Model because they believe that government intervention is required to mitigate the negative externalities posed by market control of encryption technology.
- I assign a valance of one for groups that specify a consortium of government sector, private sector, or international organizations as lead actors. In this situation, government and private sector actors work together as co-equals in developing a solution that can be adopted by international actors. Tighter cooperation occurs when each partner contributes political leadership and technological knowledge in owning the problem and shares management, fiscal, and resource burdens for the solution. A group of actors may follow the Organizational Behavior Model because the development and implementation of an encryption solution requires voluntary cooperation among organizations in the government and private sectors.
- I assign a valance of zero for groups that specify the private sector as the lead actor. Compared to the government sector, the private sector may be better at creating solutions that are responsive to market forces. In accordance with the idea of rational action, the market will determine costs and benefits of information access and information security requirements. Competitive actors

from all sectors can develop encryption alternatives, but the private sector has technological expertise, timing, marketing skill, and trust advantages preferred by consumers. A group of actors may follow the Rational Actor Model because they believe that rational choices and market forces should have full control over encryption technology.

B. Problem Perception - What

The second criterion is the perception of the problem. The general problem is balancing information access and security requirements for digital data through controlled encryption use. Actor groups may solve the whole problem at once or parts of the problem as solutions become available. The scope of the perceived problem often determines the strategy used to solve the problem and directs the order in which pieces of the problem are solved.

- I assign a valance of two for groups that perceive a complex problem with international and domestic policy dimensions and with interrelated economic, national security, public safety, and technology leadership issues. Often complex problems require political orchestration of many disparate actors to reach a policy decision. The results of such a decision may appear sub-optimal to a rational actor and may appear too complicated for implementation by specialized organizations. A group of actors may follow the Governmental Politics Model because they believe that only their group has the power to handle the tasks of making rational decisions, reacting to

market forces, controlling organizational behaviors, and satisfying political agendas.

- I assign a valance of one for groups that perceive a composite problem requiring segmented solutions. A composite problem can be divided into smaller problems that match the power, jurisdiction, resources, or technical expertise of the participating groups. Actors often divide problems into international or domestic dimensions and according to economic, security, or technology leadership objectives. A group of actors may follow the Organizational Behavior Model because their perceptions on their pieces of the problem match their organizational cultures and organizing capabilities.
- I assign a valance of zero for groups that perceive a simple problem with a solution directed by rational economic considerations. A simple problem involves the narrow consideration of technical or quantitative factors and the development of several alternatives in the search for the optimum solution. A group of actors may follow the Rational Actor Model because they perceive that solving the information access and security problem is a utility maximizing exercise.

C. Favored Alternative - How

The third criterion is the policy actor group's favored alternative or solution. Some policy actor groups may be open to alternatives that affect both the information access

and security problems, while other groups may favor alternatives biased toward particular aspects of these problems.

- I assign a valance of two for groups favoring alternatives such as new laws and regulations that balance information access and security requirements in a consensual manner. Cooperation between the executive and legislative branches is required because new laws and regulations often affect international partners, domestic constituents, and the balance of political power. A group of actors may follow the Governmental Politics Model because they believe that the development of laws and regulations, which satisfy privacy, economic, national security, and public safety requirements, is inherently a political process.
- I assign a valance of one for groups favoring alternatives adapted from past precedents, routines, and standards to satisfy pending information access and security problems. A group of actors may follow the Organizational Behavior Model because they believe that following past precedents, organizational processes, and routines are effective in quickly solving difficult problems with privacy, economic, national security, and public safety aspects.
- I assign a valance of zero for groups favoring alternatives that satisfy information access and security problems through utility maximizing mechanisms such as the use of the market, the development of alternatives that allow choice, and the reinforcement of trust in technology leaders. Markets are generally responsive to rational consumer actions, and encryption

technology developers will create various products to satisfy consumer demands and to maintain consumer trust. Trust in a technology leader allows users to accept alternatives based on the reputation of the developer, as indicated by market share and popular beliefs. The government is also capable of making utility maximizing decisions by developing information control alternatives and allowing users to make choices. A group of actors may follow the Rational Actor Model because they believe that the acts of developing alternatives and making informed choices are the primary components of making decisions.

D. Decision Timing - When

The fourth criterion is the decision timing perceived by the policy actor groups. Decision timing can be overt by following a specific crisis resolution timeline or can be incremental and tacit by allowing actors to decide on their own and in the background. Often in the technology policy realm, the decision timing cannot be forced and thus, depends on the emergence of solutions suitable for competition in the market.

- I assign a valance of two for groups that perceive the need for an immediate decision to solve the information access and security problem. Often an escalating problem forces crisis response activities that solve the problem and gain political power for the lead actor. Once a crisis is solved, political power is enhanced and subsequent crisis response activities usually follow. A group of actors may follow the Governmental Politics Model because they believe

that the government will be the first to experience all the facets of the information control problem and that inaction will demonstrate leadership and political weaknesses.

- I assign a valance of one for groups that perceive the requirement for incremental or tacit decisions on an evolving problem that politicians and the market are unable to solve alone. A group of actors may follow the Organizational Behavior Model because they believe that organizations with technical expertise and resources can make adequate progress by solving pieces of the information control problem.
- I assign a valance of zero for groups that will wait for the production of alternatives before making a decision. A group of actors may follow the Rational Actor Model because they believe that waiting for the development of alternatives reduces suboptimal and sometimes irrational choices caused by organizational behaviors and political influences on the policymaking process. These actors also believe that consumers and users are the best judges of when alternatives are ready and the value of each alternative.

The demonstration of valance changes from one analytical period to the next may be important in determining the long-term decision-making pattern of a particular group. Although actor groups may find it comfortable to follow their past or preferred decision patterns, a long-term tendency may exist for actor groups to learn through feedback mechanisms, such as single or double-loop learning, and to change their decision behaviors. Actor groups that are more effective in making policies may converge on a

common decision model. One possible reason for convergence is that actor groups are copying successful behaviors of other actor groups. Another possible reason is that they are exhibiting learned behaviors, which are complementary to other groups sharing the same decision model or a common mix of decision model valances. In contrast, actor groups that exhibit divergent decision model valances may be less effective in policymaking because they cannot share their leadership and resource burdens with other actor groups or may not be able to gain the trust of other actor groups. Table 3-2 summarizes the criteria, their assigned valances and supported decision model.

Table 3-2 Criteria and Valances

Criteria	Valances	Suggested Allison Model
Lead Actor	2 = government sector 1 = consortium 0 = private sector	<ul style="list-style-type: none"> • GPM • OBM • RAM
Problem Perception	2 = complex problem 1 = composite problem 0 = simple problem	<ul style="list-style-type: none"> • GPM • OBM • RAM
Favored Alternative	2 = new laws and regulations 1 = past precedents / routines 0 = utility maximizing	<ul style="list-style-type: none"> • GPM • OBM • RAM
Decision Timing	2 = urgent / crisis 1 = incremental / tacit 0 = contingent on choices	<ul style="list-style-type: none"> • GPM • OBM • RAM

Research Displays

I will use research displays to present the valances of each group over three analytical periods. Displaying valances over time may reveal decision-making patterns and may indicate convergence toward or divergence from preferred decision-making models. According to Miles and Huberman, data displays are normally presented in a matrix or a network style.¹¹⁶ I will use a matrix style for the presentation of findings within an analytical period and will use a network style for the presentation of findings across the three analytical periods.

My development of analytical periods was dependent upon encryption events to demarcate each period. For the First Mover Period, 1973-1986, I used the open development of secret key and public key encryption technologies as the start of the period. In this period, the government and private sectors saw the development of encryption technology as the solution to the digital information protection problem caused by the growing numbers of computers in use. Congress passed the *Privacy Act of 1974* during this period, and this act served as a motivator for encryption development.

For the Competitive Period, 1987-1997, I used the passage of the *Computer Security Act of 1987* as the start of the period. In this period, Congress passed laws to protect the security of data stored on computers and to allow limited government access to data for national security and public safety reasons. The executive branch had its own

¹¹⁶ Miles and Huberman, *Qualitative Data Analysis*, 90-171.

competitive method for information technology control, which did not agree with Congress. Competition also allowed the private sector to develop solutions to the information security problem with little domestic interference from the government. The government did try to control the international aspects of encryption technology, and this period saw the proliferation of encryption regulations and standards and the collapse of the government championed escrowed-key encryption scheme.

For the Status Quo Period, 1998-2004, I used the passage of the *Digital Millennium Copyright Act* as the start of the period. In this period, Congress passed laws to protect the economic value of information on a global scale, but failed to pass legislation choosing between encryption freedom and government access to data. This period saw the prevention of information warfare attacks as the prime motivator for satisfying information security requirements. Satisfying information access requirements was relegated to the policy background. Table 3-3 contains the three analytical periods, the encryption events that demarcate each period, and a description of each period. I will use these three analytical periods to segment my longitudinal analysis and to highlight trends in decision behaviors.

Table 3-3 Analytical Periods

Period	Demarcation and Events	Description
First Mover, 1973-1986	Development of digital data encryption. Passage of the <i>Privacy Act of 1974</i>	Period covers the initial development and uses of secret and public key encryption
Competitive, 1987-1997	Passage of the <i>Computer Security Act of 1987</i> . Proliferation of personal computers and the Internet. Failure of government escrowed encryption.	Period covers the proliferation of encryption regulations and the competitive use of voluntary and involuntary standards to control encryption. Period also covers the rise of electronic rights advocates.
Status Quo, 1998-2004	Passage of the <i>Digital Millennium Copyright Act</i> . The globalization of information and national security threats.	Period covers a stable agreement on the importance of satisfying information security requirements that help national security, public safety, economic, and privacy issues. Satisfying information access requirements remains in the background.

Chapter Four: Data and Results

I used textual, graphical, and engineering data to explain the actions of four analysis units, each corresponding to a group of actors. These four groups provided the analytical breadth for my research, and I used the First Mover, Competitive, and Status Quo Periods to provide longitudinal depth. In each of these three periods, I used encryption events to focus my investigation on the substantive activities of the four groups and to reduce extraneous data. My analysis starts with a First Mover Period demarcated by a seminal 1973 magazine article on encryption.

First Mover Period: 1973-1986

The First Mover Period spans fourteen years and starts in 1973 when a popular magazine article alerted the public to the dangers presented by the misuse of digital information and suggested an encryption solution. During this period, actors in the private and government sectors sought technical solutions to protect digital information from theft, adulteration, and exploitation. Also in this period, the requirement to protect digital information coincided with a maturing political agenda to protect privacy rights. Two emergent technologies capable of protecting digital information were secret key encryption and public key encryption. Development and policy control of these two encryption technologies during this period primarily involved the activities of the four

actor groups. I selected encryption events to focus my analysis by examining contemporary magazines and books published during the First Mover Period.

Secret key encryption made its public appearance in 1973 when *Scientific American* carried a digital information protection article by renowned cryptographer Horst Feistel. Feistel was an IBM engineer working on a solution to “the privacy problem presented by modern computers.”¹¹⁷ Feistel’s proposed solution was to use secret key encryption to protect digital information. Feistel’s article marked an important encryption event by suggesting the use of a technology previously unavailable to the private sector and to most of the non-defense government sector. In the ensuing years, the National Bureau of Standards incorporated IBM’s solution into a first ever government Data Encryption Standard (DES). Feistel’s article suggested that private sector technology actors and government agencies were important contributors to encryption development and nascent encryption policy.

In 1977, a *Scientific American* column introduced the mathematics behind public key encryption to a broad audience. Before this time, only the engineering, mathematics, and national security communities knew about public key encryption. Martin Gardner, who wrote the Mathematical Games column for *Scientific American*, challenged his readers to solve a mathematical contest. Gardner dramatically titled his column “A new kind of cipher that would take millions of years to break.” Gardner asked researchers at the Massachusetts Institute of Technology (MIT) to create a secret message using a 129-

¹¹⁷ Horst Feistel, “Cryptography and Data Security,” *Scientific American* 228, no. 5 (May 1973): 15.

digit number as the source of the two encryption keys used for a public key encryption scheme.¹¹⁸ These MIT researchers were Ronald L. Rivest, Adi Shamir, and Leonard Adleman and were the developers of the now popular RSA public key encryption algorithm. In his column, Gardner showed the importance of the private sector in taking actions that influenced encryption policy.

Investigative author James Bamford published his famous book about the National Security Agency in 1982. In *The Puzzle Palace*, Bamford explored the secretive activities of the NSA, much to the chagrin of the intelligence and defense communities.¹¹⁹ Bamford described the friction between the legislative and executive branches as these actors championed opposing goals of protecting privacy rights and providing access to information for national security and public safety purposes. In analyzing the passage of the *Foreign Intelligence Surveillance Act of 1978 (FISA)* by Congress, Bamford found that executive branch actions leaned toward assuming broad national security powers to collect intelligence and congressional actions leaned toward limiting the surveillance of Americans and protecting the right to privacy.¹²⁰ Since encryption can both hurt national security by negating *FISA* activities and help protect

¹¹⁸ Martin Gardner, *Mathematical Games*, "A New Kind of Cipher That Would Take Millions of Years to Break," *Scientific American* 237, no. 8 (August 1977): 120.

¹¹⁹ From personal experience in 1982, military members working at NSA or supporting NSA's field activities were discouraged from buying, reading, or discussing the book. Although Draconian sounding, there was merit in discounting his book, as active lunchroom debates by NSA insiders could be used to confirm Bamford's propositions. Informants did monitor conversations. In 1984, USAF Electronic Security Command officials questioned me about a fellow officer overheard making statements that cast doubt on his suitability to hold a security clearance.

¹²⁰ Bamford, *The Puzzle Place*, 367-379.

privacy rights, I analyzed the actions of the legislative and executive branches with respect to balancing national security and privacy requirements.

I ended the coverage of the First Mover Period in 1986, as the passage of the *Computer Security Act of 1987* started a new period where actors vigorously competed to specify policies on the control of encryption technology.

Congressional Group

In the First Mover Period, the primary actor in the Congressional Group was Congress as a whole in passing the *Privacy Act of 1974*, the *Arms Export Control Act* as amended in 1976, the *Foreign Intelligence Surveillance Act of 1978*, and the *Export Administration Act of 1979*. These laws directly limited the power of the executive branch and indirectly constrained the domestic and global uses of encryption technology. Another active member of the Congressional Group during this period was the Senate Select Committee on Intelligence as it questioned the roles of the National Bureau of Standards (NBS) and the National Security Agency in developing the Data Encryption Standard. The text of these laws just mentioned, the *Congressional Record*, and committee reports provided the data for analyzing the actions of the Congressional Group in shaping encryption policy. I analyzed this data according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

Actors in the Congressional Group believed that the legislative branch of government was the lead actor in the effort to protect privacy, while satisfying public safety and national security requirements. This group realized that the government itself was a major threat to the privacy of digital data and believed that the private sector would face a similar problem with corporations threatening the privacy of individuals. During the Senate debate on S. 3418, which became the *Privacy Act of 1974*, bill cosponsor Senator Charles H. Percy (R-Illinois) discussed two threats to privacy:

I hope we never see the day when a bureaucrat in Washington D.C. or Chicago or Los Angeles can use his organization's computer facilities to assemble a complete dossier of all known information about an individual. But, I fear this is the trend. Many of our Federal agencies have become omnivorous fact collectors—gathering, combining, using, and trading information about persons without regard for his or her rights of privacy. Simultaneously, numerous private institutions have also amassed huge files and information retrieval systems containing millions of files of unprotected information on millions of Americans. Our ability as individuals to control access to personal information about us has all but completely faded.¹²¹

In the text, Senator Percy identified the threats to privacy as bureaucrats in government agencies and unprotected digital data in the private sector. At the time, a major part of the privacy protection problem was internal to the federal government, and actors in the Congressional Group saw themselves as being the leaders of a governmental reform movement. While the executive branch was the target of government sector privacy reform, Congress also intended to protect information privacy in the private sector.

¹²¹ *Congressional Record*, 93rd Congress, 2d sess., 1974, 120, pt. 27: 36894.

Bill cosponsor Senator Edmund S. Muskie (D-Maine) noted the importance of Congress' actions in protecting privacy and claimed, "Many observers have characterized the 93rd Congress as the 'Privacy Congress.'" Senator Muskie went on to claim that Congress had the leading role within government: "While the courts have begun to recognize the capacity of the Government to invade individual privacy by the gathering and misuse of information, it is the responsibility of Congress to develop specific legislation in this area."¹²²

Congress also took the lead in protecting privacy information in the private sector with the creation of a Privacy Protection Commission to study the problem:

In considering this legislation it was understood that the privacy considerations do not stop at the Federal Government. Our concern for the handling of information about individuals extends beyond Federal agencies to State and local government and to the private sector.¹²³

Congress did not have the required consensus to pass legislation to solve the problem in the private sector. However, the Privacy Protection Commission produced findings that supported subsequent privacy laws on medical records and certain financial information. In addition to taking the lead in protecting privacy in both sectors, actors in the Congressional Group believed that the government needed to ensure access to information for national security and public safety requirements.

¹²² *Congressional Record*, 93rd Congress, 2d sess., 1974, 120, pt. 27: 36896.

¹²³ *Ibid.*, 36897.

The domestic and international availability of privacy tools, such as encryption, forced governmental action to protect national security and public safety without jeopardizing the right to privacy and the economic health of American information technology industries. Not trusting the power and decisions of the executive branch, Congress took action by passing the *Arms Export Control Act* in 1976 and the *Export Administration Act of 1979*. Actors in the Congressional Group thought it reasonable to use complicated sets of laws and regulations as control mechanisms over the executive branch, international actors, domestic industries, and private citizens.

Congress attempted to gain control of exports that had national security implications through the passage of H.R. 13680, the *Arms Export Control Act*. This act specified a “United States Munitions List” that regulated “the import and export of defense articles and defense services” and provided “foreign policy guidance to persons of the United States involved in the import and export of such articles and services.”¹²⁴ The Munitions List explicitly regulated encryption technology imported and exported by both the government and private sectors. More subtly, the Munitions List controlled the encryption technology available to persons in the United States. During the debate on H.R. 13680, bill sponsor Representative Thomas E. Morgan (D-Pennsylvania) made it clear that the intent of Congress was to wrest some control from the executive branch:

¹²⁴ *Arms Export Control Act, U.S. Statutes at Large* 90 (1976): 744.

Mr. Chairman, this bill, H.R. 13680, like its predecessor, S. 2662 which was vetoed on May 7, represents a historic initiative by the Congress to take a more active role in the field of military sales and security assistance.¹²⁵

Since the Munitions List contained items that were not munitions, such as encryption technology, Congress received protests from domestic industries desiring more export business and from privacy rights advocates fearing government restrictions.

Actors in the Congressional Group were unwilling to allow substantial private sector or executive branch control of dual-use technologies and passed the *Export Administration Act of 1979*. Congress required that the Secretaries of Commerce and Defense use a published Commerce Control List (CCL) to specify technology items requiring export licenses.¹²⁶ During the debate on S. 737, which would become the *Export Administration Act of 1979*, bill sponsor Senator Adlai E. Stevenson III (D-Illinois) stated Congress' policy intent:

Mr. President, S. 737 would establish an export control policy which protects vital security and foreign policy interests without unnecessarily restricting U.S. exports. It would reduce the number of controlled items and focus national security controls on technologies and related products critical to military systems. It would set the criteria the President must consider before imposing export controls for foreign policy purposes.¹²⁷

The text shows that Congress viewed itself as the lead actor in balancing national security requirements against the economic value of exports. The executive branch was to follow

¹²⁵ *Congressional Record*, 94th Congress, 2d sess., 1976, 122, pt. 12: 14434.

¹²⁶ *Export Administration Act of 1979, U.S. Statutes at Large* 93 (1979): 506-510.

¹²⁷ *Congressional Record*, 96th Congress, 1st sess., 1979, 125, pt. 16: 19936.

the policy set by Congress. The Congressional Group also took the lead in curtailing executive power in the domestic national security area.

Congress passed the *Foreign Intelligence Surveillance Act of 1978* to ensure national security, to protect privacy rights, and to limit executive power. Government abuses of power during the Watergate Era complicated legislation in that the trust relationships among the branches of government now needed explicit specifications. During the debate of S. 1566, which became the *Foreign Intelligence Surveillance Act of 1978*, freshman Senator Malcolm Wallop (R-Wyoming) noted the ability of Congress to specify these relationships among the branches of government, but questioned the wisdom of doing so:

Mr. President, the interesting thing is that it was not the courts but Congress who discovered the abuses of the recent past, and who brought them to the attention of the courts. Perhaps it would be a wiser choice for us to take that direction, rather than to intricately intermesh the three separate branches of our Government. When one does that one makes it impossible for one branch to render a real judgment on the other. Should all branches of government be involved in a decision the time could come when injured persons would have no one left to appeal to.¹²⁸

Congress did not listen and involved the judicial branch in controlling the executive branch, but did listen to Senator Wallop in extending congressional oversight into the national security and intelligence areas. If the executive branch were to bend the legal bounds of privacy rights in order to enhance national security, then the legislative branch would closely examine this activity.

¹²⁸ *Congressional Record*, 95th Congress, 2d sess., 1978, 124, pt. 9: 10896.

In 1979, Congress used its oversight powers to investigate the involvement of the executive branch in tampering with encryption technology used by the government and private sectors. Such tampering may have sacrificed privacy rights in favor of enhancing government surveillance capabilities. The Senate Select Committee on Intelligence produced an unclassified summary of its findings and recommended that the “appropriate committees of Congress should address the question of public cryptography by clarifying the role which the Federal Government should have in policies affecting public cryptography.”¹²⁹ This text supports the claim that Congress; in addition to developing multiple and contentious laws to balance national security, privacy, and export policies; now had to oversee federal department policies on encryption technology that could upset this balance.

The view of the government as the lead actor by the Congressional Group matched Allison’s GPM organizing concept of “Players in Positions.”¹³⁰ The players were legislators who debated multiple legislations required to solve economic, national security, and privacy problems. Legislators in various power positions from freshmen to senior bill sponsors used their powers to solve these problems, to increase Congress’ power over the executive branch, and to further their own political agendas. I therefore assigned a Lead Actor valance of “2” to the Congressional Group for being the

¹²⁹ Senate Select Committee on Intelligence, *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard*, Staff Report, 95th Congress, 2d sess., 1978, Committee Print, 4.

¹³⁰ Allison and Zelikow, *Essence of Decision*, 298.

government lead in solving the digital information protection and encryption control problems.

B. Problem Perception Valance

Actors in the Congressional Group perceived the digital information protection issue as a complex problem with divergent congressional and executive branch views and with international ramifications. Congress used new and amended laws to protect privacy and to limit national security and public safety problems caused by expanded privacy rights. In passing the *Privacy Act of 1974*, actors in this group found that there was a significant threat posed by digital data and that there was a constitutional requirement for protecting privacy:

SEC. 2. (a) The Congress finds that –

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the

Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.¹³¹

The text shows that Congress perceived a domestic threat to privacy caused by the “use of computers and sophisticated information technology” in the federal government. This law implied that the federal government, in performing its daily activities, was a potential threat to privacy. Thus, congressional efforts would first focus on the federal government and then the private sector with future legislation.

A debate captured in the *Congressional Record* revealed the complexity of the digital information protection problem and the perceptions of Congress in solving this problem. Senator Sam J. Ervin Jr. (D-North Carolina) sponsored S. 3418 that would become the *Privacy Act of 1974*. During the debate, Senator Ervin claimed that Congress could overcome this complex problem:

Mr. Philip Buchen testified before the committee on behalf of the White House Domestic Council on privacy. The burden of his testimony was that the problems of privacy and confidentiality are so varied and complex that they are beyond the legislative capabilities of Congress to address in a comprehensive bill imposing similar standards on all agencies.

I disagree with those who hold this view. I believe the need has been demonstrated for a rule of law concerning the technology, policies, and practices of Government which affect the freedoms of Americans.¹³²

The text shows that the administration did not believe that Congress could solve a complex social and technical problem by a “rule of law.” Congress passed S. 3418, but

¹³¹ *Privacy Act of 1974, U.S. Statutes at Large* 88 (1974): 1896.

¹³² *Congressional Record*, 93rd Congress, 2d sess., 1974, 120, pt. 27: 36892.

the complex problem required several additional laws to address national security and public safety concerns that resulted from the implementation of the *Privacy Act of 1974*.

One product of the *Privacy Act of 1974* was the federal government's development of digital encryption. However, this development soon required Congress to create control mechanisms for this new technology. The Computer Security Guidelines for Implementing the Privacy Act of 1974, FIPS PUB 41, documented the domestic uses of data encryption in the federal government.¹³³ Congress used H.R. 13680, which would become the 1976 *Arms Export Control Act*, and the *Export Administration Act of 1979* to control the complex problem posed by the international flows of dual-use technologies such as encryption. In the debate on H.R. 13680, Congress reaffirmed the use of a Munitions List that federal agencies would use to restrict the export of dual-use technology.¹³⁴ Congress also debated the value of a keeping a legislative veto in H.R. 13680 to challenge the decisions of the executive branch. President Gerald R. Ford rejected a prior bill containing a legislative veto, but Congress was adamant in retaining some level of post-legislative control over arms exports:

The legislation vetoed by the President contained seven provisions which would have given the Congress the authority to veto executive actions by passage of a concurrent resolution which does not require Presidential signature. The bill reported today drops five of these provisions.¹³⁵

¹³³ U.S. Department of Commerce, National Bureau of Standards, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Federal Information Processing Standards Publication 41 (Washington, D.C.: GPO, 30 May 1975), 19.

¹³⁴ *Congressional Record*, 94th Congress, 2d sess., 1976, 122, pt. 13: 16203.

¹³⁵ *Congressional Record*, 94th Congress, 2d sess., 1976, 122, pt. 12: 14434.

Congress also created export liberalization laws that were in contention with export controls. Congress faced the difficult problem of limiting the exports of dual-use technology products while ensuring the global competitiveness of American information technology industries.

Congressional debate of S. 737, which became the *Export Administration Act of 1979*, revealed the complexities in controlling the export of dual-use technology. During the debate, Senator John Heinz (R-Pennsylvania) described the difficult, often paradoxical, problem of restricting technology exports to protect national security:

That may be the simplest way to illustrate what I mean and what we mean when we say the rate of change of society and of technology in particular, is increasing. It is increasing at a rate that is going to get larger and larger. So, every time we try to protect ourselves, every time we forget that we are a maritime nation in the historic sense, every time we draw barriers between ourselves and the rest of the world or between ourselves and each other in technological ways and economical ways, all we are doing is acting to our own disservice. We are restricting the rate at which we can grow, where as the rest of the world is growing at this ever-increasing rate.¹³⁶

A critical and logical prerequisite for an export control law or regulation was that the technology in question should not be readily available in foreign markets. The concept of “foreign availability” was a unique approach to this problem. Under this concept, the United States would have to work in unison with other governments to restrict jointly the exports of the technology in question.¹³⁷ Adding to this complexity was the “ideas and processes” case where a technology, such as an encryption algorithm, did not have a

¹³⁶ *Congressional Record*, 96th Congress, 1st sess., 1979, 125, pt. 16: S19964.

¹³⁷ *Congressional Record*, 96th Congress, 1st sess., 1979, 125, pt. 16: S19937.

physical form to control. Once released or leaked, encryption algorithms would become globally available, and a logical application of the foreign availability rule would preclude encryption control. However, national security and public safety concerns were powerful enough to perpetuate encryption control idiosyncrasies in the *Export Administration Act of 1979*, even to the extreme of placing restrictions on technology that the federal government had already made available to the world. Power politics behind national security and public safety concerns also challenged parts of the *Privacy Act of 1974*.

The debate surrounding S. 1566, which would become the *Foreign Intelligence Surveillance Act of 1978 (FISA)*, revealed the complexities of attempting a re-balance of power among the branches of government and between national security requirements and privacy rights. During the debate, a statement attributed to Senator Edward Kennedy (D-Massachusetts) by Senator Paul G. Hatfield (D-Montana) succinctly summarized the complexity of the problem:

The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens. My objective over the past six years has been to reach some kind of fair balance that will protect the security of the United States without infringing on our citizen's human liberties and rights.¹³⁸

¹³⁸ *Congressional Record*, 95th Congress, 1st sess., 1978, 124, pt. 9: 10902.

The Senate devoted a large part of their debate to discussing the involvement of the judicial branch, in the form of a FISA Court, to assist with the “fair balance” mentioned by Senator Kennedy. A provision relevant to protecting American citizens against foreign surveillance from agents operating within the boundaries of the United States was not included in *Foreign Intelligence Surveillance Act of 1978*.

Encryption technology, though not mentioned in the debate of S. 1566, could have protected American citizens and corporations against foreign surveillance. However, this protection would have added great complexity to S. 1566 and would have upset the compromises made between national security requirements and privacy rights. In weighing the magnitude of the surveillance threat against Americans, some members of Congress saw the United States government as a threat bigger than the one posed by foreign governments. However, Senator Daniel Patrick Moynihan (D-New York) pointed out in the debate that this perception might be wrong and that spying does threaten citizens:

Accordingly, Mr. President, I should like to call further attention to this problem of the intrusion by foreign intelligence agencies in the private communications of American citizens. So far as one can tell, this is of an incomparably greater order of magnitude than anything every contemplated, much less actually carried out, by American intelligence agencies.¹³⁹

Senator Moynihan’s observation uncovered a deep complexity in the problem of balancing national security requirements against privacy rights. An information

¹³⁹ *Congressional Record*, 95th Congress, 1st sess., 1978, 124, pt. 9: 10893.

protection law may have been more effective than a counter-intelligence law designed to catch spies. Protecting the privacy of communications would reduce the foreign surveillance threat and improve our national security. Congress did not add this provision to the *Foreign Intelligence Surveillance Act of 1978* nor did Congress pass a separate bill to use technology to protect privacy. These actions bolstered the suspicions by some members of Congress that domestic surveillance was politically more important than the protection of privacy.

The view of a complex problem by the Congressional Group matched Allison's GPM organizing concept of "Parochial Priorities and Perceptions" where the political positions of decision makers and the games they played in past legislation influence their current perceptions.¹⁴⁰ Successive legislations to protect privacy and to control encryption stemmed from complex interactions of international and domestic interests and the development of solutions acceptable to Congress. I therefore assigned a Problem Perception valance of "2" to the Congressional Group for perceiving a complex problem.

C. Favored Alternative Valance

The Congressional Group realized early on that it took laws to protect privacy, maintain access to information for national security and public safety purposes, and control encryption technology used to protect privacy. Senator Sam J. Ervin Jr., who sponsored the *Privacy Act of 1974*, likened his proposed legislation to the Bill of Rights:

¹⁴⁰ Allison and Zelikow, *Essence of Decision*, 298.

This bill provides an information bill of rights for the citizen and a code of fair information practice for the departments and agencies of the executive branch. There have been many bills introduced to protect the privacy of certain groups of citizens. S. 3418 is legislation aimed at protecting the privacy of all Americans, whenever the Federal Government collects, keeps, or uses personal information from or about them.¹⁴¹

The text indicates that Congress viewed privacy rights as a matter of information protection from the “departments and agencies of the executive branch.” Executive branch excesses of the Watergate Era fueled a congressional debate that considered legislative solutions to manage the federal departments more closely. Several members of the Senate proposed a joint oversight committee with powers to examine “whether the Government is complying fully with the law.”¹⁴² In the areas of privacy abuses and executive branch excesses, Congress used legislation to curtail executive power in regulating the export of “munitions” such as encryption devices.

Congress used the renewal of two laws to engage the federal departments in the complex tasks of limiting exports, while not hurting domestic industries, and to force more openness from the executive branch, while not violating the Constitution. In the House debate on the *Arms Export Control Act*, Representative Charles W. Whalen Jr. (R-Ohio) cited the responsibility of Congress to renew laws:

Congress must enact the provision of this legislation in order to carry out its responsibilities and to prod the administration into providing the American people with a fuller explanation of the basis and rationale for our expanding arms sales program. Arms sales have important foreign policy, national security and arms

¹⁴¹ *Congressional Record*, 93rd Congress, 2nd sess., 1974, 120, pt. 27: 36891.

¹⁴² *Ibid.*, 36901.

control implications and should be monitored in a coherent fashion by the U.S. Government. The bill before us today will help give overall direction to administration policy and provide a general framework within which individual priorities can be more clearly determined.¹⁴³

Explicit in Representative Whalen's commentary was the intent of Congress to "give overall direction to administration policy." One way for Congress to challenge executive branch decisions was to specify in legislation how Congress wished to solve the operational problems of the federal departments.

Congress used the 1979 renewal of the *Export Administration Act of 1969* to debate the precise meaning of terms such as "critical technologies" in order to pass a detailed law on export controls. During the debate, Congress uncovered a reason why the Departments of Commerce, Defense, and State were unable to work together to control technology exports.

The reference to military systems also ignores an important change that has occurred in U.S. military technology. For many years the military provided the cutting edge of the development of new technologies. Funds for military research and development were used extensively to push outwards the frontiers of commercial scientific technological innovation. However, all of that has been significantly reversed. Now new technology is developed with commercial applications in mind. Indeed, the integration of sophisticated technology into military systems now lags behind the use of high technology in consumer goods and industrial products....

It is important that the statutory framework for our modern export control policy makes it crystal clear the dual civilian/military uses of critical technologies.¹⁴⁴

¹⁴³ *Congressional Record*, 94th Congress, 2nd sess., 1976, 122, pt. 12: 14437.

¹⁴⁴ *Congressional Record*, 96th Congress, 1st sess., 1979, 125, pt. 15: 19961.

Congress viewed Senator Henry M. Jackson's (D-Washington) call for a "statutory framework" on dual-use technology as a solution more desirable than the myriad of departmental policies and decisions that previously controlled technology exports. Congress incorporated this legal framework into the *Export Administration Act of 1979* by requiring the Secretary of Commerce to publish a Commerce Control List that explicitly specified the controlled dual-use technologies.¹⁴⁵ While the responsibility for creating this list was clear, Congress did not provide a clear scheme for the executive branch to decide upon which commercial technologies, such as encryption, had military significance. The lack of policy direction resulted in an explicit Commerce Control List that contained contentious and debatable items.

In the area of privacy rights, Congress provided the executive branch with clear legal direction on how to protect privacy rights when conducting surveillance of foreign agents working in the United States. During the debate on the *Foreign Intelligence Surveillance Act of 1978*, Senator Kennedy spoke of the need for a law to balance privacy rights against national security requirements:

Mr. President, this legislation is designed to strike a balance, a careful balance that will protect the security of the United States without infringing on the civil liberties and rights of the American people. I believe the time has at last arrived when Congress and the Executive together can fill one of the last loopholes in the laws governing wiretapping and other electronic surveillance in

¹⁴⁵ *Export Administration Act of 1979, U.S. Statutes at Large* 93 (1979): 506.

the United States. One should view this bill for what it is, a major effort by the Congress, long overdue, to place foreign surveillance under the rule of law.¹⁴⁶

In using these words, Senator Kennedy asserted that only a law could control the manner in which the executive branch would authorize and implement intelligence surveillance. This new law contained a unique feature not found in the privacy, arms, and export laws thus far discussed.

Congress selected a unique judicial mechanism to control activities of the executive branch. Only a new law could have created a "special court" that would later become known as the Foreign Intelligence Surveillance Court or FISA Court. The use of the FISA Court to approve special wiretap warrants was a controversial but unique solution that made the judicial branch an active arbitrator in determining the limits of executive power. The debate on the House version of the *Foreign Intelligence Surveillance Act of 1978*, H.R. 7308, explained the choice of using the judiciary. Representative Wyche Fowler, Jr. (D-Georgia) asserted that the executive branch could not be trusted:

Some observers have commented that the safeguards concerning foreign intelligence surveillance that have recently been established within the executive branch render this legislation unnecessary.... What is done by executive order can be undone by Executive order and we in Congress have a responsibility, not only to ourselves as an institution but also to the people who sent us here, to fulfill our constitutional duty and to legislate national policy.¹⁴⁷

¹⁴⁶ *Congressional Record*, 95th Congress, 2nd sess., 1978, 124, pt. 9: 10888.

¹⁴⁷ *Congressional Record*, 95th Congress, 2nd sess., 1978, 124, pt. 21: 28149.

This text and the other texts used as evidence revealed that the Congressional Group favored laws as solutions to a complex domestic privacy protection, technology export control, and political power problem.

The use of multiple laws as solutions by actors in the Congressional Group matched Allison's GPM general proposition of "Action and Intention" where powerful legislators served as "actions channels" that sponsored and guided proposed laws through the legislative process.¹⁴⁸ The intentions of individual legislators were to solve privacy, economic, export, and national security problems. However, the totality of their actions reduced the power of the executive branch by increasing Congress' foreign affairs and domestic management responsibilities. Congress' actions also opened a new action channel in a political game by using the judicial branch as an active arbitrator of national security decisions made by the executive branch. I therefore assigned a Favored Alternative valance of "2" to the Congressional Group for using laws to achieve their goals.

D. Decision Timing Valance

The Congressional Group exhibited a sense of urgency in satisfying a growing requirement for the protection of privacy information. Along with this requirement, there was a crisis within Congress on how to limit the abuses resulting from the executive branch's constitutional dominance in the foreign policy and national security areas.

¹⁴⁸ Allison and Zelikow, *Essence of Decision*, 306.

During the debate on the *Privacy Act of 1974*, bill sponsor Senator Ervin summarized the urgency of the privacy protection problem and the past abuses that demanded change:

Somehow, the varied and wide-ranging functions which have been thrust very rapidly upon the Federal management machinery of an earlier time, have left great loopholes for the gathering, use and disclosure of information about Americans in ways and for reasons that should give us serious pause. The advent of computer technology and new ways of information storage and sharing which have made it possible for government to provide new services and to carry out new programs, have also encouraged the extension of some practices of doubtful wisdom or constitutionality. These practices have been sanctioned or tolerated by administrations regardless of the party in power. For this reason the concern over the resulting threats to freedom has brought complaints to Congress from Americans in all walks of life.¹⁴⁹

Senator Ervin also noted the following in the debate: "The bill is based on long-standing complaints of governmental threats to privacy which will haunt Americans in the years ahead unless this legislation is enacted."¹⁵⁰ During the next five years, the Congressional Group required three other urgent pieces of legislation to balance national security and public safety requirements against economic and privacy concerns.

The 1976 introduction of H.R. 13680, which amended the *Foreign Military Sales Act*, came after the President vetoed a similar Senate bill, S. 2662. The *Arms Control Export Act*, H.R. 13680, gave Congress greater oversight into the export of dual-use technologies such as encryption. According to bill sponsor Representative Morgan, there was an urgent need to produce legislation:

¹⁴⁹ *Congressional Record*, 93rd Congress, 2d sess., 1974, 120, pt. 27: 36891.

¹⁵⁰ *Ibid.*

The committee has worked long, hard under great pressure, to come back this soon with a bill that we feel is a good honest compromise, a compromise which retains the most essential and worthwhile reforms of S. 2662 while bowing to the most valid of the President's objections.¹⁵¹

From the text, Representative Morgan believed that Congress could find a compromise with the executive branch.

The urgency of the bill did not force the House to reach a resolution during the May 19, 1976 debate. However, the critical nature of funding the legislatively coupled 1977 foreign military assistance program forced the reconciliation of numerous amendments during the subsequent June 2 debate. The House continued the arduous debate and at one point spent two hours on a single issue, the South Korea funding limit.¹⁵² After numerous amendment debates from various representatives and notable stalling by Representative John M. Ashbrook (R-Ohio), the House engrossed the third reading of the bill. Attempts by Representative Ashbrook to recommit the bill to the Committee on International Relations and to point out that a quorum was not present failed to stop passage of H.R. 13680.¹⁵³ Other bills dealing with national security and executive branch powers perpetuated a sense of urgency in Congress.

The looming expiration of *Export Administration Act of 1969* forced a July 21, 1979 Senate debate on S. 737, which would become the *Export Administration Act of 1979*. Congress sought more control over the export of dual-use technology to boost the

¹⁵¹ *Congressional Record*, 94th Congress, 2d sess., 1976, 122, pt. 12: 14434.

¹⁵² *Congressional Record*, 94th Congress, 2d sess., 1976, 122, pt. 13: 16220.

¹⁵³ *Ibid.*, 16242.

economy and to limit the effects of export restrictions that were justified by national security reasons. Senator Stevenson opened the debate with a sense of urgency:

Mr. President, S. 737 is necessary to extend and revise the authority to control U.S. exports and to authorize appropriations to meet the expense of administering export controls. The existing authority which is provided in the Export Administration Act of 1969 expires September 30....

Mr. President, this legislation is one product of a year long study of U.S. export policy by the Subcommittee on International Finance.¹⁵⁴

During the debate, Senator Stevenson had to answer questions on how Congress could protect national security through export controls when technology evolved faster than legislation. Senator Paul E. Tsongas (D-Massachusetts) expanded on the question: “High-technology products advance at rapid rate, but performance levels are reviewed infrequently – only every 3 to 4 years when COCOM reviews take place.”¹⁵⁵ The Coordinating Committee on Multilateral Export Controls or COCOM was an informal supra-national agreement to control dangerous technologies such as nuclear reactors and missile components. S. 737 authorized an indexing scheme to reduce the requirement of yearly legislative action. Instead of requiring urgent legislation, the *Export Administration Act of 1979* automatically relaxed exports restrictions as controlled technologies diffused into foreign markets.

In the case of encryption technology, the United States government 56-bit Data Encryption Standard (DES) became a political pawn in the assessment of foreign

¹⁵⁴ *Congressional Record*, 96th Congress, 1st sess., 1979, 125, pt. 16: 19936.

¹⁵⁵ *Ibid.*, 20009.

availability. DES was the de facto measure of foreign availability as the United States government developed and released this technology. Periodic regulatory crises occurred when stronger encryption algorithms appeared in foreign markets and United States encryption vendors petitioned to index the export restrictions. In this case, Congress defaulted to the executive branch to make an indexing determination. However, the executive branch disappointed Congress by holding steady at the 56-bit DES limit for over ten years. Congress used a different regulatory scheme to balance national security requirements against privacy rights.

The debate on S. 1566, which would become the *Foreign Intelligence Surveillance Act of 1978*, revealed that Congress was at a crisis point in limiting executive power used under the guise of fulfilling national security requirements. Senator Kennedy, who was chairman of the Judiciary Committee, noted the buildup to the crisis:

Mr. President, today the U.S. Senate writes a new chapter in the ongoing 10-year debate to regulate foreign intelligence electronic surveillance. In considering S. 1566, the Foreign Intelligence Surveillance Act of 1978, the full Senate at long last has the opportunity to place foreign intelligence electronic surveillance under the rule of law. The abuses of recent history sanctioned in the name of national security and documented in detail by the Church committee highlight the need for more effective statutory controls and congressional oversight.¹⁵⁶

The ranking member of the Judiciary Committee, Senator James Strom Thurmond (R-South Carolina), tactfully admitted the urgent need for S. 1566 when he stated, "Mr. President, I ask my colleagues to judge this bill on its legislative record over the past few

¹⁵⁶ *Congressional Record*, 95th Congress, 2d sess., 1978, 124, pt. 9: 10887.

years in the Senate.”¹⁵⁷ This bi-partisan approach assured final passage of the bill, but the bill had compromises and a serious gap in policy logic.

The lack of a solution to balance the power of executive and legislative branches delayed S. 1566 for years. Although the *Foreign Intelligence Surveillance Act of 1978* found a unique solution with the FISA Court, Congress in their urgency disregarded other solutions such as using encryption to protect Americans from foreign surveillance in the first place. Senator Birch Bayh (D-Indiana) who was chairman of the Senate Select Committee on Intelligence stated, “American citizens have as much right not to have the Russians eavesdropping on them as not to have their own Government eavesdropping on them.”¹⁵⁸ The idea that protecting privacy could help national security was lost to a political exercise that limited executive power.

The urgent use of legislation by actors in the Congressional Group to fix critical problems, to extend expiring laws, and to control executive power matched Allison’s GPM general proposition of “Problems and Solutions.” In these cases, the Congressional Group focused “not on the total strategic problem but rather on the decision that must be made today or tomorrow.”¹⁵⁹ Urgent decision-making during congressional debates culminated years of research and investigative work on difficult economic, privacy rights, and national security issues. However, solutions to the total strategic problem, such as ensuring privacy rights in the private sector, assisting American dual-use technology

¹⁵⁷ *Ibid.*, 10892.

¹⁵⁸ *Ibid.*, 10894.

¹⁵⁹ Allison and Zelikow, *Essence of Decision*, 307.

exports, and protecting Americans from surveillance through encryption use, lost out to a crisis in shifting the balance of political power. I therefore assigned a Decision Timing valance of "2" to the Congressional Group for acting with a sense of political urgency when balancing privacy rights, economic concerns, and national security requirements.

Encryption Technology Group

In the First Mover Period, the Encryption Technology Group affected encryption policy by researching, developing, and marketing secret key and public key encryption subsystems. Since the United States government did not volunteer existing national security encryption systems for civilian use, the private sector had to develop its own systems. Secret key encryption was the product of industrial research and development, and public key encryption was the product of university research and development. The actors in the Encryption Technology Group contributed to encryption policy by developing competitive alternatives to solve the information security problem. In addition, actors in this group approached the national security aspects of encryption control in a manner different from the other three groups. Engineering conference reports, journal and magazine articles, government correspondence, opinions of technology leaders, and patent applications provided the data for analyzing the actions of the Encryption Technology Group. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

The Encryption Technology Group believed that the private sector, being the inventors and developers of non-military encryption technologies, was the leader in the information security effort. While the government sector could fallback upon encryption systems used for national security or “classified” data, the private sector did not have a similar option. Potential users of encryption in the private sector were the banking and finance industries, and early encryption work sought to ensure the privacy of data used for banking and finance functions. In 1973, Horst Feistel discussed the leading role of private industry in solving the digital data privacy problem: “In tackling the privacy problem presented by modern computers at the Thomas J. Watson Research Center of the International Business Machines Corporation[,] we have given the central role to cipher techniques.”¹⁶⁰ IBM achieved the early lead in developing commercial encryption products by performing the required applied research tasks. In his *Scientific American* article, Feistel mentioned his work with an “IBM system named Lucifer” that would become the technical basis for the United States government’s Data Encryption Standard.¹⁶¹

IBM’s lead in applied research of secret key encryption subsystems allowed IBM to patent an encryption algorithm that the United States government would eventually need for itself to protect digital data on mainframe computers. IBM used its technology

¹⁶⁰ Horst Feistel, “Cryptography and Data Security,” *Scientific American* 228, no. 5 (May 1973): 15.

¹⁶¹ *Ibid.*, 21.

leadership to ensure that all mainframe computers would be able to use a common encryption algorithm. IBM did this by publishing a notice in the *Official Gazette of the United States Patent and Trademark* that surrendered its patent rights to the federal government:

The International Business Machines Corporation hereby grants to any party a nonexclusive, royalty free-license to make, use and sell apparatus, within or without the U.S. Government, which employs the data encryption information published in the Federal Register of March 17, 1975, Vol. #40, Fed. Reg. 12134-12138 for consideration in the Federal standard-making process, or complies with an encryption standard based on such information, or complies with a revised standard based on such information ...¹⁶²

The text does not indicate an explicit motive behind IBM's release of its encryption technology, but subsequent actions support the claim that the motive was the establishment of a first mover advantage.

The American National Standard Institute (ANSI), an organization founded to increase the competitiveness of American businesses, adapted IBM's patented encryption technology in the form of the United States Data Encryption Standard (DES). ANSI approved DES as the American National Standard Data Encryption Algorithm X3.92-1981 on December 30, 1980.¹⁶³ Since the banking and financial communities preferentially used ANSI standards, IBM's technology leadership and government support allowed DES to become the dominant encryption standard for United States

¹⁶² *Official Gazette of the United States Patent and Trademark Office* 934 (13 May 1975): 452.

¹⁶³ American National Standard Data Encryption Algorithm, ANSI x3.92-1981 (New York: American National Standards Institute Inc., 30 December 1980).

banking and finance industries. However, the United States government inhibited the international competitiveness of IBM's technology.

During the Crypto 81 conference sponsored by the Institute for Electrical and Electronic Engineers (IEEE), marketing consultant J. Michael Nye noted that inconsistent United States encryption policy did not help domestic industry:

The restrictive export requirements combined with loose or non-existent import regulations regarding cryptographic equipment places U.S. manufacturers at an extreme disadvantage in the marketplace. In one sense, an agency of the U.S. government is encouraging the development and use of DES based systems as a cryptographic standard in the future for non-classified communications. Such a standard is sorely needed in order to ensure the orderly growth of communication security systems while maintaining interoperability. On the other hand, other government agencies are in the business to discourage the international use of DES based systems by restricting the export of DES chips to be incorporated into foreign manufactured communications security equipment.¹⁶⁴

The text suggests that encryption standards help "U.S. manufacturers" by "maintaining interoperability" and this idea reinforces the rationale behind IBM's release of its encryption patent rights. The text also points out that United States encryption policy limiting the export of encryption chips appeared irrational from the encryption vendors' perspective. Since the DES algorithm was in the public domain, overseas manufacturers could eventually make their own chips if forced to by restrictive United States export regulations. This could hurt United States information technology industries. In a related

¹⁶⁴ J. Michael Nye, "The Import/Export Dilemma," Crypto '81, in *Advances in Cryptology 1981-1997: Electronic Proceedings of the Crypto and Eurocrypt Conferences 1981-1997*, ed. Alan Gersho (New York: Springer-Verlag, 1998), 136.

encryption technology area, the development of public key encryption allowed United States encryption vendors to maintain their technology leadership.

The invention of public key encryption, by Stanford University engineers, created a competitive alternative to DES and secret key encryption. Inventors Whitfield Diffie and Martin E. Hellman knew about the requirement for a competitive encryption system that did not require the passing and guarding of secret keys:

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create the need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.¹⁶⁵

The text shows that the use of encryption in “commercial applications” created a demand for better encryption systems. This form of technological determinism drove inventors to develop a public key encryption subsystem, and in turn, stimulated public and government demand for complete encryption systems.

The actions of the Encryption Technology Group matched Allison’s RAM organizing concept of a “Unified National Actor,” in which members of a group act as a

¹⁶⁵ Whitfield Diffie and Martin E. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory* IT-22, no. 6 (November 1976): 644.

“single agent” in solving a common problem.¹⁶⁶ To solve the digital information protection problem in the private sector, actors in industry and academia used their technology leadership to introduce secret and public key encryption solutions to the market. I assigned a Lead Actor valance of “0” to the Encryption Technology Group for perceiving that the private sector was the leader in developing information security solutions.

B. Problem Perception Valance

Actors in the Encryption Technology Group perceived a simple problem in that digital information required protection from all unauthorized parties, including the government. This group perceived two related problems in proving that encryption worked and in managing encryption keys. This group did not worry about the malicious use of encryption or the transfer of encryption technology to hostile foreign powers, because these issues would have made the information protection problem too complex. Ideas on encryption back doors and archived encryption keys, which would have allowed trusted parties to recover plaintext information with or without the owner’s permission, were not in the problem scope considered by the group. In the early 1970s, IBM engineer Horst Feistel was one of the first people to see the problem as the simple protection of digital data to ensure privacy:

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers

¹⁶⁶ Allison and Zelikow, *Essence of Decision*, 24.

contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or group. It is asserted that it soon will be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in many separate locations under widely diverse jurisdictions. It will be argued here, however, that a computer system can be adapted to guard its contents from everyone but authorized individuals by enciphering the material in forms highly resistant to cipher-breaking.¹⁶⁷

The text suggests that increases in computational power and the amount of information stored on computers worked together synergistically to create a digital information protection problem. In the text, Feistel stated that the solution should be “highly resistant to cipher-breaking.” If this were not the case, then the encryption solution would give a false sense of security. The information protection problem would not be simple if computational power grew faster than the strength of encryption systems. In this case, unauthorized users could eventually employ powerful computers to defeat encryption.

Experts in the area of code breaking or “cryptanalysts” generally believed, but could not prove, that improvements in digital encryption algorithms would outpace the rapid improvements in computational power. In a simplification of the mathematics behind cryptanalysis, if a powerful computer could accurately predict the encryption key by examining the plain and cipher texts, then the encryption system was weak and the algorithm would soon be broken. Whitfield Diffie, working for BNR, Inc., commented on the effects of increased computational power:

¹⁶⁷ Horst Feistel, “Cryptography and Data Security,” *Scientific American* 228, no. 5 (May 1973): 15.

It is a surprising fact that decreases in the cost of computation do not benefit the cryptosystem designer and the cryptanalyst equally. If a cryptographic method is of any value at all – if cryptanalysis takes an effort which is more than a linear function of the effort required to produce a cryptogram – a decrease in the cost of computation benefits the cryptographer to the detriment of the cryptanalyst. This is because the increased computing power that the system designer can afford to employ on encryption will require a more than proportional increase on the part of the cryptanalyst.¹⁶⁸

The text shows that encryption vendors believed that the digital information protection was a problem made simple by the use of strong encryption and that code breakers faced “a more than proportional” challenge in defeating encryption. There was no mathematical proof to this assertion other than empirical evidence gathered over time. This lack of proof and unfamiliarity with the business model behind encryption technology stifled early encryption vendors.

In 1979, encryption vendors explored the market for information security solutions enabled by the use of DES. According to business technology journalist H. P. Burstyn, “Motorola, IBM, Intel, Fairchild and Rockwell Collins” were in the DES market.¹⁶⁹ This market was “slow growing” and the financial sector had the largest user share of the market followed by the government and industrial sectors. Burstyn uncovered evidence that although financial users were “evaluating the DES,” experts were debating the security of DES and how much would it cost to break DES.¹⁷⁰ In a related subject,

¹⁶⁸ Whitfield Diffie, “Cryptographic Technology: Fifteen Year Forecast,” *Crypto '81*, in *Advances in Cryptology 1981-1997: Electronic Proceedings of the Crypto and Eurocrypt Conferences 1981-1997*, ed. Alan Gersho (New York: Springer-Verlag, 1998), 94.

¹⁶⁹ H. P. Burstyn, “Slow Growing Encryption market to spurt in ‘80’s,” *Electronic Business* (January 1979): 76-77.

¹⁷⁰ *Ibid.*, 76-77.

Burstyn noted that encryption vendors were also considering the use of public key encryption to distribute DES keys, but this now obvious use of public key encryption was not apparent to the IBM manager being interviewed.¹⁷¹ Over time, the experiences of the business and financial sectors proved the security of DES. If code breakers could not directly defeat strong encryption, then the next area of vulnerability would be the security and distribution of encryption keys.

The security of the encryption key threatened the simplicity of using encryption as the basis for information security tools. In secret key encryption, duplicates of the encryption key allow the sender and receiver to have confidential communications. Anyone else who has a copy of this key can eavesdrop on these communications. Thus, stealing the key of a remote receiver would compromise the data and communications of all users that made prior use of the stolen key. Although public key encryption could conceptually solve the key management problem, a practical implementation had to be developed. In 1983, MIT inventors Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman won a patent for an algorithm to implement public key encryption based on the mathematically hard problem of factoring numbers larger than a 100 digits. These inventors knew that public key encryption could solve the key management problem faced by secret key encryption.

The present invention provides a *public key* system for establishing private communications and also for providing private communications with the signature. A characteristic of this system is that the public revelation of the

¹⁷¹ *Ibid.*, 77.

encryption key does not reveal the corresponding decryption key. As a result, couriers or other secure means are not required to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only the intended recipient can decipher the message since only he knows the corresponding decryption key.¹⁷²

The text shows that these inventors perceived the importance of the key management problem behind encryption use and developed a solution that is used today in which “the public revelation of the encryption key does not reveal the corresponding decryption key.” Rivest, Shamir, and Adleman leveraged their patent to start a company that, today, still uses the original “RSA” initials in its name.¹⁷³

The actions of the Encryption Technology Group matched Allison’s RAM organizing concept of “The Problem,” in which “a response to a strategic situation” gained ownership of the digital information protection issue by making it a solvable problem.¹⁷⁴ Actors in the Encryption Technology Group used their technical skills to develop an encryption solution that focused on the strength of the encryption algorithm and the management of encryption keys. Other issues such as malicious use of encryption or technology transfer to hostile governments did not significantly influence the perceptions of this group. I assigned a Problem Perception valance of “0” to the Encryption Technology Group for perceiving a simple problem, uncomplicated by the liability of malicious use or national security concerns.

¹⁷² Ronald L. Rivest, et al., “Cryptographic communications system and method,” U.S. Patent # 4,405,829, 20 September 1983.

¹⁷³ RSA Security, RSA Laboratories webpage, 2004, < <http://www.rsasecurity.com/rsalabs/> >, accessed March 2004.

¹⁷⁴ Allison and Zelikow, *Essence of Decision*, 24.

C. Favored Alternative Valance

Actors in the Encryption Technology Group favored utility maximizing solutions to solve the information security problem. All viable solutions to this problem required that the benefits from using encryption had to exceed the costs of both developing encryption technology and getting people to trust and use encryption systems. Users would also require both secret key and public key encryption solutions, as the key distribution problem would eventually become apparent to encryption users. Since the benefits of data security and privacy were hard to quantify, actors in this group used the cost of breaking encryption as a quantitative proxy for the benefits provided by encryption use. In 1977, Stanford engineers Diffie and Hellman estimated the cost of breaking the Data Encryption Standard:

The following section provides the basic argument concerning the standard's inadequate level of security. It shows that, using the simplest of cryptanalytic attacks, a \$20 million machine can be built to break the proposed standard in about 12 hours of computation time. The equivalent cost per solution is only \$5000 (obtained by depreciating the machine over five years). Thus, the proposed standard's level of security against attack is high today – but not excellent, since major intelligence agencies possess the financial resources and the interest to build such a machine.¹⁷⁵

The text shows, despite Diffie and Hellman's skepticism, that it would take a "\$20 million machine" to break the Data Encryption Standard and that only "major intelligence agencies" would be able to break DES. According to the text, if it were to cost less than

¹⁷⁵ Whitfield Diffie and Martin E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer* 10, no. 6 (June 1977): 74.

\$5000 to encrypt data, then the value added by DES encryption would be a rational solution to protect information from intelligence agencies and presumably from all unauthorized users.

In theory, lower cost encryption would produce higher numbers of encryption users. One common way to minimize the cost of encryption was to mass-produce government approved encryption devices. However, factors in addition to the cost of a standardized encryption system influenced users. William H. Murray, an IBM manager, described the decision process behind offering IBM encryption technology for government use:

When the NBS published the request for proposals for DES, I argued that IBM should not propose LUCIFER or any Feistel algorithm. I argued, based upon history, that publishing an algorithm would likely shorten its life. More important I thought, was that it would diminish its value to IBM. Incidentally, I thought that the idea behind the standard was only one of interoperability.

While it was hardly likely that anyone was listening to me then, fortunately for all of us, cooler, brighter heads prevailed. Dr. Lewis Branscomb, who was the IBM Chief Scientist and who had come to IBM from NBS, understood what many of us have only come to understand later. That is, the fundamental strength of an algorithm is necessary but it is not sufficient for its wide acceptance. It is also necessary that collectively we know something about that strength that we can communicate to other people in such a way to create the necessary trust and confidence.

The role of the standard and the NBS was to make a statement about the strength and to give authority to that statement. The statement about strength was that the cheapest known attack was an exhaustive attack against the key.¹⁷⁶

¹⁷⁶ William H. Murray, "The Data Encryption Standard: 20 Years Later," remarks of a panelist, 20th National Information Systems Security Conference, Baltimore, Maryland, October 1997.

The text shows that IBM eventually found that “interoperability” or standardization concerns became secondary to new concerns about encryption strength and trust in the encryption solution. IBM was responsible for engineering the proper encryption strength, and the government was responsible for generating trust in the secret key solution. While implementing the secret key encryption solution had split responsibilities, implementing the public key encryption solution was left solely to the private sector.

Diffie and Hellman, the inventors of public key encryption, understood the inherent limitation of secret key encryption systems and keenly understood that a utility-maximizing solution would require the incorporation of a key distribution system that was internal to the information security solution:

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communication parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.¹⁷⁷

The text indicates that the inventors viewed business people as being the first users of public key encryption. Businesses would consider minimizing “cost and delay” factors as primary requirements for an encryption solution, which secret key encryption could

¹⁷⁷ Whitfield Diffie and Martin E. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory* IT-22, no. 6 (November 1976): 644.

not fulfill. Additional benefits provided by public key encryption solutions would further bolster the advantages of this solution over secret key encryption.

Rivest, Shamir and Adleman, the patent holders of the first practical and strong public key encryption algorithm, emphasized that there were added benefits to using their public key encryption subsystem in the form of providing digital signatures. Users could digitally sign messages with their private keys and recipients could verify the authenticity of these messages by using the public keys of the signatories:

Furthermore, the message can be "signed" by deciphering it with the privately held decryption key. Anyone can verify the signature using the corresponding publicly revealed encryption key corresponding to the originator. Signatures cannot be forged and the signer cannot later deny the validity of his signature.¹⁷⁸

The text suggests that the inventors of the "RSA" implementation of public key encryption found a way to guarantee message authenticity, such that the digital signature could not be "forged," and found a way to enforce non-repudiation, such that the digital signer of the message could not "later deny the validity of his signature." With the added benefits of authenticity and non-repudiation, the public key solution was the utility-maximizing solution for use in the private sector. However, some actors in the government sector did not have the same value perspectives, as did actors in the Encryption Technology Group.

¹⁷⁸ Ronald L. Rivest, et al., "Cryptographic communications system and method," U.S. Patent # 4,405,829, 20 September 1983.

Encryption researchers expanded the utility of public key encryption by suggesting the use of digital signatures in the national security area. At Crypto '82, a multi-disciplinary conference on all aspects of encryption, Leonard M. Adleman proposed an “electronic notary public” to help verify nuclear weapons treaty data:

In this paper we describe the mathematical solution to a communication security problem, which arose in connection with the Nuclear Test Ban Treaty, and for which only physical solutions were known. The problem concerns the implementation of an electronic notary public – a device which can certify information for a group of mutually distrusting parties – among which may be the builder of the device.¹⁷⁹

The text indicates that the utility of the public key encryption solution went beyond the private sector and could include the government sector. However, many in the government sector considered encryption solutions as threats to national security and public safety, thus rejecting the large claims of utility by the Encryption Technology Group.

The actions of the Encryption Technology Group matched Allison’s RAM general proposition that increasing the utility value of a solution “increases the likelihood of that action being chosen.”¹⁸⁰ The actors in the Encryption Technology Group developed competitive secret and public key encryption solutions that the private and government sectors could use. This group also believed that their encryption solutions had positive utility in the national security area by protecting and digitally signing military technical

¹⁷⁹ Leonard M. Adleman, “Implementing an Electronic Notary public,” Crypto '82, in *Advances in Cryptology 1981-1997: Electronic Proceedings of the Crypto and Eurocrypt Conferences 1981-1997*, eds. David Chaum, Ronald L. Rivest and Alan T. Sherman (New York: Springer-Verlag, 1998), 259.

¹⁸⁰ Allison and Zelikow, *Essence of Decision*, 25.

data. I assigned a Favored Alternative valance of “0” to the Encryption Technology Group for generating utility maximizing solutions to solve the information security problem.

D. Decision Timing Valance

Actors in the Encryption Technology Group made decisions that were contingent upon the development of encryption solutions, the maturation of digital hardware and software technologies, and government support. Actors in this group favoring a secret key encryption solution followed a time pattern of research and development, patent application and award, and government release. Arthur Sorkin, a researcher at Lawrence Livermore National Laboratory investigated IBM’s 1970s vintage Lucifer encryption algorithm and found that IBM used Lucifer as a technology baseline for the National Bureau of Standards’ Data Encryption Standard (DES). Sorkin found that Lucifer “was the subject of several U.S. patents” and that “the-state-of-the-art in LSI [large scale integration] at the time Lucifer was constructed had an influence upon design of the device.”¹⁸¹ An examination of Feistel’s “Block Cipher Cryptographic System” patent, which Sorkin referenced, revealed that Feistel filed for a patent on June 30, 1971, and the United States Patent and Trademark Office (USPTO) awarded IBM patent # 3,798,359 on March 19, 1974. This timing suggests that IBM sought and waited for full patent protection before offering its encryption technology to the government.

¹⁸¹ Arthur Sorkin, “Lucifer, a Cryptographic Algorithm,” *Cryptologia* 8, no. 1 (January 1984): 23.

Encryption technology control was not a primary consideration for IBM because of the perceived hardware implementation of encryption. A further examination of the Feistel patent supports Sorkin's finding that the envisioned cryptographic device was dependent on existing hardware technology.¹⁸² Sometime in the summer of 1974, IBM officially submitted a candidate algorithm to the National Bureau of Standards (NBS), which would eventually become the Data Encryption Standard. On February 25, 1975, Ehram, et al., filed a patent for IBM that specifically claimed an encryption algorithm almost identical to DES, but did not use the name of DES. The USPTO awarded IBM patent # 3,958,081 on May 18, 1976. This newer patent also envisioned encryption being implemented in a hardware cryptographic device.¹⁸³ During the period between the filing and award of the Ehram patent, IBM published a notice in the May 13, 1975 *Official Gazette*:

b. all those claims in any other United States patent, which is presently assigned to IBM or which is hereafter assigned to IBM, the infringement of which claims could not be avoided by any apparatus which can be constructed and operated for the purpose of employing the published data encryption information or complying with the standard(s)....

In the event that the standard is not established by the Department of Commerce by September 1, 1976, then such license shall extend only to apparatus manufactured after the date of publication of this notice and prior to September 1, 1976.¹⁸⁴

¹⁸² Horst Feistel, "Block Cipher Cryptographic System," U.S. Patent # 3,798,359, 19 March 1974. Filed on 30 June 1971.

¹⁸³ William Friedrich Ehram, et al., "Block cipher system for data security," U.S. Patent # 3,958,081, 18 May 1976. Filed on 25 February 1975.

¹⁸⁴ *Official Gazette of the United States Patent and Trademark Office* 934 (13 May 1975): 452.

The text shows that IBM was willing to surrender its secret key encryption patents contingent upon the timely government publication of the Data Encryption Standard. NBS did not publish DES by September 1, 1976, so IBM published another *Official Gazette* notice moving the deadline to March 1, 1977.¹⁸⁵ Figure 4-1 shows that IBM made decisions contingent upon prior research, patent awards, and NBS actions.

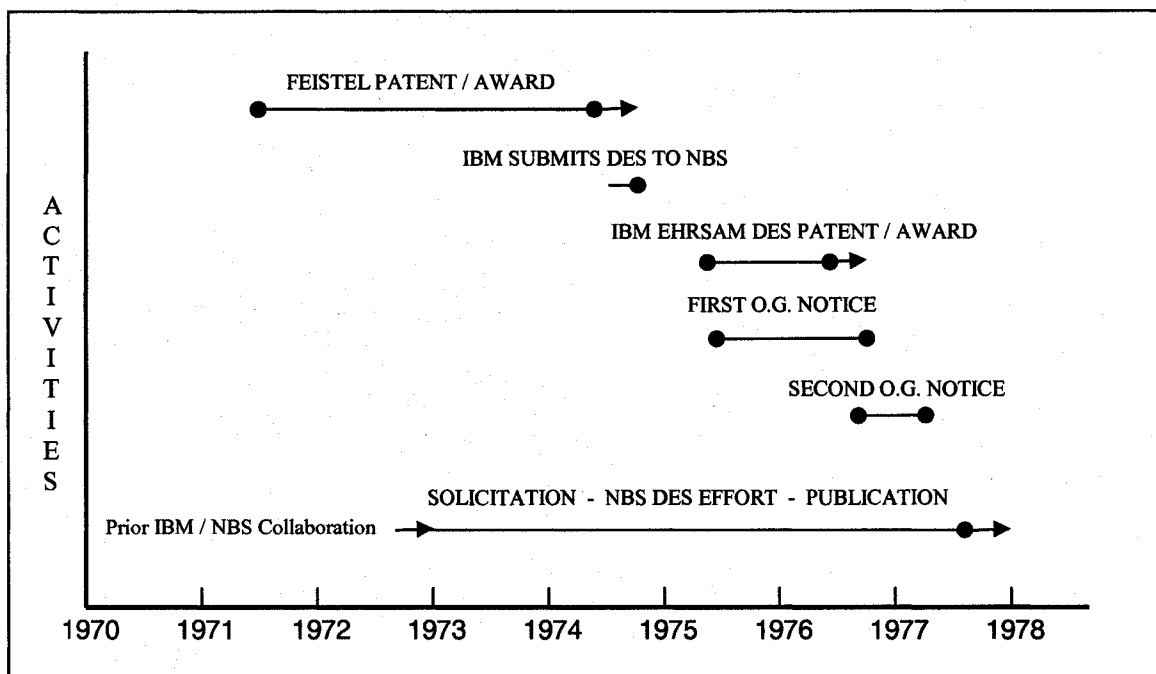


Figure 4-1 Timeline of IBM activities leading up to the publication of DES

Actors in the Encryption Technology Group favored a public key encryption solution that followed a time pattern of research and development, patent application, and award, and that waited for the maturation of digital hardware and software technologies.

¹⁸⁵ *Official Gazette of the United States Patent and Trademark Office* 949 (31 August 1976): 1717.

Lacking the close working relationship that IBM and NBS shared, the actors in the Encryption Technology Group did not make decisions contingent upon government support of public key encryption. Instead, these actors made pragmatic decisions contingent upon development of mathematical algorithms implementing public key encryption and upon the proliferation of 32-bit personal computers.

There is some evidence that the government slowed down development of public key encryption by questioning patent awards. This action may have soured the relations between academia and the government. Hellman, *et al.*, filed for a patent on the concept of public key encryption on September 6, 1977, and the USPTO awarded to Stanford University patent # 4,200,770 on April 29, 1980.¹⁸⁶ The government owned some of the rights to this patent by virtue of its funding the research. Rivest, *et al.*, filed for a patent on an algorithm capable of implementing public key encryption on December 14, 1977, and the USPTO awarded to the Massachusetts Institute of Technology patent # 4,405,829 on September 20, 1983.¹⁸⁷ During this period, Vice Admiral Bobby R. Inman acknowledged that NSA sought to classify cryptography patents for national security reasons:

In the Inventions Secrecy area there has existed for many years a statutory provision permitting the Commissioner of Patent and Trademarks to impose a secrecy order on any invention submitted for patent the public disclosure of which could be detrimental to national security. In two recent cases, NSA sponsored

¹⁸⁶ Martin E. Hellman, *et al.*, "Cryptographic apparatus and method," U.S. Patent # 4,200,770, 29 April 1980.

¹⁸⁷ Ronald L. Rivest, *et al.*, "Cryptographic communications system and method," U.S. Patent # 4,405,829, 20 September 1983.

secrecy orders; intensive and continuing technical review by the Agency permitted them to be withdrawn.... In sponsoring secrecy orders under the inventions Secrecy Act, the Agency's sole consideration is the detrimental effect on the Agency's mission, and thus on the security of the United States, that would result from the proliferation aboard of sophisticated cryptologic technology.¹⁸⁸

The text shows that, "In two recent cases, NSA sponsored secrecy orders." NSA did not reveal any details about these two cases. However, USPTO had already awarded patents on secret key encryption. This left patents on public key encryption open for a possible challenge by NSA. Figure 4-2 shows these dates and the unusual time delay in awarding a patent for the RSA algorithm.

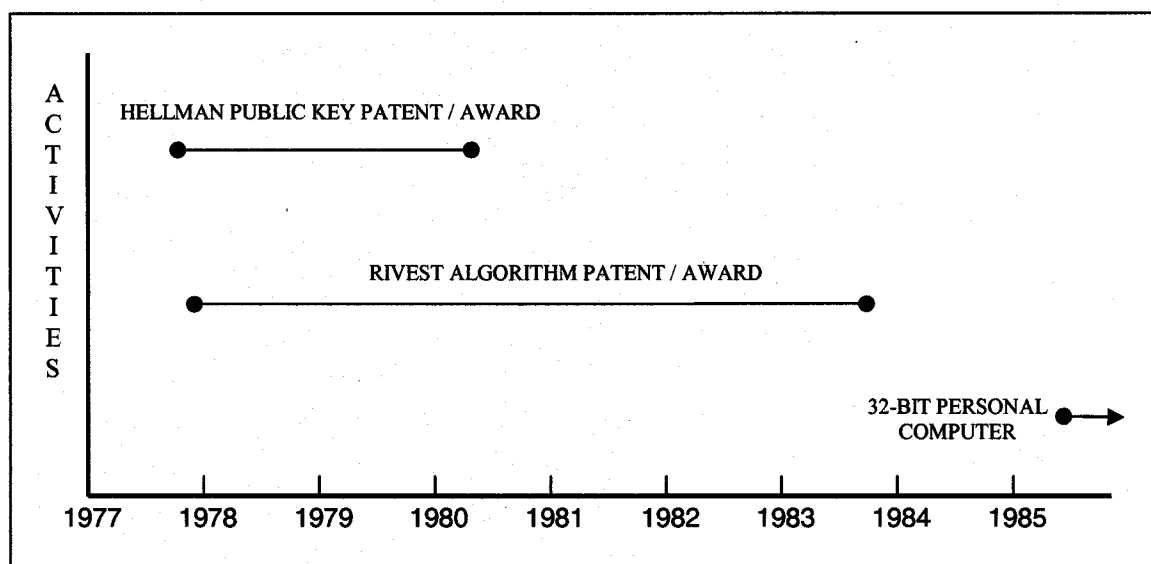


Figure 4-2 Public key encryption activities and the wait for computer power

¹⁸⁸ Bobby R. Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector," *Signal Magazine* (March 1979): 12.

After award of the Rivest patent, actors in the Encryption Technology Group had to wait until the development of 32-bit personal computers before launching a viable commercial public key encryption product. Intel Corporation introduced the 32-bit 80386 processor in 1985, and Figure 4-2 shows this event. A time trial of the RSA public key encryption algorithm on a vintage 80386-based computer took 66 seconds to encrypt a page of text as compared to the 0.17 seconds required by the secret key Data Encryption Standard algorithm.¹⁸⁹ Thus by the end of the First Mover Period in 1986, the newest personal computers were able to perform public key encryption at a tolerable speed for business users. The key management advantage of public key encryption came at a cost to encryption speed and was contingent on the introduction of advanced 32-bit computers. In addition, the lack of a communication system such as the Internet hindered development of complete encryption systems.

Actors in the Encryption Technology Group exhibited behaviors that matched Allison's RAM general proposition whereby a decrease in the utility value of a solution "decreases the likelihood of that action being chosen."¹⁹⁰ Actors in the Encryption Technology Group made different decisions regarding secret and public key encryption solutions. Actors who made secret key encryption contingent upon government sponsorship incurred a time cost penalty of approximately two years, but gained the benefit of increased trust in this new technology. Actors who overcame government

¹⁸⁹ I ran these time trials on a vintage Gateway 80386 "DX" computer running at 33 Mhz and using DOS-based software from Dr. Chris Gaj. File size was 1900 bytes.

¹⁹⁰ Allison and Zelikow, *Essence of Decision*, 25.

indifference and delay on public key encryption had to wait for computers that were more powerful and incurred a time cost penalty of approximately six years. The value of superior key management capability did not offset the first mover advantage of secret key encryption. I assigned a Decision Timing valance of "0" to the Encryption Technology Group for making decisions contingent upon choices that increased the value of their respective encryption solutions.

Executive Group

In the First Mover Period, the primary actors in the Executive Group affecting encryption policy were the president, intelligence agencies, and the Secretaries of Commerce, Defense, and State. The president, through routine orders and directives, enabled the federal departments to develop encryption technology to protect privacy. However, federal departments contributed to encryption policy by their preference to use long-established regulations to protect national security and by their reluctance to place newly enacted privacy laws on an equal level with these regulations. Executive orders, directives, regulations, congressional testimony, and opinions from leaders in the executive branch provided the data for analyzing the actions of the Executive Group. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

In the First Mover Period, actors in the Executive Group worked with Congress to satisfy national security requirements, protect privacy rights, maintain technology leadership, and increase technology exports. The Executive Group focused on the national security aspects of evolving information and encryption technologies and displayed leadership in the information security area by attempting to regulate privacy protection. However, after the Watergate Era abuses, Congress rebuked presidential forays into leading the domestic privacy protection effort. President Gerald R. Ford made a statement to Congress on the pending *Privacy Act of 1974* to support executive branch control of the privacy issue through his Domestic Council:

Immediately after I assumed the Chairmanship, as Vice President, of the Cabinet-level Domestic Council Committee on the Right of Privacy, I asked the Office of Management and Budget to work jointly with the Committee staff, the executive agencies, and the Congress to work out realistic and effective legislation at the earliest possible time. Substantial progress has been made by both the Senate and the House on bills extending personal privacy protections to tens of millions of records containing personal information in hundreds of Federal data banks.¹⁹¹

Congress did not believe that the Domestic Council could manage the privacy issue and acted against President Ford's implied continuance of the Domestic Council as a solution. Congress opted for a new law that specified stringent federal privacy regulations for the protection, review, and release of personal information by the federal government. Thus, the Executive Group lost the lead to Congress in the privacy protection area, but was able

¹⁹¹ Gerald R. Ford, *Public Papers of the Presidents of the United States: Gerald R. Ford, 1974* (Washington, D.C.: GPO, 1975), 243.

to maintain its historical leadership role in the national security area and gain a leadership role in the information security area.

Actors in the Executive Group used encryption policy to satisfy long-standing international relations and national security requirements for information security and, with equal importance, to satisfy information access requirements. Controlling the Soviet threat in the 1970s and the early 1980s served as a prime motivator for the Executive Group. A common topic of presidential speeches was restricting technology that could fall into Soviet hands and subsequently be used against the United States. President Jimmy Carter, worried about the Soviet occupation of Afghanistan, stated the following in his 1981 State of the Union Address: "The maintenance of national security is my first concern, as it has been for every president before me."¹⁹² President Carter also indicated that the executive branch would control the science and technology area to protect national security:

Science and technology are becoming increasingly important elements of our national security and foreign policies. This is especially so in the current age of sophisticated defense systems and of growing dependence among all countries on modern technology for all aspects of their economic strength. For these reasons, scientific and technological considerations have been integral elements of the Administration's decision-making on such national security and foreign policy issues as the modernization of our strategic weaponry, arms control, technology transfer, the growing bilateral relationship with China, and our relations with the developing world.¹⁹³

¹⁹² Jimmy Carter, *Public Papers of the Presidents of the United States: Jimmy Carter, 1980-81*, vol. 3 (Washington, D.C.: GPO, 1982), 2976.

¹⁹³ *Ibid.*, 2962.

Controlling the science and technology behind encryption in addition to controlling information access and security requirements proved difficult for the Executive Group.

Actors in the Executive Groups had limited control over encryption technology because of the historical absence of a federal department on science and technology. Federal science and technology leadership was distributed among several federal departments and quasi-independent federal agencies. Members of the Encryption Technology Group, which all were in the private sector, developed and marketed encryption-based information security tools for the government and private sectors. Members of the National Security Council System (NSCS) perceived a serious threat arising from the availability and use of these commercial information security tools. Hostile foreign powers, such as the Soviet Bloc nations, could use encryption to deny the intelligence and law enforcement communities information access. In a rare published statement, Vice Admiral Inman, then as the Deputy Director of the Central Intelligence Agency (CIA), cautioned the academic and private technology sectors about publishing details on encryption technology:

One sometimes hears the view that publication should not be restrained because "the government has not made its case," almost always referring to the absence of specific detail for public consumption. This reasoning is circular and unreasonable. It stems from a basic attitude that the government and its public servants cannot be trusted. Specific details about why information must be protected are more often than not even more sensitive than the basic technical information itself. Publishing examples, reasons and associated details would certainly damage the

nation's interests. Public review and discussion of classified information which supports decisions is not feasible or workable.¹⁹⁴

The inability and frustration of the NSCS to control encryption technology directly was apparent in the tone of Admiral Inman's comments. His logic on "why information must be protected" appears weak today, but in the context of the Cold War, any information on encryption technology and the availability of exported encryption systems were thought to help the Soviet threat.

In January 1984, President Ronald Reagan publicly notified Congress about the hostile uses of encryption technology and thereby prejudiced the American public that the users of encryption were evil. President Reagan reported that the Soviet Union was in violation of the Strategic Arms Limitation Treaty II by encrypting information:

Three SALT II concerns are addressed: encryption, SS - X - 25, and SS - 16.

4. Encryption -- Impeding Verification

-- *Obligation*: The provisions of SALT II ban deliberate concealment measures that impede verification by national technical means. The agreement permits each party to use various methods of transmitting telemetric information during testing, including encryption, but bans deliberate denial of telemetry, such as through encryption, whenever such denial impedes verification.

-- *Issue*: The study examined the evidence whether the Soviets have engaged in encryption of missile test telemetry (radio signals) so as to impede verification.

-- *Finding*: Soviet encryption practices constitute a violation of a legal obligation prior to 1981 and a violation of their political commitment subsequent to 1981. The nature and extent of encryption of telemetry on new ballistic missiles is an

¹⁹⁴ Bobby R. Inman, "Classifying Science: A Government Proposal...", *Aviation Week and Space Technology* (8 February 1982): 10-12.

example of deliberate impeding of verification of compliance in violation of this Soviet political commitment.¹⁹⁵

The text shows that President Reagan coupled the routine encryption of telemetry data with a growing Soviet nuclear threat. This coupling added to the leadership stature of executive branch by demonstrating the intelligence prowess of the United States. In addition, this coupling inferred that encryption users had something malevolent to hide. These allegations left open to speculation the true capabilities of the United States government. How much information could and could not be decrypted is still a national security secret, which perpetuates a purposefully ambiguous perception that the intelligence community can break many encryption schemes. However, actors in the Executive Group knew that it was nearly impossible to gain information access without legal or surreptitious assistance. Ambiguous perceptions on encryption use and the United States government's capability to access encrypted information had lasting effects on encryption policy. Most actors in the Executive Group would view encryption use as hurting national security by denying information access and would rarely view encryption use as helping national security by protecting information.

The perception by actors in the Executive Group that the government was the lead actor in solving the information access and security problems matched Allison's GPM organizing concept of "Players in Positions."¹⁹⁶ According to this concept, information control policy was made by actors "occupying a position in the major channels for

¹⁹⁵ Ronald Reagan, *Public Papers of the Presidents of the United States: Ronald Reagan, 1984*, vol. 1 (Washington, D.C.: GPO, 1986), 296-8.

¹⁹⁶ Allison and Zelikow, *Essence of Decision*, 296-8

producing action on national security issues.”¹⁹⁷ The passage of the *Privacy Act of 1974* limited these “action channels” from dealing with domestic information access requirements. This allowed the Executive Group to concentrate on information access requirements for national security purposes. The Soviet threat provided the motivation to retain policy actor leadership in information control area, despite the law-making powers of Congress and the technology leadership of the private sector. I therefore assigned a Lead Actor valance of “2” to the Executive Group for being the lead actor on the national security part of the information control problem.

B. Problem Perception Valance

Actors in the Executive Group perceived that information security and privacy protection were parts of a composite problem with Congress solving the legislative piece and the executive branch solving the national security piece. The Executive Group further shared the information security problem with the federal departments, federal agencies, and the private sector. In a move to decentralize routine decision-making activities in the Executive Office of the President, President Nixon issued Executive Order 11717 on May 9, 1973. This order moved functions from the Office of Management and Budget, which President Nixon created from the Bureau of the Budget, to the federal departments and federal agencies. While the 1965 *Brooks Act* specified that the Secretary of Commerce would advise the President on “uniform Federal

¹⁹⁷ *Ibid.*, 296.

automatic data processing standards,” E.O. 11717 changed this decision-making process.¹⁹⁸

Sec. 2. There are hereby transferred to the Secretary of Commerce all functions being performed on the date of this order in the Office of Management and Budget relating to the establishment of Government wide automatic data processing standards, including the function of approving standards on behalf of the President.¹⁹⁹

The text shows that the president gave the Secretary of Commerce direct authority to make decisions on Automatic Data Processing Standards, which included federal government encryption standards. With the Secretary of Commerce handling one piece of the information security problem through federal standards, the Departments of Defense, State, and Justice were to handle the other pieces.

President Ford, in his statement on the pending *Privacy Act of 1974*, thought that privacy protection was part of a composite information access and security problem: “In legislating, the right of privacy, of course, must be balanced against equally valid public interests in freedom of information, national defense, foreign policy, law enforcement, and in a high quality and trustworthy Federal work force.”²⁰⁰ The executive branch relied upon the combined efforts of the Department of Defense and the Department of State to handle the national defense and foreign policy aspects of the problem.

¹⁹⁸ *Brooks Act, U.S. Statutes at Large* 79 (1965): 1128.

¹⁹⁹ President, Executive Order 11717, “Transferring certain functions from the Office of Management and Budget to the General Services Administration and the Department of Commerce,” *Federal Register* 38, no. 91 (11 May 1973): 12315.

²⁰⁰ Gerald R. Ford, *Public Papers of the Presidents of the United States: Gerald R. Ford, 1974* (Washington, D.C.: GPO, 1975), 243.

Actors in the Executive Group believed that the Department of State could solve both national defense and foreign policy issues caused by the on-going development of encryption technology solutions. In accordance with the 1968 *Foreign Military Sales Act* and its 1976 version renamed the *Arms Control Export Act*, the President had the authority to control encryption technology:

The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall constitute the United States Munitions List.²⁰¹

As in prior years, the executive branch delegated the task of deciding what would be considered as “defense articles.” The Department of State, in coordination with the Department of Defense, used a World War II legacy “cryptographic devices” category to regulate the import and export of encryption technology.²⁰² Although “border measures” controlling encryption technology were under the Department of State’s Title 22 of the Code of Federal Regulations, the Department of Defense originated the Munitions List that contained the cryptographic devices category. Thus, the Department of Defense had primary control over the foreign policy and national security effects caused by the export of encryption technology. As long as encryption technology remained in a hardware form, control by the Munitions List was viable.

²⁰¹ *Arms Export Control Act, U.S. Statutes at Large* 90 (1976): 744.

²⁰² U.S. Department of State, Arms, Ammunition, and Implements of War, *Code of Federal Regulations*, vol. 22, secs. 121, 121.01 and 121.1 (Washington, D.C.: GPO, 1969), 222 and 273. Microfiche.

The advent of public key encryption in 1977 would have posed a complex problem to the Executive Group by making border measures ineffective, as this form of encryption was software based. However, the lack of proliferated and interconnected computers during the First Mover Period minimized the threat and allowed the Executive Group to ignore public key encryption. There is evidence, by analogy, that the Department of Defense's National Security Agency suppressed the public key encryption problem by remaining silent on this technology. The United Kingdom's counterpart of NSA, the Communications-Electronics Security Group (CESG), claimed that it discovered the principles behind public key encryption in the early 1970s. CESG withheld this information from the public because of national security concerns. British public key encryption discoverer, J. H. Ellis, explained the reason: "Revelation of these secrets is normally only sanctioned in the interests of historical accuracy after it has been demonstrated clearly that no further benefit can be obtained from continued secrecy."²⁰³

Actors in the Executive Group also had the opportunity to control public key encryption at its inception. The inventors of public key encryption, Martin Hellman, Whitfield Diffie, and Ralph Merkle, indicated in their patent application that the United States government had some rights to public key encryption: "The Government has rights in this invention pursuant to Grant No. ENG-10173 of the National Science Foundation

²⁰³ J. H. Ellis, *The History of Non-Secret Encryption*, 1987, <<http://www.cesg.gov.uk/site/publications/media/ellis.pdf>>, accessed March 2004.

and IPA No. 0005.”²⁰⁴ Since the United States Patent and Trademark Office is part of the Department of Commerce, the Executive Group could have adapted public key encryption to solve part of the digital information protection problem or suppressed the technology to solve potential national security and foreign policy problems. One explanation for inaction by the Executive Group was their failure to perceive the rapid spread of computers required to implement public key encryption. Thus, the Executive Group focused on controlling existing hardware-based secret key encryption.

The perception by actors in the Executive Group that the privacy, information security, and encryption control problems were related pieces of a larger problem matched Allison’s OBM organizing concept of “Factored Problems and Fractioned Power.”²⁰⁵ According to this concept, this group selected pieces of a composite problem that the Departments of Commerce, Defense, and State could solve. The Executive Group ignored private sector development of public key encryption, because this technology did not pose an immediate threat. In addition, it was not clear which executive branch actor could best solve this problem. I therefore assigned a Problem Perception valance of “1” to the Executive Group for perceiving a composite problem.

²⁰⁴ Martin E. Hellman, et al., “Cryptographic apparatus and method,” U.S. Patent # 4,200,770, 29 April 1980.

²⁰⁵ Allison and Zelikow, *Essence of Decision*, 166-167.

C. Favored Alternative Valance

Actors in the Executive Group favored the continuation of past precedents to solve the privacy and information security problems and the national security and foreign policy problems caused by the growing use of encryption technology. In 1974, President Nixon created the Domestic Council Committee on the Right of Privacy to change the privacy rights condition into a problem by proposing an executive branch solution:

Many of the good things in life that Americans take for granted would be impossible or impossibly high-priced, without data retrieval systems and computer technology. But until the day comes when science finds a way of installing a conscience in every computer, we must develop human, personal safeguards that prevent computers from becoming huge mechanical, impersonal robots that deprive us of our essential liberties....

To meet a challenge of these dimensions, we need more than just another investigation and just another series of reports. That is why I am today establishing in the White House a top priority Domestic Council Committee on the Right of Privacy. This will not be another research group. It will be a panel of the most able men and women in the Government, and it will be primed for high-level action.²⁰⁶

President Nixon's suggested use of his Domestic Council came about from prior actions set in motion. In 1970, he informed Congress of reorganizations in the Executive Office of the President to include new policy and budget organizations.²⁰⁷ The creation of his Domestic Council and the Office of Management and Budget took place on July 1,

²⁰⁶ Richard Nixon, *Public Papers of the Presidents of the United States: Richard Nixon, 1974* (Washington, D.C.: GPO, 1975), 196-198.

²⁰⁷ Richard Nixon, *Public Papers of the Presidents of the United States: Richard Nixon, 1970* (Washington, D.C.: GPO, 1971), 257-263.

1970.²⁰⁸ Although Congress would later reject President Ford's 1974 offer to use the Domestic Council to solve the privacy problem, the executive branch did have some success in following past precedents to develop and control possible privacy solutions using encryption technology.

Continuing with his precedent to concentrate on policy and budgetary decisions within certain sections of the Executive Office of the President, President Nixon delegated technical decisions and functions to their appropriate federal departments. In the case of establishing automatic data processing standards, President Nixon used Executive Order 11717 to transfer this function from the Office of Management and Budget to the Secretary of Commerce in 1973.²⁰⁹ This transfer of responsibility allowed the creation of a United States government encryption standard by an organization responsive to the Secretary of Commerce and not under tight presidential control.²¹⁰ Other federal departments also followed legacy precedents in controlling encryption technology.

The Departments of Defense and State maintained regulatory control of encryption technology by following Cold War regulations that prohibited the export of encryption

²⁰⁸ President, Executive Order 11541, Prescribing the Duties of the Office of Management and Budget and the Domestic Council in the Executive Office of the President," *Federal Register* 35, no. 128 (2 July 1970): 10737.

²⁰⁹ President, Executive Order 11717, "Transferring certain functions from the Office of Management and Budget to the General Services Administration and the Department of Commerce," *Federal Register* 38, no. 91 (11 May 1973): 12315.

²¹⁰ U.S. Department of Commerce, National Bureau of Standards, "Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage; Solicitation of Proposals," *Federal Register* 38, no. 93 (15 May 1973): 12763.

technology. In contrast, throughout the First Mover Period, Department of Commerce regulations were silent on the economic advantages of exporting encryption technology. In 1954, President Dwight D. Eisenhower used Executive Order 10575 to create the United States Munitions List.²¹¹ The Munitions List represented an agreement between the Secretaries of Defense and State on specific defense items and dual-use technologies that required controls. The *Federal Register* periodically publishes this list, which is also found in the Department of State's Title 22 of the Code of Federal Regulations (CFR). For example, the 1958 version of Title 22 of the CFR, Section 121 – Arms, Ammunition and Implements of War controlled encryption technology under the heading of “Cryptographic devices (encoding and decoding).”²¹² Following this precedent and with little change over the years, the 1985 version of 22 CFR Section 121 controlled “Speech scramblers, privacy devices, cryptographic devices and software (encoding and decoding).”²¹³ The addition of term “software” to the 1985 version was the only change to handle twenty-seven years of advancement in the state of technology. Similar to policy actions taken on the export side of encryption control, the domestic side of controlling new information technology used adaptations of past actions.

Actors in the Executive Group were reticent on the negative economic effects of encryption control and on the domestic uses of encryption technology to protect national

²¹¹ President, Executive Order 10575, “Administration of Foreign-Aid Functions,” 5 November 1954, *Federal Register* 19, no. 218 (9 November 1954): 7249-7253.

²¹² U.S. Department of State, Arms, Ammunition, and Implements of War, *Code of Federal Regulations*, vol. 22, sec. 121.21 (Washington, D.C.: GPO, 1958), 202. Microfiche.

²¹³ U.S. Department of State, United States Munitions List, *Code of Federal Regulations*, vol. 22, sec. 121.1 (Washington, D.C.: GPO, 1985), 326. Microfiche, 1 March 1985 Edition.

security and personal privacy. Although the 1979 *Export Administration Act* championed the economic gains provided by free trade, the Department of Commerce's Title 15 of the Code of Federal Regulations did not encourage the licensing of encryption technology for export. Changes to Title 15 that favored encryption exports would have to wait until the Clinton administration.²¹⁴ Likewise, the *Foreign Intelligence Surveillance Act of 1978* acknowledged the threat of hostile foreign surveillance, but the Department of Justice's Title 18 of the United States Code did not encourage the use of encryption by citizens as protective measures to eliminate this threat. The passage of the *Electronic Communications Privacy Act of 1986* changed Title 18 to favor the use of encryption for commercial purposes. However, Title 18 also did not encourage citizens to use encryption to protect against spying by foreign agents.²¹⁵ These instances of policy reticence by actors in the Executive Group suggest that they did not want to weaken the export bans called for by the Munitions List and did not want to hinder surveillance of foreign agents by promoting widespread encryption use. A legacy of policy reticence on promoting encryption use may explain the government's suppression of public key encryption and failure to exercise control over its encryption technology patent rights. The executive branch selectively viewed the use of information security tools as posing too much of a national security and public safety risk when compared to its domestic benefit gained from protecting privacy and valuable information.

²¹⁴ U.S. Department of Commerce, Commerce Control List, *Code of Federal Regulations*, vol. 15, sec. 738 (Washington, D.C.: GPO, 1997), 165-177. Microfiche.

²¹⁵ *Electronic Communications Privacy Act of 1986, U.S. Statutes at Large* 100 (1986): 1848-1873.

The following of past precedents by actors in the Executive Group matched Allison's OBM general proposition that "Implementation Reflects Previously Established Routines."²¹⁶ In finding alternatives to solve the composite problem of protecting privacy rights and digital information, promoting economic exports, and ensuring national security, this group favored repeating fragmented past actions instead of examining the whole problem to determine an optimum and better-integrated alternative. I therefore assigned a Favored Alternative valance of "1" to the Executive Group for favoring national security concerns and slighting domestic and economic concerns on the privacy and information security problems.

D. Decision Timing Valance

Evidence shows that actors from the Executive Group made incremental decisions on controlling the export of encryption technology and tacit decisions on suppressing public key encryption technology. As discussed earlier, the Department of State was responsible for implementing Title 22 of the Code of Federal Regulations. The International Traffic in Arms Regulations (ITAR) section controls the import and export of military articles by using a Department of Defense originated United States Munitions List. Since the Department of State routinely publishes changes to the United States Munitions List, these changes can be used as evidence for analysis.

²¹⁶ Allison and Zelikow, *Essence of Decision*, 178.

When viewed from an information technology perspective, the 1969 version of 22 CFR Section 121 – Arms, Ammunitions and Implements of War contains the United States Munitions List that has changed incrementally over the years. Even when the *Arms Export Control Act* and the *Export Administration Act of 1979* wrought significant statutory changes to the United States Munitions List, the encryption section of this list changed little. The Department of State set the encryption policy baseline in 1957 by creating a United States Munitions List that included “Cryptographic devices (encoding and decoding).”²¹⁷ A December 1966 revision added a few words, “Cryptographic devices (encoding and decoding), and specifically designed components therefore.”²¹⁸ A July 1969 major revision to 22 CFR did not include a United States Munitions List, but did have a note about the list being “issued at a later date.”²¹⁹ In August 1969, the updated United States Munitions List formed a policy baseline for encryption technology that would last until 1984:

CATEGORY XIII—AUXILIARY MILITARY EQUIPMENT

(a) Aerial cameras ...

²¹⁷ U.S. Department of State, "International Traffic in Arms," *Federal Register* 22, no. 250 (27 December 1957): 10875.

²¹⁸ U.S. Department of State, "International Traffic in Arms," *Federal Register* 31, no. 233 (2 December 1966): 15175.

²¹⁹ U.S. Department of State, "International Traffic in Arms," *Federal Register* 34, no. 134 (17 July 1969): 12029.

(b) Speech scramblers, cryptographic devices (encoding and decoding), and specifically designed components [therefore], ancillary equipment, and especially devised protective apparatus for such devices, components, and equipment.²²⁰

The text shows that the 1969 baseline was a minor and incremental change to what worked in the past. The addition of speech scramblers showed a move toward including analog privacy devices to the list, while the term “especially devised protective apparatus” appears to be a typographic error of “specially designed protective apparatus.” Uncaught errors further the claim that the Department of State did not put much effort into making incremental changes to the United States Munitions List. The next revision took almost 15 years to make.

The Departments of Defense and State did little to change control of encryption technology by modifying the United States Munitions List, despite the revolutionary changes being brought about by the advancements in information technology. The national security concerns of the 1976 *Arms Export Control Act* and the economic concerns of the *Export Administration Act of 1978* suggested that actors in the Executive Group would have to make difficult policy decisions regarding the export of information security tools. In 1980, the Department of State concluded, “The last significant revision of the ITAR had been completed in 1969, and there was in addition a need to simplify the complex structure and language of the regulations.” However, the proposed revision to

²²⁰ U.S. Department of State, “International Traffic in Arms,” *Federal Register* 34, no. 156 (15 August 1969): 13275.

the encryption paragraph of the United States Munitions List was incremental in substance:

CATEGORY XIII—AUXILIARY MILITARY EQUIPMENT

(a) Aerial cameras ...

(b) Speech scramblers, privacy devices, cryptographic devices (encoding and decoding), and specifically designed components [therefore], ancillary equipment, and especially devised protective apparatus for such devices, components, and equipment.²²¹

The text indicates that the information security paradigm set forth by the development of secret and public key encryption in the 1970s merely warranted the addition of the phrase “privacy devices” to the United States Munitions List. A more rational change would have delineated the components of encryption technology and specified the controls on each component. Since encryption technology depends primarily on algorithms, the Department of State could have enhanced Section 125 of 22 CFR that deals with controlling technical data, under which digital encryption algorithms designs would fall.

The Department of Commerce suggested using encryption export controls by stating the following in the 1977 Data Encryption Standard: “Cryptographic devices and technical data regarding them are subject to Federal Government export control as specified in Title 22, Code of Federal Regulations, Parts 121 through 128.”²²² However, the Department of Commerce took no regulatory action under the *Export Administration*

²²¹ U.S. Department of State, “Revision of the International Traffic in Arms Regulations (ITAR),” *Federal Register* 45, no. 246 (19 December 1980): 83971.

²²² U.S. Department of Commerce, National Bureau of Standards, *The Data Encryption Standard (DES)*, Federal Information Processing Standard Publication 46 (Washington, D.C., July 1977), 2.

Act of 1978 to encourage or discourage the export of encryption technology. The deference by the Department of Commerce to the Department of State's United States Munitions List represented a tacit decision not to complicate the regulatory status of encryption technology. This was done despite the statutory direction to enhance technology exports. Thus, the Department of State was free to make incremental and tacit changes to encryption controls irrespective of effects on domestic information technology industries.

In 1984, the Department of State published a critical change to the United States Munitions List thereby assuming greater control of encryption technology to include public key encryption:

CATEGORY XIII—AUXILIARY MILITARY EQUIPMENT

(a) Aerial cameras ...

(b) Speech scramblers, privacy devices, cryptographic devices and software (encoding and decoding), and components specifically designed or modified therefore, ancillary equipment, and protective apparatus specifically designed or modified therefore.²²³

The text shows a small change to correct the "especially devised" phrase found in the earlier regulations and the tacit insertion of the word "software." The decision to expand the United States Munitions List to include cryptographic software greatly affected the growing use of public key encryption. Unlike the original hardware implementations of

²²³ U.S. Department of State, "Revision of the International Traffic in Arms Regulations (ITAR)," *Federal Register* 49, no. 236 (6 December 1984): 47688.

secret key encryption, public key encryption gained its flexibility and functionality from software implementations of mathematical algorithms that could run on personal computers. Thus, software control represented a policy decision made by the Departments of Defense and State to prevent proliferated encryption technology from threatening national security. The Department of Commerce did little to counter-balance the ensuing economic losses resulting from restricting encryption exports, while the Department of Defense continued to increase its role in encryption control through subsequent executive decisions.

The issuance of the 1984 National Security Decision Directive (NSDD) 145 by President Reagan gave the Department of Defense's National Security Agency temporary dominance over encryption standards. In a process not vetted by congressional debate, NSDD-145 assigned to NSA the responsibility for encryption used to protect all federal digital information. NSA already had responsibility to protect federal classified data using "Type I" encryption, and this new responsibility would be for "Type II" and "Type III" encryption systems for sensitive, but unclassified information:

7. The National Manager for Telecommunications Security and Automated Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunication systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive

Order and implementing procedures, and applicable Presidential directive. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.²²⁴

The power given to the Director of NSA is found in the phrases, “Act as the government focal point for cryptography” and “Review and approve all standards” and suggests that NSDD-145 directly challenged the authority of the National Bureau of Standards to develop encryption standards. This tacit decision to increase the power of NSA served as the basis for a political battle between the executive and legislative branches.

The use of incremental changes and tacit decisions by the actors in the Executive Group to control encryption technology matched Allison’s OBM general proposition of “Limited Flexibility and Incremental Change.”²²⁵ The Departments of Defense and State, constrained by the legacy United States Munitions List, made small changes irrespective of the large statutory shift to liberalize exports. The Executive Group made a tacit decision to control encryption software by the inserting a single word into the United States Munitions List and by increasing the power of NSA. I therefore assigned a Decision Timing valance of “1” to the Executive Group for making incremental changes

²²⁴ Ronald Reagan, National Security Decision Directive 145, “National Policy on Telecommunications and Automated Information Systems Security,” 17 September 1984: 7.

²²⁵ Allison and Zelikow, *Essence of Decision*, 180.

and tacit decisions to support national security and public safety requirements over privacy and economic concerns.

Government Agencies Group

In the First Mover Period, primary actors in the Government Agencies Group were the National Bureau of Standards (NBS) and the Defense Department's National Security Agency (NSA). These actors worked together with IBM in developing the Data Encryption Standard. Official notices published in the *Federal Register*, United States patents, and Federal Information Processing Publications provided the data for analyzing the actions of this group. The primary task of the Government Agencies Group was to solve the growing information security problem caused by the computerization of sensitive data in industry and government. The solution was the development of a first ever Data Encryption Standard that would ensure data security through a standardized implementation of extant digital technology. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor valance

Evidence shows that actors from the Government Agencies Group believed that they were working with private sector actors as a consortium in solving the information security problem. During the 1970s, no single group of actors had the resources, technical knowledge, and authority to develop and implement a universally acceptable data encryption standard. Assertions by reputable authors, such as James Bamford and

Bruce Schneier on the actions and motivations of individual actors in the Government Agencies Group, often substitute for documented evidence on the contributions of the National Bureau of Standards and the National Security Agency to encryption policy. The sparseness of textual data from this period limits explanation of the nuanced relationship between NBS and NSA. However, available evidence adequately explains how government agencies worked as part of a consortium to develop the first encryption standard.

Text from the April 1981 Federal Information Processing Standard 74 (FIPS PUB 74), Guidelines for Using and Implementing the NBS Data Encryption Standard, shows that NBS had the responsibility and authority to take the lead in the development of data encryption technology and standards:

NBS has the responsibility for developing Federal Information Processing Standards through Public Law 89[-]306 and Executive Order 11717. The Institute for Computer Sciences and Technology (ICST) has the responsibility within the NBS to recommend and coordinate standards and guidelines for improved computer utilization and information processing within the Federal Government, as well as for developing the technology needed to support these standards activities. Because of the unavailability of general cryptographic technology outside the national security arena, and because security provisions, including encryption, were needed in unclassified applications involving Federal Government computer systems, NBS initiated a computer security program in 1973 which included the development of a standard for computer data encryption. Since Federal standards impact on the private sector, NBS solicited the interest and cooperation of industry and user communities in this work.²²⁶

²²⁶ U.S. Department of Commerce, National Bureau of Standards, Guidelines for Using and Implementing the NBS Data Encryption Standard, Federal Information Processing Standard 74 (Washington, D.C., April, 1981), 7.

While the 1973 initiation date mentioned in FIPS PUB 74 corresponded with the initial DES solicitation found in the May 1973 *Federal Register*, the initiation date does not match the 1972 date found in the 2001 Centennial Celebration document published by the National Institute of Standards and Technology (NIST).²²⁷ Such a mistake points to the diffuse beginnings of the Data Encryption Standard that are now being forgotten.

However, the critical information found in FIPS PUB 74 was an admission of the “unavailability of general cryptographic technology outside the national security arena” during the early 1970s. Since NSA did not volunteer an encryption solution, NBS used the expertise of NSA in adapting an encryption solution from IBM. The technical expertise of NSA influenced NBS, but did not lead to the domination of one federal agency over another.

The IBM Lucifer algorithm served as a technical baseline that prevented NSA from dominating NBS, because consensus was required among IBM, NBS, and NSA before large changes could be made. One of the biggest controversies allegedly pointing to NSA dominance was the selection of a 56-bit encryption key for DES instead of the 112-bit key found in an earlier algorithm developed by IBM.²²⁸ Pundits claimed that this selection seriously weakened DES to allow for domestic surveillance by NSA. Aside from legal issues that prevent NSA from spying on United States citizens, basic

²²⁷ William E. Burr, “Data Encryption Standard,” in *A Century of Excellence in Measurements, Standards, and Technology: A Chronicle of Selected NBS/NIST Publications 1901-2000*. NIST Special Publication 958, ed. David R. Lide (Washington D.C.: GPO, January 2001), 250-253.

²²⁸ Arthur Sorkin, “Lucifer, a Cryptographic Algorithm,” *Cryptologia* 8, no. 1 (January 1984): 25. The article analyzes the 128 bit Lucifer algorithm, but only 112 bits of the key were effective as 16 bits were used as check bits.

engineering and practical implementation concerns show that the original IBM 112 bit encryption key was not cost effective. Since DES handles 64-bit chunks of data as a single block, a cost effective key size would be around 64-bits. For practical reasons, the developers halved the IBM specified 112-bit key to produce a reasonable 56-bit key.²²⁹ FIPS PUB 74 depicts a practical argument for the size of the DES encryption key by describing a hardware DES test device that uses one row of 16 four-bit or hexadecimal thumb wheels to set the DES encryption key and a second row of 16 hexadecimal thumb wheels to set the data block:

A separate unit was built to operate the DES device manually. This unit has two sets of 16 rotary thumbwheel switches: 16 for the data and 16 for the key. Each switch has 16 positions: hexadecimal digits 0-9 and A[-]F. These allow 64-bit entry of key, plaintext, and cipher into the DES device. The test unit also contains control buttons and binary switches to provide the control signals necessary for operating the DES. The test unit is only used for off-line demonstrations of the DES device and for maintenance testing.²³⁰

Figure 4-3 shows a pictorial rendition of such a test device. This simple and efficient use of hardware would be difficult to achieve with a 112-bit encryption key, as the key would require 32 thumb wheels to implement, take longer to process, and provide little extra security for the expected lifetime of DES.

²²⁹ If the data in a block produced all combinations of 64 bits, then there would be 2^{64} or 1.85×10^{18} combinations possible. Since encryption keys provide a one-to-one mapping of data blocks to encrypted blocks, an optimum encryption key would be 64-bits in length and would supply 1.85×10^{18} keys. However, in the 1970s, FISP PUB 1 specified the use of 7-bit ASCII characters to represent digital data. Eight ASCII characters can fit in a 64-bit data block when a parity bit is added to each 7-bit ASCII character. Since most standard text documents can be generated from 72 different characters (52 upper and lower case letters, 10 digits, and about 10 characters for punctuation and currency designators), the number of different input blocks is 72^8 or 1.4×10^{15} . The 56-bit DES key provides 7.2×10^{16} different keys, which is a number that exceeds the normal number of different input blocks. Thus, the 56-bit DES key length was optimum for simple implementations of DES and character sets.

²³⁰ NBS, Federal Information Processing Standard 74, 15.

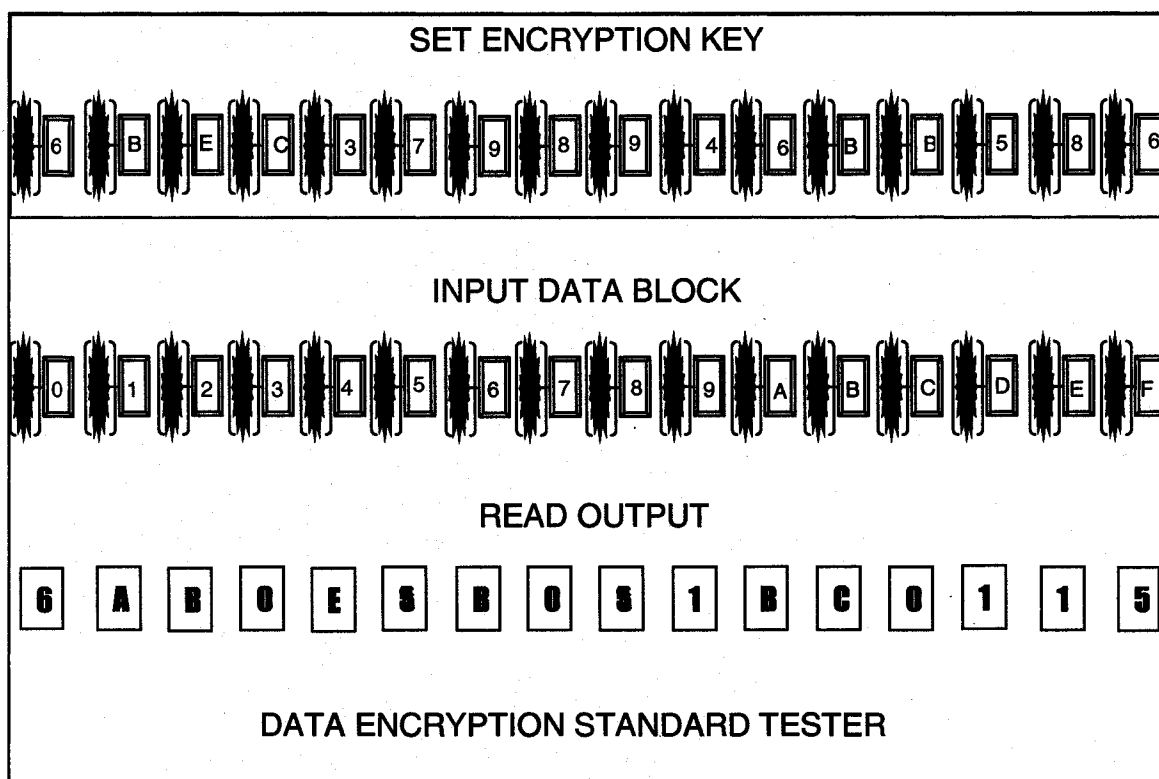


Figure 4-3 Author's rendition of a digital encryption standard test device, which illustrates the practical aspect of reducing the key size to fit on 16 thumb wheels instead of the 32 suggested by IBM's original design.

The National Security Agency garners suspicion whenever it provides technical expertise to academia, industry, or other government agencies. NSA sent a letter to the *Houston Chronicle* in 1992 to allay fears that the United States government was tampering with, weakening, or restricting encryption as to allow eavesdropping by United States intelligence agents. With respect to tampering during the development of DES, NSA's denial to the *Houston Chronicle* was consistent with NSA's 1978 congressional testimony on the subject:

Regarding the Data Encryption Standard (DES), we believe that the public record from the Senate Committee for Intelligence's investigation in 1978 into NSA's role in the development of the DES is responsive to your question. That committee report indicated that NSA did not tamper with the design of the algorithm in any way and that the security afforded by the DES was more than adequate for at least a 5-10 year time span for the unclassified data for which it was intended. In short, NSA did not impose or attempt to impose any weakness on the DES.²³¹

The strongest evidence that supports this denial of tampering by NSA comes from the fact that DES is the most analyzed encryption algorithm in the world because of its longevity and popularity. After three decades, DES has not been defeated through crypto-analytical efforts short of trying all the encryption keys.

The cooperative action of two diverse federal agencies in the development of a new type of government standard matched Allison's OBM organizing concept of "Organizational Actors," where a "constellation of loosely allied organizations" works together on a mutually important project.²³² After realizing that a rational competition among information technology vendors was not possible, NBS and NSA followed their organizational behaviors and worked with IBM to develop the Data Encryption Standard. I therefore assigned a Lead Actor valance of "1" to the Government Agencies group for using a consortium approach in developing the Data Encryption Standard.

²³¹ Michael S. Conn, Chief Information Policy, National Security Agency, Letter to Joe Abernathy, *Houston Chronicle*, 10 June 1992. Available at <
http://www.epic.org/crypto/dss/nsa_abernathy_letter.html>, accessed May 2004.

²³² Allison and Zelikow, *Essence of Decision*, 166.

B. Problem Perception Valance

The National Bureau of Standards perceived the information security problem as being a composite problem that affected both non-defense government and private sector computer users. In May 1973, the same month as Feistel's *Scientific American* article, NBS ran a solicitation notice in the *Federal Register* titled "Cryptographic Algorithms for Protection of Computer Data during Transmission and Dormant Storage." NBS used the following text in their notice to describe the problem:

Over the last decade, there has been an accelerating increase in the accumulations and communications of digital data by the government, industry and by other organizations in the private sector. The contents of these communicated and stored data often have very significant value and/or sensitivity. It is now common to find data transmissions which constitute funds transfers of several million dollars, purchase or sale of securities, warrants for arrest or arrest and conviction records being communicated between law enforcement agencies, airline reservations and ticketing representing investment and value both to the airline and passengers, and health and patient care records transmitted among physicians and treatment centers.²³³

The text indicates that NBS initially perceived the problem as protecting the vulnerability of digital data in both the government and private sectors. This perceived scale and scope of the problem made it a composite problem, as the phrase "government, industry and by other organizations in the private sector" included two sectors. The perceived problem was not complex, as NBS did not consider the international aspects of allies and hostile foreign powers using an encryption solution developed by the United States government.

²³³ U.S. Department of Commerce, National Bureau of Standards, "Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage; Solicitation of Proposals," *Federal Register* 38, no. 93 (15 May 1973): 12763.

The activities of the NBS during the next two years also suggest that the perceived information security problem was composite.

In August 1974, which was fifteen months after their initial solicitation, NBS dramatically reduced their perception of the information security problem by removing the private sector piece. In a re-solicitation notice published in the *Federal Register*, the NBS used the following text to focus on half of the original data protection problem: "Under the provisions of Pub. L. 89-306 and Executive Order 11717, the Secretary of Commerce is authorized to establish uniform Federal ADP [automatic data processing] Standards. NBS plans to publish, in the near future, an algorithm for computer data encryption as a standard for use by Federal agencies."²³⁴ As noted in the "Foundation and Theory" chapter, the 1965 *Brooks Act* (PL 89-306) charged the Secretary of Commerce with advising the President on automatic data processing standards. Executive Order 11717 subsequently gave the Secretary of Commerce the authority to develop automatic data processing (ADP) standards. Since the NBS is an organization under the Department of Commerce, the specification of "Federal agencies," as being the primary beneficiaries of an encryption standard, focused NBS on a piece of a composite problem that matched its authorized jurisdiction. NBS maintained this problem perception even though a first-ever encryption standard would affect the all of the federal government, the private sector, and eventually the global technology community.

²³⁴ U.S. Department of Commerce, National Bureau of Standards, "Encryption Algorithms for Computer Data Protection; Reopening of Solicitation," *Federal Register* 39, no. 167 (27 August 1974): 30961.

Twenty-two months after publishing their initial solicitation notice, NBS again changed their perception of the information security problem. In a March 17, 1975 *Federal Register* notice, the NBS requested comments on what it termed a "Data Encryption Algorithm." The notice used the following text, which narrowed their problem perception to domestic issues only: "[C]ryptographic devices and technical data relating to them may come under the export controls of Title 22, Code of Federal Regulations, Parts 121 through 128."²³⁵ As Title 22 applies to the Department of State, NBS was not responsible for potential problems incurred by federal and private sector entities that exported and imported the devices containing the Data Encryption Algorithm. This NBS transfer of responsibility to the Department of State was problematic, as NBS had already published the technical schematics and essential details for the Data Encryption Algorithm in their *Federal Register* notice. Thus, NBS's publication of an encryption standard solved their part of a composite problem, but created problems for actors in the executive branch.

The August 1, 1975 proposed Data Encryption Standard (DES) published in the *Federal Register* further supports the claim that NBS perceived a composite information security problem. Twenty-eight months after their initial solicitation, NBS added another piece to their original "non-defense government use" scope statement, which now included protecting unclassified data. This expansion in scope allowed the government sector, including the Department of Defense, to use DES. This expansion also allowed

²³⁵ U.S. Department of Commerce, National Bureau of Standards, "Encryption Algorithm for Computer Data Protection: Request for Comments," *Federal Register* 40, no. 52 (17 March 1975): 12134.

NBS to enter into a domain previously reserved for NSA. The proposed standard used the following text in its Applicability section:

Applicability. The Data Encryption Standard will be used by Federal agencies for protecting unclassified computer data when the responsible authority for the data or the computer systems of that agency has stipulated that cryptographic protection is required. Data that is considered sensitive by the responsible authority or data which has a high value or represents a high value should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or dominant storage.... This standard is not applicable for the cryptographic protection of computer data that is classified according to the National Security Act of 1947 or the Atomic Energy Act of 1947, as amended. Provisions of these Acts and their implementing regulations specify the means for protecting classified data."²³⁶

The term "unclassified computer data" was defined by NBS to mean "sensitive" data that could use DES for protection. According to the proposed standard, DES was not to be used in protecting classified data, but NBS provided no rationale on why DES was unsuitable for protecting such data. A possible explanation is that there was a tacit agreement between NBS and NSA to maintain separate unclassified and classified information encryption domains. Thus, the final 1977 Federal Information Processing Standard for DES was applicable for use in protecting all unclassified federal government data.²³⁷ By restricting the scope of their solution to only unclassified data, the NBS solved a piece of a composite problem. The use of DES to protect only unclassified information and the apparent reluctance of NBS to challenge the classified information security domain held by NSA cast suspicion upon the security of DES. The uncovered

²³⁶ U.S. Department of Commerce, National Bureau of Standards, "Federal Information Processing Data Encryption: Proposed Standard," *Federal Register* 40, no. 149 (1 August 1975): 32396.

²³⁷ U.S. Department of Commerce, National Bureau of Standards, *The Data Encryption Standard (DES)*, Federal Information Processing Standard Publication 46 (Washington, D.C., July 1977).

evidence explains this suspicion simply by noting that NBS selected parts of a composite problem that it perceived to be under NBS jurisdiction and did not pursue parts that infringed upon other government organizations such as NSA.

The selection of a problem scope by NBS and NSA to stay within their authorities matched Allison's OBM organizing concept of "Factored Problems and Fractionated Power."²³⁸ In this case, an organization selects a piece of the whole problem that best suits its organizational power and that fits within its area of primary responsibility. NBS saw the problem as the protection of unclassified digital information used by the government. NSA saw the problem as helping a peer federal agency with technical advice. I therefore assigned a Problem Perception valance of "1" to the Government Agencies Group for perceiving a composite problem.

C. Favored Alternative Valance

During the four plus years required to develop the Data Encryption Standard, actors in the Government Agencies Group explored several paths toward using a government standard to solve the information security problem. The text in the 1973 *Federal Register* solicitation notice indicates that the NBS did not originally envision a solution that required a government encryption standard:

The National Bureau of Standards under Department of Commerce
authorities and responsibilities for fostering, promoting, and developing U.S.
trade and commerce, and based on the National Bureau of Standards

²³⁸ Allison and Zelikow, *Essence of Decision*, 166.

responsibility for the custody, maintenance, and development of the National standards of measurement, and the provision of means and methods for making measurements consistent with those standards, solicits proposals for algorithms for the encryption of computer data to ensure their protection during transmission over exposed communication facilities or while recorded on media and in transport or in storage. It is the intent of the NBS to collect the submitted algorithms, select those suitable for commercial and nondefense government use and to publish guidelines relative to employing encryption.”²³⁹

The important words in this text describe the responsibilities of the NBS as being “the custody, maintenance, and development of the National standards of measurement.” The development of a digital data encryption standard deviated significantly from prior NBS work on digital measurement technologies, such as their test algorithms for the performance measurements of FORTRAN and COBOL programming compilers.²⁴⁰ Therefore, the original NBS solicitation appeared to be the start of an expedition to “collect the submitted algorithms, select those suitable for commercial and nondefense government use and to publish guidelines relative to employing encryption.” Such activities had little to do with developing standards of measurement.

Subsequent evidence indicates that NBS officially came about the encryption standard solution in 1974, but had been working on the information security problem with IBM well before this date. Working under the assumptions that NBS had little capability to develop an encryption algorithm on its own and that NSA would not submit a military encryption algorithm for civilian use, NBS had to wait until a private sector

²³⁹ NBS, “Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage; Solicitation of Proposals,” *Federal Register* 38; 12763.

²⁴⁰ John Cugini, “FORTRAN test programs,” in *A Century of Excellence in Measurements, Standards, and Technology: A Chronicle of Selected NBS/NIST Publications 1901-2000*. NIST Special Publication 958, ed. David R. Lide (Washington D.C.: GPO, January 2001), 258-259.

encryption algorithm became officially available to serve as a developmental basis for a new type of standard. In March 1974, the United States Patent and Trademark Office awarded separate patents to John Lynn Smith and to Horst Feistel for the elements and ideas of a digital cryptographic system. USPTO assigned both patents to the IBM Corporation.²⁴¹ Although the USPTO and NBS are organizations that operate within the Department of Commerce, the NBS would not have known about the details of Smith and Feistel's patent applications filed in 1971.²⁴² However, the movement of employees and ideas among NBS, NSA, and IBM suggests that all parties working on DES knew of the technology and pending patents. The August 27, 1974 *Federal Register* re-solicitation notice for encryption algorithms by the NBS came four months after the March 1974 patent awards. This timing indicates that NBS had previously planned to adapt the encryption technology found in IBM's patents and waited for IBM to receive its patents.

The 1974 NBS re-solicitation notice contained the following text that describes their envisioned solution:

Because of the significant value or sensitivity of communicated and stored data, the need for adequate protection of this data from theft and misuse has become a national issue. It is generally recognized that encryption represents a primary means of protecting data during transmission and a useful means of protecting stored data, provided that encryption techniques of adequate strength are devised, validated and integrated into a system's architecture. In order to insure

²⁴¹ John Lynn Smith, "Recirculation Block Cipher Cryptographic System," U.S. Patent # 3,796,830, 12 March 1974. Filed on 2 November 1971.

Horst Feistel, "Block Cipher Cryptographic System," U.S. Patent # 3,798,359, 19 March 1974. Filed on 30 June 1971.

²⁴² The USPTO normally keeps the contents of patent applications confidential until award, even from other federal agencies. I confirmed this with Dr. Edward Webman <Edward.Webman@USPTO.GOV> of the USPTO in May 2003.

compatibility of secure data transfer methods among Federal government agencies and their suppliers of data, it is necessary to make available such an encryption standard and guidelines for its use.²⁴³

This text represents the first official government use of the term “encryption standard.” From the text, the purposes of this standard were to specify encryption algorithms of “adequate strength” and to “insure compatibility of secure data methods.” From this point on, encryption strength and compatibility requirements became objects of debate among decision makers and between implementation and regulatory organizations.

A 2001 centennial celebration document published by the National Institute of Standards and Technology (NIST) asserted that the Data Encryption Standard had its conceptual origin at least two years before the 1974 NBS re-solicitation notice: “In 1972, the NBS Institute for Computer Sciences and Technology (ICST) initiated a project in computer security, a subject then in its infancy. One of the first goals of the project was to develop a cryptographic algorithm standard that could be used to protect sensitive and valuable data during transmission and in storage.”²⁴⁴ As the *Federal Register* notices and patents pertaining to DES do not reference this preliminary work, my research could not substantiate NIST’s claim of development activities for a “cryptographic algorithm standard” prior to 1974.

In March 1975, NBS published a notice in the *Federal Register* that requested comments on a new type of government standard based on the design work of IBM. The

²⁴³ NBS, “Encryption Algorithms for Computer Data Protection; Reopening of Solicitation,” *Federal Register* 39: 30961.

²⁴⁴ Burr, “Data Encryption Standard,” 250-253.

Federal Register notice used the following text to name the candidate standard: "The following algorithm was received in response to these submissions and satisfies the primary technical requirements for the algorithm of a Data Encryption Standard."²⁴⁵ Thus, the NBS established a union between an encryption algorithm and a federal automated data processing (ADP) standard and called this new combination the Data Encryption Standard or DES. In an adjacent notice in the March 17, 1975 *Federal Register*, the NBS explained that DES was unlike a normal ADP standard:

In the normal case, the Department of Commerce establishes a performance standard which does not require the use of any patent in its implementation. In the present case, it is not possible to meet an urgent national security need for security in computer systems with a performance standard. Rather, it will be necessary to establish a design standard which requires the use of an algorithm. It is possible that the apparatus which implements and performs the algorithm may be covered by one or more domestic or foreign patents which are presently assigned to the International Business Machine Corp. or which may be subsequently obtained by IBM.²⁴⁶

The text suggests that NBS strongly sought a government ADP standard to solve a "national security need," even to the point of using a proprietary algorithm as the basis for this standard. As discussed earlier, some actors in the executive branch did not share this perception of a national security requirement.

The selection of an automated data processing standard by NBS matched Allison's OBM general proposition that "Existing Organized Capabilities Influence Government

²⁴⁵ NBS, "Encryption Algorithm for Computer Data Protection: Request for Comments," *Federal Register* 40, 12134.

²⁴⁶ International Business Machines Corp., "License Under Patents," *Federal Register* 40, no. 52 (17 March 1975): 12138.

Choice.”²⁴⁷ In the case of digital information security, NBS favored using a government standard that was cooperatively built using technology shared by IBM and advice from NSA. Automated data processing standards worked in the past, and NBS continued to follow this precedent. I therefore assigned a Favored Alternative valance of “1” to the Government Agencies Group for developing the Data Encryption Standard as their solution to the information security problem.

D. Timing Valance

The evidence suggests that actors from the Government Agencies Group made incremental and tacit decisions as they learned to solve the information security problem within organizationally derived constraints. The lack of a government technology solution; the close relationship among IBM, NBS, and NSA; and the selection of a deliberative and methodical development process were the main factors in the four-year development of the Data Encryption Standard. The initial solicitation by the National Bureau of Standards in the May 1973 *Federal Register* used the following text to highlight a pending information security problem:

The increasing volume, value and confidentiality of these records regularly transmitted and stored by commercial and government agencies has led to heightened recognition and concerns over their exposure to unauthorized access and use. This misuse can be in the form of theft or defalcations of data records representing money, malicious modification of business inventories or the

²⁴⁷ Allison and Zelikow, *Essence of Decision*, 176-177.

interception and misuse of confidential information about people. The need for protection is then apparent and urgent.²⁴⁸

From words in the text, a sense of urgency seemed genuine. However, the actions of NBS proved otherwise. Instead of pressuring the National Security Agency for available military and national security encryption solutions, NBS decided to solicit private sector solutions to the information security problem.

A lack of private sector candidates blocked NBS's plan to select an optimum solution and subsequently forced an incremental approach. While Feistel's May 1973 *Scientific American* article publicly signaled the availability of an encryption solution from IBM, the May 1973 NBS solicitation did not yield the desired number of alternatives from other information technology companies. Thus, NBS decided to re-solicit algorithms in August 1974 with a *Federal Register* notice titled "Encryption Algorithms for Computer Data Protection; Reopening of Solicitation." The timing and text of the re-solicitation notice suggests that NBS was still planning to make a rational choice among competitive submissions:

In order to ensure that a full opportunity to submit algorithms for consideration is accorded to all parties, and due to the currency, timeliness and pertinence of the effort, NBS is reopening the initial solicitation for these algorithms described in the May 15, 1973 Federal Register notice. Computer data encryption algorithms and comments relative to the publication of such a standard and guidelines for usage are hereby solicited.

²⁴⁸NBS, "Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage; Solicitation of Proposals," *Federal Register* 38: 12763.

Responses to this solicitation should be submitted to the Director, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington D.C. 20234 on or before September 26, 1974.²⁴⁹

However, the text from the August re-solicitation notice shows that a short one-month interval was allowed for new submissions and suggests that NBS had tacitly decided to use an encryption solution from a single vendor. Figure 4-4 shows these events.

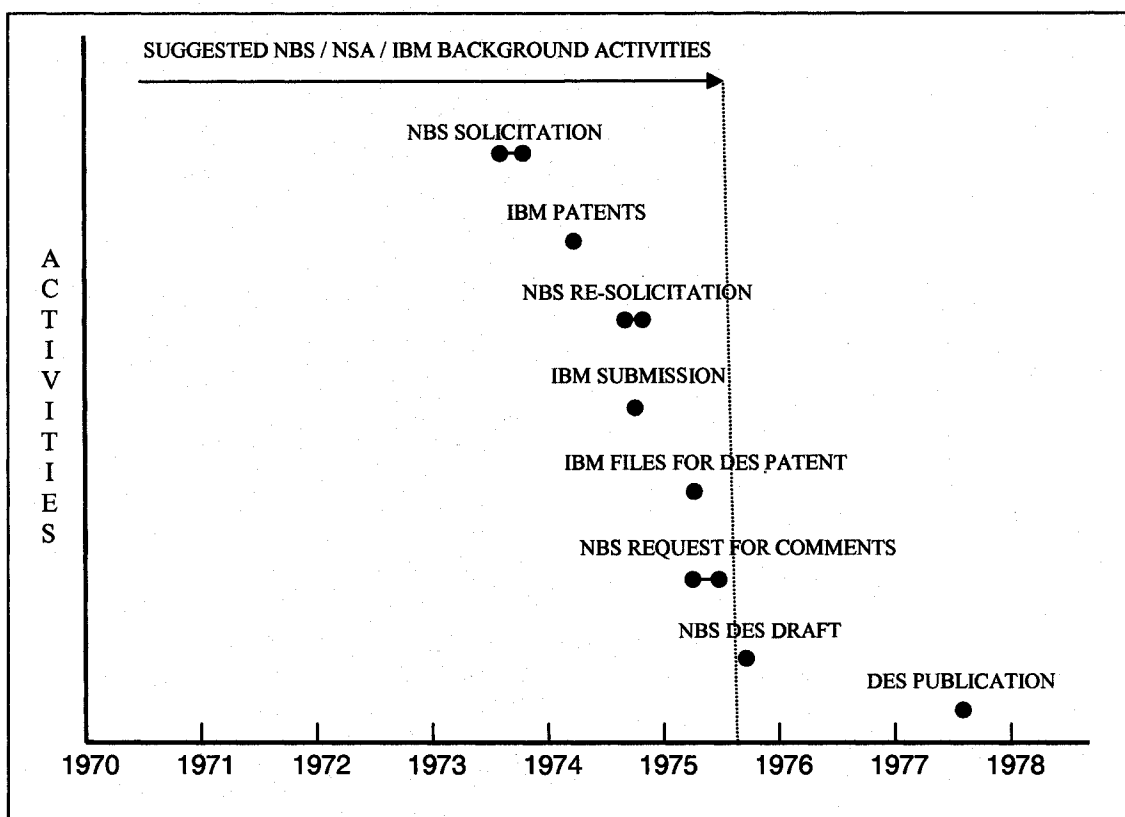


Figure 4-4 Timeline of NBS and IBM activities leading up to the publication of DES

²⁴⁹ U.S. Department of Commerce, National Bureau of Standards, "Encryption Algorithms for Computer Data Protection; Reopening of Solicitation," *Federal Register* 39, no. 167 (27 August 1974): 30961.

The timing of the re-solicitation notice allowed IBM to submit their newly patented ideas officially to NBS one year after the end of the initial solicitation period. Figure 4-4 displays this timing. Two IBM patent awards in March 1974 provide evidence that NBS formally knew about the technical details of the IBM solution and decided to adapt this technology as the new data encryption standard.

A review of the 1971 patent filings by John Lynn Smith for a “Recirculation Block Cipher Cryptographic System” and Horst Feistel for a “Block Cipher Cryptographic System” suggests that there was a close technical relationship between IBM research and development efforts and NBS’s final DES specification.²⁵⁰ In addition, the patent filing dates suggest that NBS and IBM may have had several years to work together, unofficially and in the background, on encryption technology to solve the information security problem. Although the NBS re-solicitation notice would have allowed submissions from other vendors, the one-month extension period appeared to favor a submission by IBM.

The text and timing of a March 1975 *Federal Register* request for comments notice on the draft digital encryption standard suggest that IBM submitted a jointly developed encryption algorithm in September 1974 and that NBS cooperated with IBM’s desires to protect its property rights by waiting six months before asking for public comments:

²⁵⁰ John Lynn Smith, “Recirculation Block Cipher Cryptographic System,” U.S. Patent # 3,796,830, 12 March 1974. Filed on 2 November 1971.

Horst Feistel, “Block Cipher Cryptographic System,” U.S. Patent # 3,798,359, 19 March 1974. Filed on 30 June 1971.

Solicitations for computer data encryption algorithms were published by NBS in the *Federal Register* issues of May 15, 1973 (38 FR 1273) and of August 27, 1974 (39 FR 30961). The following algorithm was received in response to these submissions and satisfies the primary technical requirements for the algorithm of a Data Encryption Standard.²⁵¹

The statement that “the following algorithm was received in response to these submissions” suggests a rational and impartial process for the solicitation of candidate encryption algorithms. However, an engineering review of the submitted algorithm, as published in the March 1975 *Federal Register* request for comments notice, shows a near final product that had two significant improvements over the technology covered by IBM’s March 1974 patents. The first improvement was changing the number of different “S-boxes” or substitution boxes from two to eight. S-boxes are critical to transforming the plain text data into cipher text and their greater numbers are essential for the cryptographic strength of DES. The second improvement was the design of a key scheduler that uses parts of a 56-bit encryption key to control the data flow to these S-boxes. Both these improvements were found in IBM’s new patent application filed for in February 1975, a month before the request for comments notice.²⁵² This timing suggests that IBM may have been working with NBS and NSA from 1971, through the DES algorithm solicitation period, and past the March 1975 request for comments notice.

Timing inconsistencies further suggest that IBM, NBS and NSA worked together and made tacit decisions on DES before the August 1974 re-solicitation period. The

²⁵¹ U.S. Department of Commerce, National Bureau of Standards, "Encryption Algorithm for Computer Data Protection: Request for Comments," *Federal Register* 40, no. 52 (17, March 1975): 12134.

²⁵² William Friedrich Ehrtam, et al., "Block cipher system for data security," U.S. Patent # 3,958,081, 18 May 1976. Filed on 25 February 1975.

findings of an April 1978 report by the Senate Select Committee on Intelligence documented that the government participated in the modifications of IBM's algorithm to change the S-boxes and encryption key scheduler. According to the report, the government's participation, and thus modifications, occurred after the August 1974 re-solicitation notice.²⁵³ However, if the NBS claim about receiving a nearly complete encryption algorithm from IBM one month after the August 1974 re-solicitation notice is true, then all this engineering re-work had to have happened in a few weeks. This is unlikely. The event timings in Figure 4-4 suggest that a background activity period existed where IBM, NBS and NSA worked together until the draft standard was completed. This claim is consistent with information found in NIST's 2001 Centennial Celebration document, which describes a commingling of IBM, NBS and NSA employees during the early 1970s.²⁵⁴

The use of incremental and tacit decisions in the development of a new type of government standard matched Allison's OBM general proposition that "Implementation Reflects Previously Established Routines."²⁵⁵ NBS and NSA, following their standard operating procedures, made incremental decisions about developing the Data Encryption Standard. These actors also made tacit decisions on technical modifications to DES without waiting for results from the publicly advertised decision milestones. I therefore

²⁵³ Senate Select Committee on Intelligence, *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard*, Staff Report, 95th Congress, 2d sess., 1978, Committee Print, 1-4.

²⁵⁴ Burr, "Data Encryption Standard," 250-253.

²⁵⁵ Allison and Zelikow, *Essence of Decision*, 176-177.

assigned a Decision Timing valance of “1” to the Government Agencies Group for using incremental and tacit decisions in developing the Data Encryption Standard.

First Mover Period Summary

The four actor groups investigated during the First Mover Period undertook actions and exhibited behaviors consistent with Allison’s decision models. In addition, these actions and assigned valances served to calibrate these models for subsequent analyses. Table 4-1 summarizes these findings and shows that the Congressional Group exhibited behaviors best described by the Governmental Politics Model and favored laws as political expedients to confront an overly powerful executive branch.

Table 4-1 First Mover Period Summary

Analysis Unit	Lead Actor	Problem Perception	Favored Alternative	Decision Timing	Allison Model
Congressional Group	2 government sector	2 complex	2 laws / regulations	2 urgent	GPM
Encryption Technology Group	0 private sector	0 simple	0 utility maximizing	0 contingent on choices	RAM
Executive Group	2 government sector	1 composite	1 precedents / routines	1 incremental / tacit	OBM GPM
Government Agencies Group	1 consortium	1 composite	1 precedents / routines	1 incremental / tacit	OBM

Only the Encryption Technology Group perceived a simple information security problem involving data protection, which they solved with emerging encryption

technology solutions. Their secret key encryption solution captured the first mover advantage and the Rational Actor Model best describes their actions. The Executive Group followed a pattern of behavior that was largely described by the OBM, but with a Lead Actor valance matching the Governmental Politics Model. The Executive Group, having to worry about national security issues and individual federal departments, favored using a dated United States Munitions List to control information security technology. Actors in the Government Agencies Group followed a pattern of behavior best described by the Organizational Behavior Model. Actors in this group favored encryption standards, but required help from the private sector, as the National Security Agency did not offer the use of its classified encryption algorithms. In the Competitive Period, actors in the Executive Group would attempt to steer the Government Agencies Group away from the influence of the Encryption Technology Group.

Competitive Period: 1987-1997

The Competitive Period spans eleven years and starts with the passage of the *Computer Security Act of 1987*. During this period, the use of computers or “automated data processing equipment” (ADPE) increased the productivities of the government and private sectors to such a dramatic extent that policymakers and users became concerned about accessing and securing the valuable digital information resident on these computers. The growth of the Internet and the connections of computers into the World Wide Web during this period created a network that simultaneously increased the amount of valuable information transacted by computer users and threatened the security of the same information. Government, individual, and commercial developers offered competitive secret and public key encryption subsystems to solve the digital information vulnerability problem and, in some cases, to allow national security and public safety access to protected information.

A competition between the federal government and the private sector based on national security, privacy, and economic concerns shaped encryption policy by creating disparate information security solutions available to computer users. Restrictive solutions favored by some actor groups limited the capabilities of encryption algorithms and required users to give the government access to their encryption keys. Other actor groups favored a choice of encryption solutions with computer users and the market

being the regulators of algorithms and access to keys. The creation of competitive choices between restrictive and liberal encryption solutions involved actors from the four analytical groups and required the expansion of the Encryption Technology Group to cover the emergence of electronic rights activists. These activists influenced the decision agenda by testifying at congressional hearings and by using the news media.

An examination of encryption events identified in contemporary magazines and newspapers published during the Competitive Period showed that there was a fight between the government sector and the private sector over the optimum extent of laws and regulations covering encryption technology. The *Computer Security Act of 1987* limited the ability of the government to create encryption policy by executive branch decisions. However, this law did give encryption standards the policy weight to be effective. Individual activists were aware of the power found in government standards and were able to affect the decision agenda on important aspects of encryption policy. These new actors in the Encryption Technology Group suspected that the government had an encryption control agenda such as the one manifested by the 1991 development of the Digital Signature Standard (DSS). DSS used public key encryption technology, but the government's development of an algorithm for digital signatures further deviated from the precedent set by the 1977 Data Encryption Standard. DSS development had limited involvement from the private sector, and the government enticed users to adopt DSS over competitive commercial standards. A 1991 *Wall Street Journal* article claimed that the National Institute of Standards and Technology "dealt a blow to efforts by U.S. computer and software makers to forge a standard for authenticating electronic

documents to protect them from tampering.”²⁵⁶ The article also claimed that NIST intended “to back an alternative approach it devised in a partnership with the National Security Agency, the federal agency in charge of electronic intelligence gathering.”²⁵⁷ In a reaction to the growing government control of public key encryption, computer scientist Philip Zimmermann gave a complete software-based encryption system to his friends for distribution. A *U.S. News and World Report* article lauded this event and the recognition given to Mr. Zimmermann by another member of the Encryption Technology Group: “This week, the Electronic Frontier Foundation, a cyberspace civil liberties organization, will give Zimmermann a prestigious Pioneer Award, for helping protect citizens’ privacy by creating a powerful encryption program called ‘Pretty Good Privacy’ (PGP) and making it available for free.”²⁵⁸ I will analyze the actions of the Encryption Technology Group, as the new actors in this group helped shape encryption policy.

Competing with the software encryption solutions championed by the private sector, the government’s novel solution to the encryption control problem was the Escrowed Encryption Standard (EES). A 1993 *Newsweek* article entitled “The Code of the Future: Uncle Sam wants you to use ciphers it can crack” declared that the government made a mistake in developing the Data Encryption Standard and claimed that the government really required a standard in which the “Feds alone would hold the

²⁵⁶ Staff Reporter, “U.S. Plan is Seen Hurting Electronic Data Standard,” *Wall Street Journal* 218, no. 2 (9 July 1992) Eastern Edition: A4.

²⁵⁷ *Ibid.*, A4.

²⁵⁸ Vic Sussman, “Lost in Kafka territory: The feds go after a man who hoped to protect privacy rights,” *U.S. News and World Report* 118, no. 13 (3 April 1995): 32.

keys.”²⁵⁹ This article showed that Congress was not successful in preventing the developers of federal encryption standards from making encryption policy. The National Bureau of Standards’ newly developed EES produced two polar policy effects. One effect, as seen from national security and public safety perspective, was the long-awaited availability of a technical solution to solve the problems of digital information protection and allowing government access to this information. The opposite effect, as seen from the privacy rights perspective, was the pending imposition of government surveillance upon all computer users. I will analyze the actions of the Congressional Group and Government Agencies Group in managing the effects caused by the development of EES and an encryption control precursor, the Digital Signature Standard.

During this period, actors in the Encryption Technology Group worried about the international and domestic competitiveness of EES and other proposed government schemes to access protected information. The administration’s leader on technology issues, Vice President Al Gore, first championed EES and then other encryption solutions that permitted government access to information. A 1996 *Newsweek* article questioned the viability of the administration’s policy requirements to “preserve both privacy and digital wiretapping.”²⁶⁰ This article also introduced the idea that EES could cause economic damage to domestic encryption companies. Jim Bidzos, then head of RSA Data Security, believed that the government was hurting the information technology

²⁵⁹ Sharon Begley, Melinda Liu and Joshua Cooper Ramo, “The Code of the Future: Uncle Sam wants you to use ciphers it can crack,” *Newsweek* 121, no. 23 (7 June 1993): 70.

²⁶⁰ Steven Levy, “Trying to Find the Key,” *Newsweek* 128, no. 16 (14 October 1996): 91.

industry: “[I]t’s quite possible that within two years, such foreign competitors, not bounded by U.S. export laws, will steal the market from American companies.”²⁶¹ I will analyze the actions of the Executive Group in balancing national security and public safety requirements against economic and information technology leadership losses.

Congressional Group

In the Competitive Period, the primary actor in the Congressional Group was Congress as a whole in passing the *Computer Security Act of 1987*, the *Communications Assistance for Law Enforcement Act* in 1994, and the *Economic Espionage Act of 1996*. These laws challenged the dominance of the executive branch in controlling information for national security and public safety purposes and reasserted an information control policy that favored privacy rights and economic vitality. By denying the executive branch and federal agencies the required statutory tools to control dual-use technologies such as encryption, the legislative branch alone could have determined policy by passing an encryption liberalizing law with enough support to override a possible veto.

However, members of Congress were ambivalent about sacrificing national security and public safety for information privacy and economic health. The failure of Congress to pass proposed technology export legislation was in part caused by the divisive nature of the encryption control problem. In addition, the failure of Congress to pass proposed encryption liberalization legislation was caused by a lack of urgency, as the

²⁶¹ *Ibid.*, 91.

administration's encryption control plans were indecisive and were not immediate political drivers. Other active members of the Congressional Group during this period were the research services and congressional committees that helped Congress investigate information age problems and gain consensus on proposed legislation. The text of these laws and proposed legislations, the *Congressional Record*, committee reports, and commissioned studies provided the data for analyzing the actions of the Congressional Group. I analyzed this data according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

Actors in the Congressional Group believed that it had the responsibility to check the growing power of the executive branch in the area of information control. Information in databases that allegedly could be computer-processed into classified information was an issue of contention with Congress. Congress did not believe that routine information collection and management activities in the government and private sectors could jeopardize public safety and national security. In a manner similar to the data privacy issue of the last period, actors in the Congressional Group realized that the executive branch was taking the lead in controlling digital information in both sectors. During a subcommittee hearing on the *Computer Security Act of 1987*, H.R. 145, Chairman Jack B. Brooks (D-Texas) questioned the government's information control policy and acceptance of the new information age:

And the world right now is in a period that some refer to as the information age. During our lifetimes, the rapid advance in the ability to collect, process, and disseminate information has had as far-reaching an effect in our world as the industrial revolution had on the world of our forebears.

Unfortunately, there are those who fear this change. They believe that the unbridled development and use of new technology will lead us into uncertain ventures. As a result, some would turn their backs on America's commitment to innovation and progress and cloak many of our advances in secrecy and deny access to them by a large part of our population.

We cannot allow this fear to stifle our future. The challenge facing our government and our people is to strike a balance between the need to protect national security and the need to pursue the promise that the intellectual genius of America offers all of us.

H.R. 145 was developed in large part to ensure that this delicate balance is maintained and to respond to those in the national security establishment who have lost sight of this important principle.²⁶²

The text shows that the "ability to collect, process, and disseminate information" created "fear" in parts of the government. Representative Brooks, after whom the *Brooks Act* was named, saw the government's challenge as producing a law to balance information access and security. He saw the threat to this balance as originating from the "national security establishment" in the form of a 1984 National Security Decision Directive 145 (NSDD-145). Rear Admiral John Poindexter, the Assistant to the President for National Security Affairs, originated and expanded NSDD-145 to handle a new type of information.

²⁶² U.S. House, Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 100th Congress, 1st sess., 25-26 February and 17 March 1987, 1-2.

In the midst of the Iran-Contra Affair, actors in the Congressional Group believed that the executive branch had exceeded its authority to control information and were skeptical of the danger posed by unclassified digital information. NSDD-145 created a requirement to protect unclassified information, which when accumulated, processed, or compiled could jeopardize national security. With his testimony, Representative Glenn English (D-Oklahoma) focused the hearing on the primary cause of government over-control of common information:

As I begin, I want to make it clear that none of my testimony addresses questions of security for classified information. No one disputes the need for the high degree of protection for information that has been properly classified* in the interests of national defense and foreign policy. Classified information has been properly excluded from the scope of H.R. 145.

I believe that many of the problems being addressed at this hearing are the direct result of the lack of clarity in National Security Decision Directive 145. NSDD 145 introduced the elusive idea of sensitive but unclassified information the disclosure of which could adversely affect national security.

I do not understand the concept of unclassified national security information. Under the classification rules promulgated by President Reagan in 1982, federal agencies are required to classify any government information whose disclosure "could reasonable be expected to cause damage to national security."²⁶³

This text shows that organizations working in the executive branch created an information control policy that blurred the previously well-understood national security dichotomy of classified and unclassified information. Actors in the Congressional Group feared that the tools of information control, such as government-produced encryption,

²⁶³ *Ibid.*, 25-26.

would be used to limit access to “sensitive, but unclassified information” in both the government and private sectors.

Testimony from witnesses supported the claim that government security directives affected information security tools used in the private sector, despite claims to the contrary from the executive branch. Government agencies interpreting directives, such as NSDD-145, undertook actions that created uncertainty in the financial and service industries. These industries relied on government technical assistance and products to protect privacy and to secure commercially valuable information. In one case, Cheryl W. Helsing from the American Bankers Association specifically testified about the problems caused by the government when it changed encryption system requirements to protect a new category of information:

A striking example of this danger can be seen in how the NSA’s new Commercial Comsec Endorsement Program (CCEP) has impacted the financial industry. Banks have spent several years developing a new technique for assuring the integrity and authenticity of electronic funds transfers and other information that we call message authentication. At the same time, our industry began to make significant use of encryption to protect the privacy of information being stored in computers and transmitted over telecommunication facilities. Both these techniques employ the data encryption standard, more commonly known as DES, which was established by the National Bureau of Standards in 1977 and has been proven to be a reliable security technique.

Following NSDD-145, the National Security Agency announced a new set of encryption algorithms under CCEP and stated its intention of discontinuing existing DES equipment endorsed programs in January 1988. The attendant

publicity has caused widespread belief that DES is no longer a prudent safeguard, casting a shadow on our continued use of that technique.²⁶⁴

The text shows that the banking and finance industries were affected by NSDD-145 and sought regulatory stability from Congress to mitigate the effects of encryption systems required for the protection of new information control categories. Beyond regulatory stability, the private sector was also concerned about the cost and liability associated with protecting sensitive information and allowing the government to access such information.

H.R. 4922, the 1994 *Communications Assistance for Law Enforcement Act*, required that the private sector assist the government with legal surveillance activities necessary to ensure national security and public safety. Representative Brooks, as Chairman of the Committee on the Judiciary, played a critical role in having the private sector assist with court-ordered surveillance activities, while at the same time prevented the government from influencing encryption use in the private sector. In a report from the House Committee on the Judiciary, committee members produced an outline of government action required to update the *Electronic Communications Privacy Act of 1986* with allowances for law enforcement surveillance:

**CONGRESS MUST RESPOND TO THE "DIGITAL TELEPHONY"
REVOLUTION ...**

Therefore, the bill [H.R. 4922] seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly

²⁶⁴ *Ibid.*, 113.

powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.²⁶⁵

The text shows that H.R. 4922 would require a three-way balance and that privacy protection and technology advancements were valid government considerations. One way for actors in the Congressional Group to maintain a balance was to curtail law enforcement's expectation for a law directing government encryption control:

Finally, telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it. This obligation is consistent with the obligation under 18 U.S.C. Section 2518(4). Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications.²⁶⁶

The text uses a careful argument in that it would be legal for a carrier to sell encryption services without a key recovery feature. Thus, law enforcement officials would have to find another way to recover the encryption keys of suspected criminals that would presumably hide their keys. However, as commercial encryption certificate providers would normally hold the encryption keys of average users, H.R. 4922 used economic incentives to compensate service providers who assisted the government with decrypting information for court-ordered wiretaps. The economic concerns of the information services industry were again paramount when Congress tried to pass export control legislation.

²⁶⁵ House Committee on the Judiciary, *Telecommunications Carrier Assistance to the Government*, 103rd Congress, 2d sess., 4 October 1994, Report 103-827, Part I, 12-13.

²⁶⁶ *Ibid.*, 24.

Congress was under pressure to pass the proposed *Export Administration Act of 1996*, H.R. 361, because prior export control legislation had lapsed in 1994. This lapse allowed the executive branch to regulate exports through executive orders and without the legal support provided by legislation. During the floor debate, Representative Tom Campbell (R-California) argued that someone in government should help domestic industry with information technology exports:

My second and last point is that the bill should have done more on encryption and so I will take the remaining minute to say that I am hopeful that even possibly within this Congress there may be a way to address encryption, possibly our colleague from Washington State's own bill on encryption, Mr. WHITE, possibly an amendment as this bill goes into conference. The administration can do a whole lot on its own regarding the export of encryption software and hardware. Simply by reclassifying this a dual-use rather than munition, it would bring its review process out of the State Department and over to commerce where I think it would be much more realistic.

The importance of the encryption export is not simply in its own right as a market for American entrepreneurship and or research and development, but also this: As more and more computers are being used in commerce and as we go to virtual banking and international finance, the ability to encrypt is going to be an essential part of any computer system you buy. If American computers cannot have embedded in them reliable encryption, then nobody is going to buy the computer system. And then we move from a loss of maybe a billion or two to tens of billions of dollars. Indeed, the computer systems policy project estimates a \$60 billion loss to our country by the year 2000.²⁶⁷

H.R. 361 did not pass, and the text shows that it was Congress' job to legalize encryption exports or stand to lose "tens of billions of dollars." The text also shows that Congress had come to rely on the administration to do "a whole lot on its own regarding the export of encryption." This reliance was problematic as the Clinton administration and a

²⁶⁷ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 104: H7587.

primarily Republican Congress often agreed that government leadership was necessary, but disagreed on the policy direction. Actors in the Congressional Group exhibited their traditional foreign policy weakness in creating export laws, but did better with legislation on limiting international theft and destruction of domestic information by criminals and foreign operatives.

The *Economic Espionage Act of 1996*, H.R. 3723, provided a mechanism for both the House and Senate to shape government information control policy, and this law specifically mentioned the use of encryption in espionage. Although the Senate amended H.R. 3723 with numerous riders, such as establishing the Boys and Girls Clubs of America, one significant amendment was the Senate's incorporation of S. 982, the *National Information Infrastructure Protection Act of 1995* into H.R. 3723.²⁶⁸ In the Senate Committee on the Judiciary's report on S.982, Senator Orrin G. Hatch (R-Utah) discussed the shortcomings of existing laws on crimes affecting the information infrastructure:

Thus, the current provision falls short of protecting government and financial institutions computers from intrusive codes, such as computer "viruses" or "worms." Generally, hacker intrusions that inject "viruses" or "worms" into a government or financial institution computer system which is not used in interstate communications is not a Federal offense. The NII Protection Act would change that limitation and extend Federal protection from intentionally damaging viruses to government and financial institution computers, even if they are not used in interstate communications.²⁶⁹

²⁶⁸ *Economic Espionage Act of 1996, U.S. Statutes at Large* 110 (1997): 3497.

²⁶⁹ Senate Committee on the Judiciary, *The National Information Infrastructure Protection Act of 1995*, 104th Congress, 2nd sess., August 27, 1996, 10.

The text shows that the Senate was looking for an avenue to increase “Federal protection” of both government sector and business sector computers. This notional coupling of virtually all computers as being parts of a single information infrastructure represented an emerging view that criminal activities and espionage against the economic and information power of United States were equivalent to an attack on national security. Thus, actors in the Congressional Group viewed information protection as a government function.

The view of the government as the lead actor by the Congressional Group matched Allison’s GPM organizing concept of “What is the game?”²⁷⁰ Actors in the Congressional Group used “action channels” or “regularized means of taking governmental actions.”²⁷¹ Representative Brooks and his House Committee on the Judiciary, along with the Senate Committee on the Judiciary, were two of the action channels used by Congress to counter the executive branch’s control of information and encryption technology. The failure of export legislation indicated that some action channels could not develop support from the broader Congress, because important aspects of this legislation were sacrificed to gain committee consensus. I assigned a Lead Actor valance of “2” to the Congressional Group for being the government lead in solving the information security and information infrastructure protection problems.

²⁷⁰ Allison and Zelikow, *Essence of Decision*, 300.

²⁷¹ *Ibid.*, 300.

B. Problem Perception Valance

Actors in the Congressional Group perceived the information control issue as a complex problem affecting the government and the private sectors. Divergent congressional and executive branch views on the control of sensitive digital information added to this complexity. In addition, actors in the Congressional Group believed that the international effects of a broad information control policy favoring national security would be harmful to exports, the economy, and technology leadership. Representative Brooks, in a committee hearing on H.R. 145, the *Computer Security Act of 1987*, claimed that the national security establishment was largely to blame for making information security a complex problem. The committee questioned the issuance of NSDD-145 that created the category of “sensitive but unclassified information” and the subsequent broadening of this category by National Security Advisor Poindexter:

Now taken together, these actions reflect an unprecedented expansion of the military’s influence into our society, which is unhealthy politically and potentially very dangerous. Clearly, the basement of the White House and the back rooms of the Pentagon are not places in which national policy should be developed. This issue should be debated and fully aired in public hearings. In my view, it is critical that Congress reestablish civilian control over the Federal computer security program.²⁷²

The text indicates that Congress wanted to resolve complex information security issues between national security and unclassified information in a public manner. In the text, Chairman Brooks insinuated that President Reagan and his advisors should not determine

²⁷² Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 2.

information control policy, as they could not control the activities of the National Security Council staff during the Iran-Contra Affair. Beyond the national security and domestic effects caused by information control, witnesses at the hearing were also concerned about international effects.

The testimony of Jack Biddle, President of the Computer and Communications Industry Association, suggested that favoring national security concerns hurt the relationships among technology leadership, open flows of information, and economic success:

We are losing our world leadership in computer technology, because we are forfeiting our overseas markets because of DOD's fear that a blue box might slip through the Iron Curtain.

Then we see NSDD-145. And with that background of DOD paranoia clearly in our minds, it's rather frightening, because we can foresee the possibility that our scientists will not be able to communicate with each other to maintain a leading edge in technology, while the Japanese scientists will be conversing with each other in open forums.²⁷³

The text suggests that the executive branch's concern with controlling technical information, or "DOD paranoia," was hindering the economic potential of United States power. Mr. Biddle's testimony demonstrated the complex problem presented by the fungibility of power, whereby computer technology and open information flows could strengthen a service-based economy. A stronger economy could in turn support a stronger national defense establishment.

²⁷³ *Ibid.*, 367.

Congress sought more information on this complex relationship between national security requirements and information control by tasking the National Research Council (NRC) in November 1993 to study the problem. The preface of the NRC report used an excerpt from Public Law 103-160, *Defense Authorization Bill for Fiscal Year 1994*, to describe the scope of their study:

(a) Study by National Research Council.--Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall request the National Research Council of the National Academy of Sciences to conduct a comprehensive study of cryptographic technologies and national cryptography policy.

(b) Matters To Be Assessed in Study.--The study shall assess--

(1) the effect of cryptographic technologies on--

(A) national security interests of the United States Government;

(B) law enforcement interests of the United States Government;

(C) commercial interests of United States industry; and

(D) privacy interests of United States citizens; and

(2) the effect on commercial interests of United States industry of export controls on cryptographic technologies.²⁷⁴

The text shows the complexity of the problem by listing national security, law enforcement, commercial, privacy, and international economic areas as required study outputs. NRC published their findings in 1996, which was too late for congressional action in the 103rd Congress. The next Congress had to address national security and export problems created by advances in information technologies.

²⁷⁴ Kenneth W. Dam, and Herbert S. Lin, eds., *Cryptography's Role in Securing the Information Society* (Washington, D.C.: National Academy Press, 1996), ix.

Representative Tom Campbell's extended remarks on the proposed *Export Administration Act of 1996*, revealed the difficulty of updating United States export laws when challenged by international agreements and domestic controversy:

I have also expressed my concerns to Chairman Roth about the competitive disadvantage provision within the foreign availability section. I believe that there is a real danger that U.S. companies will suffer significant disadvantages within CoCom's successor, the new Wassenaar Arrangement, if the U.S. Government rigorously enforces the new internationally agreed upon export control lists while its allies and other nations within Wassenaar rubber stamp their licenses or give those licenses only cursory reviews.

I want to take time today, however, to discuss an omission from H.R. 361. That issue is encryption. It is not a part of H.R. 361, in part, because it is too controversial and might have killed the last chance that the bill has for passage during the 104th Congress. But within the category of export controls, encryption is the most important issue facing us today, and I believe that Congress would be abdicating its responsibility by not taking it up during the current session. By speaking today, I hope to build a record for early consideration of encryption legislation in the next Congress, or even for consideration in the remaining days of this Congress.²⁷⁵

The text shows that Representative Campbell was concerned about the complex relationship between H.R. 361's "foreign availability section" and the Wassenaar Arrangement that controlled exports of dual-use technologies from advanced countries. If other Wassenaar Arrangement members cheated, then the United States would be hurt economically and would suffer an increased national security threat. His remark that encryption was "too controversial and might have killed the last chance that the bill [had] for passage" provided a candid assessment on the fate of legislation incorporating the

²⁷⁵ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 104: H7587-8.

encryption control problem. When Congress needed to pass critical law enforcement legislation, the encryption topic was deliberately suppressed from open discussion.

Actors in the Congressional Group anticipated that law enforcement officials would encounter problems caused by advancements in information technology and changes in the telecommunications service sector. During the House debate on H.R. 4922, the *Communications Assistance for Law Enforcement Act*, Representative Michael G. Oxley (R-Ohio) spoke of these problems:

As a former FBI special agent, I know that the court-authorized interception of communications is one of our most important tools in the investigation of criminal conduct. By necessity, wiretaps are relied upon in the investigation of drug king pins, terrorists, and others who would use telecommunication networks to further their criminal ends.

Currently, the telecommunications industry is undertaking revolutionary changes in its technology, changes that make it impossible for police agencies to execute lawful court orders. In some cases, cellular technology and new digital features have already frustrated court-ordered wiretaps.²⁷⁶

The text shows that Representative Oxley specifically emphasized the importance of wiretapping to law enforcement investigations and mentioned the problems caused by “new digital features.” The problem of suspected criminals using encryption to hide their activities was not specifically mentioned in the floor debate.

The House Committee on the Judiciary report on H.R. 4922 framed the complex issue of satisfying surveillance requirements and maintaining privacy rights. One section

²⁷⁶ *Congressional Record*, 103rd Congress, 2d sess., 1994, 140, pt. 20: H27710.

of the report claimed, “Representatives of the telecommunications industry now acknowledge that there will be serious problems for law enforcement interception.”²⁷⁷

Another section discussed the requirements of law enforcement, but words relating to encryption and its protective and illegal uses did not appear in the discussion. A third section discussed privacy requirements in legislation and specifically mentioned that H.R. 4922 “does not limit the rights of subscribers to use encryption.”²⁷⁸ The framing of a complex problem with an encryption liberalizing solution perpetuated the surveillance problems encountered by the national security and law enforcement communities. It would take a change in the political environment before Congress could discuss this problem openly and fairly.

The failure of Representative Brooks’ 1996 reelection bid for his 22nd term signaled a change in Congress away from favoring privacy rights over national security and law enforcement requirements and a toward a more cautious position of investigating claims of encryption being used in criminal activities. During the Senate debate on the *Economic Espionage Act of 1996*, which the Senate had greatly amended to protect the national information infrastructure, Senator Chuck Grassley (R-Iowa), discussed his amendment:

I am particularly pleased that the Senate has accepted the amendment I offered with Senator KLY. The amendment commissions the first-ever study on the criminal misuse of encryption technologies....

²⁷⁷ House Committee on the Judiciary, *Telecommunications Carrier Assistance to the Government*, 15.

²⁷⁸ *Ibid.*, 18.

As chairman of the Oversight Subcommittee on the Judiciary Committee, I did an informal survey of state-level law enforcement concerning the criminal misuse of encryption. This informal survey, while not scientific, provides valuable insights into the actions of the criminal element in our society....

Ivan Ortman, a senior prosecutor in Seattle, Washington, encountered some encrypted files and password protection in a cellular phone fraud investigation. For a number of files the popular and inexpensive "PGP" type of encryption was used. Orton indicated that no effort was even made to examine the files as the police could not locate any method for "cracking that encryption."²⁷⁹

The text shows that for the first time, the Senate was made aware of the complex problem posed by information technology designed to protect privacy, but instead used to further criminal activities. Although Senator Grassley produced several examples of the negative externalities of encryption, no further amendments were offered to support the administration's effort to use a key escrow solution that would have alleviated this problem.

The view of a complex problem by actors in the Congressional Group again matched Allison's GPM organizing concept of "Goals and Interests" where "officials can frequently disagree about how broad national goals bear upon a specific issue."²⁸⁰ In the complex information control problem, this group favored economic gains and technology leadership over controlling information technology such as encryption. Even when faced with evidence on the negative externalities of encryption use, this group believed that a study was needed before specific legislation would be considered. Prevailing congressional views, that the administration's information control regulations covered too

²⁷⁹ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 129: S10883.

²⁸⁰ Allison and Zelikow, *Essence of Decision*, 298.

many sectors and that an encryption control solution was premature, did not prevent Congress from perceiving its own complex information control problem. Congress perceived the problem as having multiple aspects, such as maintaining international technology leadership, assisting law enforcement activities, enhancing exports, and protecting the information infrastructure of the government and private sectors. I therefore assigned a Problem Perception valance of “2” to the Congressional Group for perceiving a complex problem.

C. Favored Alternative Valance

Actors in the Congressional Group, especially committee chairs, believed that laws were required to counter the administration’s information control actions and to protect privacy. Laws on maintaining access to information for national security and public safety purposes and on expanding encryption exports were also required, but were secondary and subject to serious compromises. During the Senate remarks on the *Computer Security Act of 1987*, Senator Lawton Chiles (D-Florida) described how this new law would create a clear line of authority for protecting unclassified information:

National Security Decision Directive 145 – NSDD 145 – assigned significant responsibility for the Nation’s computer security matters to the Department of Defense, specifically the National Security Agency, NSA. This arrangement has given rise to widespread concern about a defense or intelligence agency having responsibility over Federal computer systems that contain nondefense and nonclassified information. To allay these concerns, this bill quite properly assigns the primary responsibility for certain computer security matters to the National Bureau of Standards....

This bill alters the previously existing Presidentially directed assignment of responsibilities in the computer security arena by making the NBS the primary agency responsible for sensitive civil sector computer matters.²⁸¹

The text shows that Congress favored a law that would remove the responsibility of computer security for unclassified information from the Department of Defense and place it with the NBS, which is an agency under the Department of Commerce. In addition, the text shows that some actors in the Congressional Group believed that the *Computer Security Act of 1987* would keep national security issues out of the "civil sector." The extension of President Reagan's national security directives into the private sector was the prime motivator for additional congressional actions.

Congress did not trust the actions of the executive branch in modifying NSDD-145 to satisfy congressional concerns. Although witnesses for the executive branch were responsive to questions from members of the House Legislation and National Security Subcommittee, Chairman Brooks set the agenda for H.R. 145, irrespective of the answers:

During their tenure, the National Security Council was transformed from an advisory office to the President into an operational element of the military and intelligence apparatus. In this role, they attempted numerous controls and restrictions over the public's access to a wide range of unclassified information. They ran roughshod over civilian agencies and private sector companies who objected to these policies. Their actions launched a campaign of intimidation which included sending members of the FBI and CIA, agents, out to "convince" companies to support their efforts.

²⁸¹ *Congressional Record*, 100th Congress, 1st sess., 1987, 133, pt. 26: S37678.

This subcommittee is meeting today to consider corrective legislation to modify the authority given to the Defense Department under this directive. As such, I believe the testimony of Admiral Poindexter and Mr. deGraffenreid is essential to the proper consideration of H.R. 145, the Computer Security Act of 1987.²⁸²

The text indicates that H.R. 145 was a power balancing legislation and that the testimony of Admiral Poindexter was requested to explain the evolution of NSDD-145 into an information control policy. The answers provided by Admiral Poindexter only increased the suspicions of Congress:

Mr. Brooks: Under your directive, what authority does the Government have to restrict public access to unclassified but sensitive information located in Federal agencies and the private sector, as well?

Admiral Poindexter: Mr. Chairman, on advice of my counsel, I decline to answer that question pursuant to my constitutional rights under the fifth amendment.²⁸³

The text indicates that a key member of the executive branch was not willing to explain the use of directives to control sensitive information that presented a threat to national security. Thus, Congress passed the *Computer Security Act of 1987* in large part to control the executive branch and made some progress on subsequent information control and technology legislations that challenged the national security prerogatives of the executive branch.

²⁸² Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 382.

²⁸³ *Ibid.*, 402.

H.R. 4922, the *Communications Assistance for Law Enforcement Act*, became law with a neutral stance on encryption control. Representative Brooks, Chairman of the Committee on the Judiciary, decided to exclude all language on encryption control:

The bill [H.R. 4922] does not address the “Clipper Chip” or Key Escrow Encryption issue. Nothing in this bill is intended to limit or otherwise prevent the use of any type of encryption within the United States. Nor does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, section 2602 protects the right to use encryption.²⁸⁴

The text shows that the Committee on the Judiciary was opposed to having H.R. 4922 support any “ban or limitation on encryption technology.” This lack of support effectively denied law enforcement officials the ability to accomplish court-ordered surveillance activities on encrypted communications. By not supporting the administration’s “Clipper Chip” or escrowed-key encryption initiative with the force of law, H.R. 4922 effectively killed the public use of the government’s escrowed-key encryption system. Without mandatory key escrow, the uncontrolled use of strong encryption systems could threaten national security and public safety. Without a supportive law, the executive branch gradually reduced the push to use CLIPPER and successor technologies such as FORTEZZA. Meanwhile, the commercial sector had already developed complete encryption systems to meet consumer demand.

H.R. 4922 contained delicate language that required the telecommunications sector to assist law enforcement officials with surveillance of digital communications and

²⁸⁴ House Committee on the Judiciary, *Telecommunications Carrier Assistance to the Government*, 24.

interconnected computers. If a telecommunications carrier supplied the encryption system and had the encryption key, then these carriers were legally obligated to help with court-ordered surveillance activities:

(3) Encryption.--A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

The text shows that the *Communications Assistance for Law Enforcement Act* did help support law enforcement activities when the “encryption was provided by the carrier.” At the time of bill passage, it seemed unlikely that criminals, spies, and terrorists would use encryption provided by telecommunications carriers. Thus, some actors in the Congressional Group saw a requirement to salvage and reuse the time and effort put into prior government encryption control schemes.

Unwilling to abandoned government escrowed-key encryption, some actors believed that legislation could obtain a balance among national security, public safety, economic, and privacy requirements. One such legislation to legalize the government’s escrowed-key encryption system was introduced by Representative George E. Brown, Jr. (D-California) on October 4, 1994, just two days after the debate on H.R. 4922. Representative Brown was an astute Congressman in the science and technology policy area and reasoned that an escrowed-key encryption law was a satisficing solution to the impasse between the administration and Congress on information control policies:

The administration has publicly stated that it does not intend to seek legislation expressly authorizing Clipper or any other Federal encryption standard because it wants flexibility to modify its encryption policy and program in response to changing circumstances. The administration's desire for flexibility, however, contributes to the public's mistrust and opposition to Clipper. The proposal was developed under an administrative directive and, therefore, could just as easily be changed in a way that might be construed to diminish privacy rights without giving the public adequate opportunity to affect the program. For this reason alone, the public is unlikely to ever accept Clipper Chip in its present form.

I, along with others, believe that a viable approach to gain public support for an initiative like Clipper is legislation to codify Federal encryption policy and govern how that policy would be implemented. In so doing, all stakeholders would have an opportunity to influence the policy. The final program would have been subjected to greater scrutiny and its implementation would be under the rule of law. It may well be that only under these circumstances would the public accept a Federal encryption standard and the needs of law enforcement could be satisfied.²⁸⁵

The text indicates that the problem with the Clinton administration's "Clipper" escrowed-key encryption initiative was "mistrust" in an encryption system controlled by the executive branch. Representative Brown reasoned that the public was "unlikely to ever accept [the] Clipper Chip." His proposed solution to the problem was to use "greater scrutiny" and the "rule of law" to develop a trustworthy government solution. Although H.R. 5199 was proposed late in the session and did not make it out of committee, his reasoning that a government escrowed-key encryption system required the force of an encryption law to be effective was sound.

Two years later, Congress passed H.R. 3723, the *Economic Espionage Act of 1996*. Heavily amended by the Senate with the appendage of the *National Information*

²⁸⁵ *Congressional Record*, 103rd Congress, 2d sess., 1994, 140, pt. 20: H28704.

Infrastructure Protection Act of 1995, H.R. 3723 became the vehicle to protect digital information and its infrastructure with criminal penalties. During the Senate debate on the *Economic Espionage Act of 1996*, Senator Patrick Leahy (D-Vermont) specifically discussed the criminal use of encryption:

Finally, this legislation [addresses] a new and emerging problem of computer-age blackmail. This is a high-technology variation on old fashioned extortion. One case has been brought to my attention in which a person threatened to crash a computer system unless he was given free access to the system and an account. One can imagine situations in which hackers penetrate a system, encrypt a database and then demand money for the decoding key. This new provision would ensure law enforcement's ability to prosecute modern-day blackmailers, who threaten to harm or shut down computer networks unless their extortion demands are met.²⁸⁶

The text shows the use of an often-cited criminal encryption of a database scenario to convince Congress on the requirement for laws to prevent information crimes. Although no specific court case in the *Congressional Record* documents such a crime and the lack of legal recourse, actors in the Congressional Group believed that legislation “would ensure law enforcement’s ability to prosecute modern-day blackmailers.”

The reliance of H.R. 3723 on punitive measures and not on proactive measures, such as requiring the use of encryption to protect valuable data, indicated that Congress was still unable to balance the encryption control problem in law. The *Economic Espionage Act of 1996* did contain a legal reporting requirement to gather data on the use of encryption in criminal activity:

²⁸⁶ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 140: S12216.

SEC. 501. USE OF CERTAIN TECHNOLOGY TO FACILITATE CRIMINAL CONDUCT.

(a) INFORMATION.—The Administrative Office of the United States courts shall establish policies and procedures for the inclusion in all presentence reports of information that specifically identifies and describes any use of encryption or scrambling technology that would be relevant to an enhancement under 3C1.1 (dealing with Obstructing or Impeding the Administration of Justice) of the Sentencing Guidelines or to offense conduct under the Sentencing Guidelines.

(b) COMPILING AND REPORT.—The United States Sentencing Commission shall—

(1) compile and analyze any information contained in documentation described in subsection (a) relating to the use of encryption or scrambling technology to facilitate or conceal criminal conduct; and

(2) based on the information compiled and analyzed under paragraph (1), annually report to the Congress on the nature and extent of the use of encryption or scrambling technology to facilitate or conceal criminal conduct.²⁸⁷

The text shows that actors in the Congressional Group were looking for information to enhance the penalties for using encryption in the furtherance of a crime. The text also indicates that Congress lacked specific knowledge on the magnitude of the negative externalities of encryption use and was not interested in cases where encryption use prevented economic espionage by securing valuable information. Thus, the *Economic Espionage Act of 1996* sought encryption control through criminal penalties and did not promote encryption liberalization.

Actors is the Congressional Group understood that Congress was jeopardizing national security and economic growth by its failure to update the *Export Administration Act of 1969*, which was last renewed in 1979. During the debate on the proposed H.R.

²⁸⁷ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 140: S12203.

361, the sponsor of the bill, Representative Toby Roth (R-Wisconsin), spoke on its critical importance:

Mr. Speaker, in conclusion, I recall introducing this bill, H.R. 361, on the first day of the Congress. My goal was simple, to reform our outdated export control system and to help our high-technology industry to create new jobs, good paying jobs, for American workers. This bill does that. It replaces a 17-year-old dinosaur with a law that is updated and forward looking. With H.R. 361's passage, we will help the United States enter the 21st century as the most successful and the most responsible exporting state in the world, and I urge all my colleagues to adopt and to vote for this legislation.²⁸⁸

The text shows the mounting frustration in Congress with its continued failure to update a "17-year-old dinosaur" with a law that would "help the United States enter the 21st century" of global trade. Without a law, administrative regulations from the executive branch would continue an outdated export regime that was generations behind the technology found in current exports.

The use of multiple laws as solutions by actors in the Congressional Group matched Allison's GPM general proposition of "Action and Intention" where the actions of Congress do not always produce intended laws.²⁸⁹ Congress intended to pass a series of legislations to address the linked areas of information control and national security, wiretapping and privacy, and exports and economic prosperity. With the passage of the *Computer Security Act of 1987*, congressional action successfully challenged the power of the executive branch to control information. However, subsequent laws were less

²⁸⁸ *Congressional Record*, 104th Congress, 2d sess., 1996, 142 pt. 104: H7584.

²⁸⁹ Allison and Zelikow, *Essence of Decision*, 306.

decisive and diverged significantly from their original intents. The *Communications Assistance for Law Enforcement Act*, as intended by Congress and not implied by its title, countered the administration's encryption control agenda. This law spawned a proposed encryption control law that did not pass. Later laws, such as the *Economic Espionage Act of 1996*, protected the information infrastructure through criminal penalties and not through the intended information security measures discussed in committee hearings and floor debates. A critical legislation on export and encryption liberalization did not have the required congressional support to pass, thus sending the wrong message to the executive branch. Despite this miscommunication, I assigned a Favored Alternative valance of "2" to the Congressional Group for passing laws to achieve their goals. The inability to pass export and encryption laws in a timely and relevant manner did affect the next valance.

D. Decision Timing Valance

Actors in the Congressional Group exhibited an initial sense of urgency in passing a law that limited the ability of the executive branch to control sensitive but unclassified information. However, Congress passed subsequent laws in an incremental manner and only after removing controversial elements of proposed legislations to gain tacit consensus. Proposed legislations on export and encryption control that could not gain consensus lingered through the period, as the underlying issues remained as conditions or problems without solutions. During a committee hearing on the *Computer Security Act of 1987*, H.R. 145, Representative Brooks proclaimed the urgent need for H.R. 145 and

countered the Director of the National Security Agency's claim that this legislation was unnecessary:

Mr. BROOKS. We certainly do appreciate them [comments], and it reflects very clearly, I understand, the NSA attitude. Mr. Miller, head of the OMB, wrote me a letter today indicating that they saw some need for changes in that wonderful directive, NSDD-145. He was willing to work with us on making some changes in this legislation, H.R. 145. I want to guarantee you that I'm going to do my best to pass it.

If you don't think it's necessary and you have some puzzlement about this, well, you can continue to testify and tell every Member of Congress what you want to do. I'll tell them what the facts are, and about all these other people that say you're trying to do them in. You can have all the locks you want at the NSA, but when you start putting them on everybody else, that's a different story. I don't want to be in handcuffs. Neither does the business community, the private sector, the banks, the businesses, the data banks, the financial institutions, the libraries, [and] the technical and educational institutions in this country.²⁹⁰

The tone of text indicates that there was an urgent requirement for H.R. 145 to protect information in the non-defense government and private sectors from over control by a security directive. The text shows that the committee chairman, Representative Brooks, was confrontational with NSA and was personally involved with the *Computer Security Act of 1987*. After passage of this act, Congress had to help law enforcement officials and the telecommunications sector reach a compromise on satisfying information access requirements.

Actors in the Congressional Group initially displayed a sense of urgency to pass the *Communications Assistance for Law Enforcement Act*, H.R. 4922, but then exhibited

²⁹⁰ House Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 298.

incrementalism by deferring the encryption control provision of this bill. Representative Edward J. Markey (D-Massachusetts) spoke of how technology advancements had increased the rate of required changes for old legislations:

Congress again responded to changes in computer and communications technology by passing the Electronic Communications Privacy Act of 1986. This law, which was sponsored by Senator LEAHY and Congressman EDWARDS, amended the 1968 Wiretap Act by protecting a new class of electronic communications, defined broadly to include everything from e-mail to databases. That legislation reflected an on-going effort to update and clarify Federal wiretap laws, as the Senate Committee put it, “in light of dramatic changes in new computer and telecommunications technologies.”

Well today, we are back at the task of updating and clarifying our wiretap law again. This time, the changes in computer and telecommunications technology are not just dramatic, they are overwhelming. The growth of digital communications over the past 8 years, the spread of fiber deeper into the local phone network, the spread and growth of wireless services – all of these developments converge to compel us to address legislatively the needs of law enforcement in the information age. The Federal Bureau of Investigation argues that as these advanced technologies get deployed, that the technology should not, in essence, repeal or modify the 1968 Wiretap Act. Instead, the Bureau argues, we must update and clarify our laws so that ability to conduct wiretaps is maintained – not expanded and not diminished – just maintained.²⁹¹

The text suggests that “overwhelming” changes in telecommunications technology could effectively “repeal or modify” old laws. The text also indicates that the revisit requirement to update old legislation was accelerating. This revisit requirement removed a sudden sense of urgency to pass legislation by relying on incrementalism. Information technology legislation could be passed in a timelier manner if it were passed periodically and in pieces.

²⁹¹ *Congressional Record*, 103rd Congress, 2d sess., 1994, 140, pt. 20: 27708.

As discussed earlier, H.R. 4922 specifically avoided the encryption control piece of the problem. In general, H.R. 4922 allowed a broad range of telecommunications service providers to avoid implementing surveillance “capability requirements” that were desired by the government.²⁹² Thus, the largest telecommunications advancement of the 1990s, the Internet, was largely excluded from discussion in the *Communications Assistance for Law Enforcement Act*:

The bill is clear that telecommunications services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunication carriers (these would include long distance carriage) need not meet any wiretap standards. PBXs are excluded. So are automated teller machine (ATM) networks and other closed networks. Also excluded from the coverage are all information services, such as Internet service providers or services such as Prodigy and America-On-Line.²⁹³

The text shows that law enforcement officials could not always expect assistance from telecommunications carriers in meeting “any wiretap standards.” This included complying with encryption standards that would facilitate wiretapping. The deferred legal information access requirements for Internet wiretaps and the information security requirements for the protection of the United States information infrastructure had to wait for the next information control bill.

The passage of the *Economic Espionage Act of 1996* was driven by incrementalism in that several major amendments dramatically expanded the original bill, H.R. 3723, in the economic and national security areas. During the Senate debate on H.R. 3723,

²⁹² House Committee on the Judiciary, *Telecommunications Carrier Assistance to the Government*, Report 103-827, Part I, 18.

²⁹³ *Ibid.*, 18.

Senator Arlen Specter (R-Pennsylvania) pointed out that this bill was not a final solution, and he focused primarily on the economic aspect of the information protection problem:

The Senate adopted S. 1556 [industrial espionage] with an amendment I offered, based on S. 1557 [economic security], to bring together in a single vehicle the prohibition on the theft of trade secrets and proprietary information by both private individuals and corporations and by foreign governments and those acting on their behalf, and passed them using H.R. 3723, the House companion bill, as the vehicle....

Adoption of this bill will not be a panacea, but is a start. Congress has started moving to protect U.S. economic interests.²⁹⁴

The text shows that H.R. 3723 was the start of a government effort designed to “protect U.S. economic interests.” Senator Leahy, who discussed the greatly expanded scope caused by appending the *National Information Infrastructure Protection Act* to H.R. 3723, followed Senator Specter in the debate:

Mr. LEAHY. Mr. President, I am delighted that the Senate is today taking the important step of passing the Economic Espionage Act and the National Information Infrastructure Protection Act of 1996 ...

Confronting cybercrime with up-to-date criminal laws, coupled with tough law enforcement are critical for safeguarding the privacy, confidentiality and reliability of our critical computer systems and networks.²⁹⁵

In the text, Senator Leahy believed that “privacy” and “confidentiality” could be protected with “up-to-date criminal laws.” This strategy to reduce information crimes through criminal penalties deferred the whole dimension of protecting information

²⁹⁴ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 140: S12208.

²⁹⁵ *Ibid.*, S12214-16.

through legislated encryption use. Encryption use could ensure both privacy and confidentiality, but would have spillover effects into the national security dimension.

In order to secure its passage in the House, the sponsors of the proposed *Export Administration Act of 1996*, H.R. 361, wanted to capitalize on the sense of urgency arising out of the great effort required to draft this legislation. However, H.R. 361's incrementalism and the tacit census to forgo critical areas, such as encryption control, were divisive enough to prevent serious consideration in the Senate. Representative Roth, sponsor of H.R. 361, discussed the long effort required to achieve a compromise bill: "We spent 14 months in bipartisan discussion, talks involving our committee, and the administration, and the Committee on National Security."²⁹⁶ In addition to emphasizing the difficulty of drafting this bill, these words reinforced the incremental and tacit decisions required to produce the draft. After passage of H.R. 361 in the House, Representative Anna G. Eshoo (D-California) entered her concerns on these decisions in the *Congressional Record*:

MS. ESHOO. Mr. speaker, today we are considering the Export Control Act, [a short title for H.R. 361] which governs the export of dual-use technologies. Ironically, it does not govern the export of encryption software, which is considered a munition and is regulated under the Arms Export Control Act. In fact, encryption software is absolutely vital in national security, electronic commerce, and personal privacy applications. I can't imagine a technology that has more civilian as well as defense applications – the very definition of dual use.

I am very concerned that current Federal controls are holding American high tech companies back from developing and marketing superior encryption products. I understand that that these controls are aimed at keeping powerful

²⁹⁶ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 104: H7584.

encryption out of the hands of terrorists and hostile nations, they are succeeding only in keeping foreign customers away from American products.²⁹⁷

The text suggests that the House passed a bill that solved only a part of the export control problem and that the House agreed not to include control of “encryption software” that was “absolutely vital in national security, electronic commerce, and personal privacy applications.” Deferring content proved to be divisive in the Senate.

In 1997, the Senate of the 105th Congress attempted to construct several encryption legislations. None were successful, as solving critical parts of the deferred export legislation proved to be impossible tasks. Without a pressing urgency to solve the complete export control problem, both members of the Senate and the administration failed to produce satisficing solutions. In a barrage of statements, Senators openly urged action on pieces of the deferred export legislation. Senator Patty Murray (D-Washington) had this opinion on the encryption control problem:

Mrs. MURRAY: Mr. President, I rise to discuss an issue of great importance to Washington state. I remain deeply concerned about the Administration’s lack of progress in working with interested Senators and industry to craft a workable, effective solution for modernizing the United States export controls on products with encryption capabilities. I have been involved in this debate for a long time, too long. We need to take action.²⁹⁸

Again, the text shows that the main problem was the “Administration’s lack of progress” toward “modernizing the United States export controls.” Other Senators saw that the promise and problems of incrementalism came from within the Senate.

²⁹⁷ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 105: E1295.

²⁹⁸ *Congressional Record*, 105th Congress, 1st sess., 1997, 143, pt. 156: S12195.

Some Senators were convinced that one form of incrementalism, which was the graduated encryption strength provisions found in proposed bills, would not work. One such bill was the proposed McCain-Kerrey bill to secure communications and networks, S. 909. Senator John Ashcroft's (R-Missouri) comments were typical in responding to bills that tailored allowable encryption strength in order to reduce national security concerns on exported encryption products:

I am persuaded that a number of the new provisions in the McCain-Kerrey bill are not necessary.

I believe that many of the provisions will not even succeed at achieving the end they seek. For example, a false choice has been offered indicating that if the U.S. continues to enforce the export policy on encryption that is currently in place, 40 bit and with special permission up to 56-bit, then law enforcement could apprehend terrorists, stop illegal gamblers and arrest pornographers. However, this argument assumes that these criminals cannot find stronger encryption elsewhere than in the United States. As has been shown several times, this assumption is false. Robust encryption is available. Germany, Japan, and the United Kingdom all have companies, such as Siemens, Nippon and Brokat, that have developed and promote 128 bit encryption.

The text shows that Senator Ashcroft believed that 40 and 56-bit encryption limitations would "not even succeed at achieving the end they seek." By 1997, encryption technology advancements made 128-bit encryption globally available. Thus, the export control problem required acknowledgement that it was too late to control strong encryption by modifying technical parameters. National security and public safety requirements would have to find another approach to gain court-ordered information access.

The passage of the *Computer Security Act of 1987* met the requirement for an urgent legislation that challenged the power of the executive branch in controlling unclassified but sensitive information. Subsequent legislations were purposefully ambiguous on encryption control or deferred the area of encryption control to future legislations. This change in behavior matched Allison's OBM general proposition that "Organizational Priorities Shape Organizational Implementation."²⁹⁹ Actors in the Congressional Group successfully overcame a threat to their power by passing legislation to counter national security directives from the executive branch. However, when technology advancements such as the development of encryption systems quickly threatened the balance between public safety and privacy requirements and the balance between national security and economic goals, Congress found that it was not an imperative to solve these problems. The enactments of the *Communications Assistance for Law Enforcement Act* and the *Economic Espionage Act of 1996* incrementally solved some problems and deferred problems on information access for law enforcement activities and information infrastructure protection through encryption use. The continued failure of export control legislations, partly because of their encryption control contents, demonstrated that a unified congressional position on information technology was not an organizational priority. Actions by the executive branch on encryption control drove significant congressional rhetoric, but were not a sufficient force to drive legislative priorities. I therefore assigned a Decision Timing valance of "1" to the

²⁹⁹ Allison and Zelikow, *Essence of Decision*, 180.

Congressional Group for making incremental and tacit changes to legislations and by deciding to defer the encryption control problem.

Encryption Technology Group

In the Competitive Period, the primary actors in the Encryption Technology Group were private individuals and members from academia, electronic rights groups, information technology vendors, and professional organizations. Most of these actors advocated encryption liberalization, which represented a unifying philosophy covering beliefs in privacy rights, technology leadership, and market determination. Actors counter to this philosophy were believers in satisfying Cold War-driven national security requirements and government specified public safety concerns. The culmination of international relations, national security, and public safety efforts supporting encryption control could not counteract private sector gains made toward encryption liberalization. Actors from the Encryption Technology Group did not support information control legislations and regulations and used policy delays caused by the competition between the executive and legislative branches to produce encryption solutions that were more optimal than the ones encouraged by the government.

Encryption liberalization advocates first appeared in the early 1970s, matured through the passage of the *Computer Security Act of 1987*, and were instrumental in the defeat of the government's Escrowed Encryption Standard. Established encryption vendors were generally passive during this period, presumably as not to perturb their lucrative government information technology contracts. However, encryption

technologists from new information technology companies were not tightly bound to the government. These technologists, along with members from academia and electronic rights groups, formed the active core of the Encryption Technology Group during this period. The Competitive Period ended with complete and affordable encryption systems being made available to the public. Company statements, court cases, engineering demonstrations, and congressional testimonies and reports provided the data for analyzing the actions of the Encryption Technology Group. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

Actors in the Encryption Technology Group believed that the private sector was the lead actor for advancements in information technology and believed that reliance on government leadership hurt the market, which provided the inducements for technology advancements. Cryptology expert Dr. David Kahn testified about these coupled beliefs during a hearing on the *Computer Security Act of 1987*:

So I don't think that the NSA can any longer expect that the public is going to place blind confidence in its integrity, and it must be subject to the very same checks and balances as all other institutions of the Government.

The other danger, a second danger from this program, is restraint of innovation in cryptography. If NSA furnishes the equipment that's going to be used, this means that private inventors will have less incentive to create and private firms less incentive to produce new cryptosystems, and the two most widely used cryptosystems of the past decade have come from private inventors. One is the so-called data encryption standard devised by a man named Horst

Feistel while he was at IBM, and the second is public-key or asymmetric cryptography.³⁰⁰

The text indicates that Dr. Kahn suspected the trustworthiness of NSA, and more importantly, believed that government led encryption efforts would provide “less incentive” for the private sector to take a leadership role. In addition, Dr. Kahn claimed that advances in secret key and public key encryption came from “private inventors.” When Dr. Kahn provided his testimony to Congress in 1987, encryption systems were normally implemented as digital hardware devices. This is one reason why he used the term “equipment” in reference to encryption systems. Private individuals were not only inventors of secret key and public key encryption subsystems, but were also behind efforts to eliminate government controls on encryption technology.

A well-known electronic rights activist, Mr. Philip Zimmermann, claimed that government control of information technology was impossible. In 1993, he testified before the House Subcommittee on Economic Policy, Trade, and Environment and delivered a prepared statement:

I am the author of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1991, it has spread organically all over the world and has since become the de facto worldwide standard for encryption of E-mail. The US Customs Service is investigating how PGP spread outside the US. Because I am a target of this ongoing criminal investigation, my lawyer has advised me not to answer any questions related to the investigation....

³⁰⁰ Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 129.

This convergence of technology-- cheap ubiquitous PCs, modems, FAX, digital phones, information superhighways, et cetera-- is all part of the information revolution. Encryption is just simple arithmetic to all this digital hardware. All these devices will be using encryption. The rest of the world uses it, and they laugh at the US because we are railing against nature, trying to stop it. Trying to stop this is like trying to legislate the tides and the weather. It's like the buggy whip manufacturers trying to stop the cars-- even with the NSA on their side, it's still impossible. The information revolution is good for democracy-- good for a free market and trade. It contributed to the fall of the Soviet empire. They couldn't stop it either.³⁰¹

In the text, Mr. Zimmermann claimed that he was a “target of an ongoing criminal investigation” for violating export laws and rationalized his actions as a natural “convergence of technology,” which the government could not stop. He used the metaphor “like trying to legislate the tides and the weather” to illustrate the limited ability of the government to control information technology and especially encryption technology. In addition, the text indicates that the motivation behind his challenge to the government was the belief that his actions were “good for democracy -- good for a free market and trade.” The liberalist view of individual action and market forces moderating state power suggested that the private sector was the lead actor in the information revolution. Mr. Zimmermann was not alone in advocating action by the private sector. Organizations generally have more power than individuals do in influencing government policy decisions.

Organizations advocating electronic rights, such as the Electronic Frontier Foundation (EFF), testified before Congress in opposition to government information

³⁰¹ House Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade and Environment, *Export Controls on Mass Market Software*, 103rd Congress, 1st sess., 12 October 1993, 105-6.

control efforts. While the growing national information infrastructure or information highway required tools for information security, government solutions offered by the executive branch were based on the CLIPPER Chip and other escrowed-key encryption schemes. In his 1994 testimony before Congress on escrowed-key encryption, EFF Executive Director Jerry Berman suggested that government solutions would not work in the market:

Finally, you offer Clipper Chip on the market, there is good reason why it is incompatible with software designs, with other communications systems. It locks us into a domestic market because no foreign country wants this chip because we are going to be holding the keys to communication. So it doesn't favor a global information highway.

What is the balance? It may solve the law enforcement problem, but it only solves it if criminals use it. As long as it is a voluntary system, that does not parse. The terrorists, the World Trade Center bombing, the international terrorist organizations – why are they going to go to Radio Shack or wherever they buy equipment in a foreign country and buy the “Clipper Chip” which says “Made by NSA,” keys held by the United States Government? That is never parsed.

The administration wants to have it both ways. They want to say that we are tough on law enforcement but we are not going to bite the bullet here and talk about what we really mean, which is that in order for this system to work, you got to mandate it. You have to tell people this is the system you are going to use.³⁰²

The text shows that electronic rights organizations, such as EFF, were not in favor of the government developing market-based encryption systems. Director Berman addressed the problem of the United States government providing global technology leadership with the example of the CLIPPER Chip. He claims in the text that, “no foreign country wants this chip” because the United States government will be “holding the keys to

³⁰² House Committee on Science, Space, and Technology, Subcommittee on Technology, Environment and Aviation, *Communications and Computer Surveillance, Privacy and Security*, 103rd Congress, 2nd sess., 3 May 1994, 55.

communication.” In addition, Director Berman implied that the government could not use a “voluntary system” because people in the United States would not use it for the same reason that foreign countries would not use it. Director Berman believed that the government would have to “tell people this is the system you are going to use” in order to make escrowed-key encryption work. Without a receptive Congress to pass such a law, the administration resorted to pressuring individuals, organizations, and corporations as a show of force.

Professional organizations, such as the Association for Computing Machinery (ACM), did not see the government as being an effective leader in the area of information technology policy. Dr. Barbara Simons, chair of the U.S. Public Policy Committee of the ACM, testified before the Senate Subcommittee on Science, Technology and Space on what the government was doing wrong with encryption policy:

DR. SIMONS. First of all, the USACM supports the development of public policies and technical standards for communications technology only when they are conducted in an open forum in which all the stakeholders may participate, such as we are doing here.

Second, the USACM believes that the U.S. should not adopt any encryption policies which place U.S. companies at a competitive disadvantage in the global market. Of course, speaker after speaker has emphasized how that is precisely what we are currently doing.

Third, the USACM supports the use of encryption for privacy protection, and encourages the development of technology and institutional practices that will provide real privacy for future users of the national information infrastructure, which we are currently building and of course which we hope will continue to be built both nationally and globally by U.S. corporations.

Fourth, the USACM remains opposed to the Clipper chip proposal and urges the administration to begin an open and public review of encryption technology.³⁰³

In the text, the USACM believed that the “United States should not adopt any encryption policies which place U.S. companies at a competitive disadvantage in the global market.” This belief placed the role of the market at the same level or higher than the role of government in determining encryption policies. In addition, the text shows that the USACM supported the “use of encryption for privacy protection” and that “U.S. corporations” would build the “national information infrastructure.” Dr. Simons’ last point saw the role of the government as meddling, which she emphasized by opposing the Clinton administration’s escrowed-key encryption efforts. Later in her testimony, Dr. Simons stated her rationale behind this opposition: “There is no room left for doubt, strong encryption products are widely available in overseas markets. Foreign companies will not purchase products from the United States if they can purchase products with higher levels of security from other producers.”³⁰⁴ Leaders in the information security and software technology industries shared this view with the USACM.

Encryption technology vendors and software companies perceived that information control by the government threatened the viabilities of both United States technology leadership and software market dominance. In 1996, President of RSA Data Security, D.

³⁰³ Senate Committee on Commerce, Science, and Transportation, Subcommittee on Science, Technology and Space, *S. 1726, Promotion of Commerce Online in the Digital Era Act of 1996, or PRO-CODE” Act*, 104th Congress, 2d sess., 26 June 1996, 100-101.

³⁰⁴ *Ibid.*, 101.

James Bidzos, testified before the Senate Subcommittee on Science, Technology, and Space. He cautioned the committee members on the dangers of government controls:

We have heard a lot lately and seen a lot in the press lately about these chips that are manufactured by a subsidiary of NTT, which is the world largest corporation. While I was in Japan last March, I was presented with the very first chips that were coming out of the manufacturing facility. I guess they thought that since one of them was an RSA chip, implementing the technology described in the United States patent than my company holds, that they thought it would be very nice to give me the first chips. I was very flattered.

I do not think they did this to impress me. I think they did that because there is a market for these chips. Somebody wants to buy them, and you do not invest the kind of money it takes to design and manufacture that kind of silicon unless there is somebody out there willing to buy it.

As far as I know, the only export controls in Japan are those that dictate that they should export products, and as many as they can....

Let me say just a word about the recent compromise proposals from the administration on export controls. The last one that everyone has been debating quite a bit is the key escrow proposal....

Bill Gates, who is of course the chairman of the world's largest software company, which owes at least some of its success to their ability to understand what their customer wants, responded to this latest key escrow proposal by calling it "no proposal."

I think there is a message in there. This is a man who understands marketing. So I think it is important to understand that some of these proposals simply are not going to work.³⁰⁵

The text suggests that encryption vendors in the United States believed that government export controls would not work for information technology products. Mr. Bidzos' story on the Japanese manufacturing his "RSA chip" and the apparent lack of export controls by the Japanese government on dual-use chips alerted Congress to the competitive nature

³⁰⁵ Senate Committee on Commerce, Science, and Transportation, Subcommittee on Science, Technology and Space, *S. 1726, Promotion of Commerce Online in the Digital Era Act of 1996, or PRO-CODE" Act*, 104th Congress, 2d sess., 12 June 1996, 53-55.

of the global information and encryption technology markets. As with other actors in the Encryption Technology Group, RSA Data Security saw no competitive merit in escrowed-key encryption. In the text, Mr. Bidzos believed that the United States government's "key escrow proposal" was "not going to work." The rationale, as implied in the text, was that the government lacked an understanding of customer requirements, which encryption vendors should have to be successful.

The perception of the private sector as the lead actor by the Encryption Technology Group matched Allison's RAM organizing concept of a "Unified National Actor," in which members of a group "have a single estimate of the consequences that follow each alternative."³⁰⁶ Individuals, organizations, and corporations saw government actions on information control and escrowed-key encryption as having negative consequences for the market. Conversely, these actors perceived that building the global information infrastructure, which they made secure by supplying trusted and affordable information security tools, was beneficial for both the global economy and the technology leadership of the United States. The debate presented by this group to Congress on encryption exports specifically showed that government policies were not market friendly and would cost the United States its technology leadership in the information security area. I assigned a Lead Actor valance of "0" to the Encryption Technology Group for acting as the private sector leader in developing and marketing information security tools.

³⁰⁶ Allison and Zelikow, *Essence of Decision*, 24.

B. Problem Perception Valance

Actors in the Encryption Technology Group perceived a simple problem, which was the cost-effective protection of valuable or personal information from unauthorized access. These actors believed that the evolving national information infrastructure and even the global information infrastructure should be protected against unauthorized access by foreign countries, the United States government, criminals, and enterprising individuals and corporations. Cheryl W. Helsing from the American Bankers Association testified on the information security problem during a hearing on the *Computer Security Act of 1987*:

The first issue of concern is the apparent move to protect all sensitive information in the same manner – business information, information of importance to national interest, as well as classified defense information. Within both the public and private sectors, there is a need for broad spectrum of information systems security standards, techniques, and tools. There must be a range of security solutions that can be matched to the value of the information being protected and the nature of the threats.

Outside of the classified national security arenas, both the private and public sectors must select cost-effective security measures.

To use a very simple analogy, to travel from point A to B, one could choose a motorcycle, a truck, or a tank. These vehicles vary widely in cost and each is best suited to a different terrain or environment.³⁰⁷

In the text, the banking industry believed that information had different values to different users and that a “range of security solutions” should match the “value of the information and the nature of the threats.” Her analogy of using a tank for transportation

³⁰⁷ Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 114.

implied that national security information protection tools were too complex and expensive for use by the non-defense federal and private sectors. Unknown to Ms. Helsing was the knowledge that the national security community did not want “cost-effective security measures” to reach the private sector, as the market did not account for the costs of maintaining government access to encrypted information.

Actors in the Encryption Technology Group would judge the actions of the national security community as being anti-market. Dr. David Kahn testified during the hearing on the *Computer Security Act of 1987* about the dangers of government information control:

It’s a very interesting curiosity that this danger was made much more patent and much more real by the fact that the National Security Agency and/or its British counterpart had years before invented public-key cryptography and had never made it public. It thereby deprived the public of the many benefits of this, and I fear that such a condition is likely to be aggravated under NSA’s program of delivering its own standard telephone units for scrambling to the public.³⁰⁸

The text suggests that the national security community restricted general knowledge about and market access to public key encryption technology. These actions “deprived the public of the many benefits” of this important encryption subsystem. At the time, the private sector was using a mature secret key encryption subsystem, which was based on the ten-year old Data Encryption Standard. However, the availability of a complementary public key encryption subsystem was a simple problem left unsettled until the early 1990s.

³⁰⁸ *Ibid.*, 129.

Working around the suspicious delay by the government to promote public key encryption, actors in the Encryption Technology Group did their own promotion of complete encryption systems. In 1993, Mr. Zimmermann testified before a congressional committee on his rationale for giving away such a system to his friends and ultimately anyone connected through the Internet:

If you want to protect electronic mail, you have to use cryptography and to use cryptography requires this second breakthrough in the late 1970's, the invention of public key cryptography. With public key cryptography you can communicate securely with people you have never met without the prior exchange of keys through a secure channel....

So the convergence of these technologies, the trappings of the information age, personal computers, modems, the Internet, the national information superhighway, all brings together all the parts necessary for everyone to use cryptography. It is no longer just the tools of the military or governments, or for diplomatic traffic. Technology is overtaking us, and if we want to have a global economy, if we want to be able to compete and participate in a global economy, we need to use the trappings of the information age and we cannot do our commerce without digital signatures and that is part of public key cryptography as well.

We need to have cryptography for our privacy. People need their privacy. People want their privacy. That is part of the reason why my product has become so popular.³⁰⁹

The text shows that Mr. Zimmermann considered the invention of public key encryption as a “breakthrough” and as the enabler of a “global economy.” As discussed earlier, the stated importance of public key encryption to commerce and the market matched Dr. Kahn’s suppositions on this technology, which he espoused during the 1987 H.R. 145 hearing. In addition, Mr. Zimmermann believed that encryption was “no longer just the

³⁰⁹ House Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade and Environment, *Export Controls on Mass Market Software*, 21.

tools of the military or governments,” but now part of the “trappings of the information age.” He also pointed out in his testimony that digital signatures and privacy protection were additional features of encryption. In a form of technological determinism, Mr. Zimmermann believed that the public availability of encryption technology would turn a complex information control problem into a simple problem, whereby individuals would determine encryption policy through market actions.

The ability of electronic rights activists to exploit the free speech guarantees under the First Amendment of the Constitution demonstrated that the judicial branch did not perceive a complex information control problem with national security and foreign policy linkages. Since encryption technology found in the private sector could be reduced to text describing mathematical algorithms and subsequent software code implementing these algorithms, government control of encryption technology could be equated with government control of free speech. To prove this point in 1995, Dr. Daniel J. Bernstein filed suit against the federal government claiming that since 1992, his First Amendment rights were abridged by export controls on his “Snuffle” encryption algorithm. He produced this algorithm and created the C language source code in 1992 as a doctoral student. Starting in 1996, federal district and appellate level courts found merit in his claims and generally ruled in his favor:

DISCUSSION

Plaintiff makes a number of allegations of unconstitutionality with respect to the AECA and ITAR. Specifically, plaintiff argues that the act and accompanying regulations, both facially and as applied, are a content-based infringement on

speech, are vague and overbroad, and infringe on the rights of association and equal protection....

For the purposes of the First Amendment analysis, this court finds that source code is speech. Having concluded that all the items at issue, including Snuffle.c and Unsnuffle.c are speech, this court must now briefly review the claims defendants contest for colorability.³¹⁰

The text shows that the United States District Court of the Northern District of California summarized Dr. Bernstein's claim as "a content-based infringement on speech" caused by government regulations. In addition, the text shows that this court used a finding that "source code is speech" as a basis for further legal analysis. From the government's perspective, the potential for such a finding and the inherent lack of controllability of software reinforced the requirement for the on going hardware-based escrowed-key encryption program. The private sector perceived this court finding as a monumental affirmation of encryption liberalization and as an association of encryption design with the First Amendment rights. Even before this ruling, electronic rights activists printed encryption source code in books and magazines and on t-shirts and neckties. Individuals could now make simple decisions on the control of software-based encryption technology without interference from changing export laws. However, the government persisted until the end of the Clinton administration to modify export regulations in order to promote its hardware-based encryption schemes and to gain as much control over software-based encryption as possible.

³¹⁰ *Bernstein v. United States Department of State, et al.*, 922 F. Supp. 1430-32 (N.D. Cal. 1996).

While private sector technology leadership and market availability of encryption helped make the domestic information control problem simple, United States government export regulations threatened to complicate the domestic market and the building of the global information infrastructure. Dr. Whitfield Diffie, who was working for Sun Microsystems at the time, testified in a 1996 Senate hearing on the dangers of government actions to prevent the global spread of encryption:

The current export control regime limits security of exportable systems to well below what is generally considered necessary for Internet commerce to fulfill its potential. Because major American corporations typically do more than half their business offshore, they are hesitant to attempt to deploy two sorts of security products, one for domestic and one for foreign use. The effect of export controls is thus to deny the benefits of cryptography to Americans....

As noted recently by a committee of the National Research Council, cryptography has the potential to protect legitimate resources and institutions of society and to facilitate the anti-social actions of both domestic and foreign opponents. Cryptographic technology is now available throughout the world in forms quite adequate to support such relatively small operations as criminal conspiracies or terrorist actions. On the other hand, large scale social phenomena such as business, civic, and personal communication require the development of a substantial infrastructure, whose deployment has been delayed by concerns over possible anti-social use. As long as we maintain a regulatory structure that impedes the use of cryptography by legitimate elements of society but is intrinsically incapable of denying it to illegitimate elements, we will succeed only in giving the advantage to our opponents.³¹¹

The text suggests that export controls on encryption adversely affected United States corporations and the maturation of the Internet. Dr. Diffie described the commercial and financial difficulties of having “two sorts of security products, one for domestic and one

³¹¹ Senate Committee on Commerce, Science, and Transportation, Subcommittee on Science, Technology and Space, S. 1726, *Promotion of Commerce Online in the Digital Era Act of 1996, or PRO-CODE” Act*, 26 June 1996, 21.

for foreign use,” when strong and interoperable encryption systems were “necessary for Internet commerce to fulfill its potential.” An important part of the text, which attacked the encryption export decisions of the administration, was the statement on foreign availability. In his argument, Dr. Diffie claimed, “Cryptographic technology is now available throughout the world in forms quite adequate to support such relatively small operations as criminal conspiracies or terrorist actions.” If criminals and terrorists already had adequate encryption technology, then encryption export regulations could never work, or in Dr. Diffie’s words, export regulation were “intrinsically incapable of denying it to illegitimate elements.” Logically, it followed that government efforts expended on encryption control served only to give “the advantage to [U.S.] opponents,” and his prophetic statement was proven in 1997.

In 1997, RSA Data Security demonstrated the obsolescence of the 20-year-old government Data Encryption Standard and their equivalent 56-bit RC5 encryption algorithm by sponsoring several encryption-cracking contests. The DES challenge was solved in June 1997 by an organization of computer users working under an effort named “DESCHALL.”

The DESCHALL effort, led by Loveland, Colorado computer programmer Rocke Verser, used networked CPUs from universities and corporations throughout the U.S. to apply "brute force" computing power to solve RSA's challenge and break a message encrypted with the government's 56-bit Data Encryption Standard (DES) algorithm....

“RSA congratulates the DESCHALL team for their achievement in cracking the 56-bit DES message,” said Jim Bidzos, president of RSA. This demonstrates that a determined group using easily available desktop computers can crack DES-

encrypted messages, making short 56-bit key lengths and unscalable algorithms unacceptable as national standards for use in commercial applications.[³¹²]

"This event dramatically highlights the fatal flaws in the most recent administration proposal, Bill S.909, "The Secure Public Networks Act of 1997," introduced by Senator John McCain (R-AZ) and Senator Bob Kerrey (D-NE). This bill, if passed, would severely hamper U.S. industry by limiting export to the 56-bit DES standard."³¹²

The text demonstrates the perception of a simple problem in that an impromptu organization was able to crack a United States government encryption standard, thereby suggesting that a stronger encryption standard was required. DES was too weak to secure valuable data, and the government had not improved upon DES because the government's focus was on using escrowed-key encryption to solve their own more complex problem. Mr. Bidzos' comments reinforced this perception by claiming that DES and other 56-bit key encryption algorithms were "unacceptable as national standards for use in commercial applications." In the text, Mr. Bidzos took the opportunity to criticize proposed legislation on exportable encryption strength by claiming, "This bill, if passed, would severely hamper U.S. industry by limiting export to the 56-bit DES standard." Even 56-bit products from Mr. Bidzos' company were found to be unacceptably weak.

In a demonstration of acceptable encryption standards available from the private sector, RSA Data Security subjected its 56-bit and 64-bit RC5 encryption algorithms to

³¹² RSA Security, "Team of Universities, Companies and Individual Computer Users Linked Over the Internet Crack RSA's 56-Bit DES Challenge, Landmark Breaking of 56-bit Government Encryption Standard Calls Administration Policy Into Question," 19 June 1997, <
http://www.rsasecurity.com/press_release.asp?doc_id=661&id=1034 >, accessed September 2004.

the same cracking challenge as DES. One anticipated result was that 56-bit RC5 was cracked by an organization called “distributed.net” in less than nine months after the start of the challenge:

CHICAGO, IL (October 22, 1997) In what could be called the largest distributed-computing effort ever, tens of thousands of computers linked across the Internet, under the leadership of distributed.net, decrypted a message encoded with RSA Labs' 56-bit RC5 encryption algorithm. Considered by many experts to be a sufficient level of encryption, this feat has cast grave doubts in the minds of analysts as to the level of encryption required to keep private data secure. "Our effort has shown that it is dangerous to consider any 56-bit key secure", says David McNett, one of the primary coordinators of this distributed supercomputing project.³¹³

The text shows that even 56-bit commercial encryption was susceptible to an organized cracking effort. David McNett, one of the organizers of distributed.net, claimed that it was “dangerous to consider any 56-bit key secure.” The 64-bit RC5, which was 256 times stronger, was not cracked during the Competitive Period and demonstrated the viability of stronger encryption.

The perception of a simple problem by actors in the Encryption Technology Group matched Allison’s RAM organizing concept of “The Problem,” whereby this group gained ownership of the information security problem by its common “response to the strategic situation.”³¹⁴ Individuals, organizations, and corporations took actions to demonstrate the inability of the government to solve this problem. Actors in the Encryption Technology Group showed that the government was adding complex

³¹³ Distributed.net, Secure Encryption Challenged by Internet Linked Computers, 22 October 1997 <<http://www.distributed.net/pressroom/56-PR.html>>, accessed September 2004.

³¹⁴ Allison and Zelikow, *Essence of Decision*, 24.

dimensions to the information control problem, which in the end would make the problem intractable. Government decisions caused illogical activities, such as restricting the export of encryption technology that was globally available and prohibiting the export of encryption software, but allowing the release of the source code on the Internet.

Believing in technological determinism, actors in the Encryption Technology Group created encryption systems with a single focus on securing valuable economic and privacy information. To entice users with the best technology available, actors in the group gave away or sold strong encryption technology without regard to the complex issues of preserving national security and expanding public safety. I assigned a Problem Perception valance of “0” to the Encryption Technology Group for perceiving a simple information security problem that was uncomplicated by national security and public safety concerns.

C. Favored Alternative Valance

Actors in the Encryption Technology Group favored utility maximizing solutions irrespective of their sources. Users would consider the trustworthiness, reliability, and cost of both government and private sector encryption solutions before choosing the better alternative. Although the 56-bit Data Encryption Standard was twenty years old by the end of the Competitive Period, DES was the primary choice for many users because of its proven capabilities and royalty free licensing. Ms. Helsing from the American Bankers Association discussed their trust in DES during a hearing on the *Computer Security Act of 1987*:

Yet, after more than 10 years in the public domain, no one has yet succeeded in compromising the security afforded by DES. There is no evidence that indicates that the technique is near the point where it could be broken and if there were, there are some simple changes that can be made to the way that DES is used that would dramatically increase the difficulty of the task.³¹⁵

The text shows that the banking industry was satisfied with the performance of DES. Moreover, the text indicates that the banking industry believed in “simple changes” which would “dramatically increase the difficulty of the task” in breaking DES. This belief was in reference to the practice of encrypting information by using Triple DES, which effectively uses three passes through the DES algorithm with two different DES keys. As computing power increased in the early 1990s, Triple DES became more practical, along with public key encryption subsystems that allowed the passing of DES and Triple DES keys between users.

The ultimate utility maximizing solution offered by an actor in the Encryption Technology Group was free of monetary cost, but according to the government, carried a large public cost to national security and public safety. Mr. Zimmermann’s Pretty Good Privacy (PGP) encryption system was freely available from the Internet within a year of its release in 1991. In his testimony to Congress, Mr. Zimmermann revealed his motivation behind this release:

Knowledge of cryptography is becoming so widespread, that export controls are no longer effective at controlling the spread of this technology. People

³¹⁵ Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 113.

everywhere can and do write good cryptographic software, and we import it here but cannot export it, to the detriment of our indigenous software industry.

I wrote PGP from information in the open literature, putting it into a convenient package that everyone can use in a desktop or palmtop computer. Then I gave it away for free, for the good of our democracy. This could have popped up anywhere, and spread. Other people could have and would have done it. And are doing it. Again and again. All over the planet. This technology belongs to everybody.³¹⁶

The text shows that Mr. Zimmermann gave away PGP because he believed it was “good for our democracy.” In an expected statement from a person who supports encryption liberalization, Mr. Zimmermann suggests in the text that encryption “technology belongs to everyone.” Other actors in the Encryption Technology Group did not agree with this statement.

Competitive actions among encryption vendors, electronic rights activists, and technology patent holding companies demonstrated the economic value of the various public key encryption subsystems available in the early 1990s. A 1994 *Wired Magazine* article suggested that Mr. Bidzos of RSA Data Security and Mr. Zimmermann were at odds on the marketability of public key encryption:

In PGP's documentation, Zimmermann called his program “guerrilla freeware.” Jim Bidzos, president of RSA and its sublicensee Public Key Partners, has called Zimmermann “an intellectual property thief. He offered to give away something that wasn't his to give.” The 39-year-old Bidzos, a burly Greek national, could easily pass for a Hollywood version of an arms dealer - and that's how he's categorized under US law, which classifies cryptographic software as “munitions” and forbids its export....

³¹⁶ House Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade and Environment, *Export Controls on Mass Market Software*, 108.

Perhaps so. But, free speech or no, anybody who used early versions of PGP in the United States could be sued - not for trying to protect their privacy, but for patent infringement. The patent for the basic algorithm at the heart of PGP - the RSA public key encryption algorithm - is assigned to MIT, which has licensed it exclusively to RSA Data Security.³¹⁷

The text suggests that electronic rights activists and encryption vendors had different views on the utility maximizing function describing the value of encryption technology. RSA Data Security had licensed the RSA algorithm from its MIT patent holder presumably to make a profit, while Mr. Zimmermann gave away the technology, which allegedly made him an "intellectual property thief." In addition, the text mentions Public Key Partners (PKP), which was a technology patent holding company that was in business with the federal government and the private sector.

Public Key Partners sought to make a profit from public key encryption technology. In a controversial move and perhaps because of legal pressure, the National Institute for Standards and Technology sub-licensed its public key encryption-based Digital Signature Algorithm (DSA) to Public Key Partners. The strategy behind the monopoly building activities of Public Key Partners was to control all the relevant patents on public key encryption technology and to make monopoly profits from the royalties. Public Key Partners did not control the RSA patent, hence the attempted business relationship with RSA Data Security, as mentioned in the *Wired Magazine* article. The *Federal Register*

³¹⁷ Simson L. Garfinkel, "Cypher Wars: Pretty Good Privacy Gets Pretty legal," *Wired Magazine* 2, no.11 (November 1994):129 and 165-66.

notice of the NIST and Public Key Partners deal showed the extent of the planned monopoly:

It is PKP's intent to make practice of the DSA free for personal, non-commercial and U.S. Federal, state and local government use. As explained below, only those parties who enjoy commercial benefit from making or selling products, or certifying digital signatures, will be required to pay royalties for practicing DSA....

Fifth, for the next three (3) years, all commercial services which certify a signature's authenticity for a fee may be operated royalty free. Thereafter, all providers of such commercial certification services shall pay a royalty of \$1.00 per certificate for each year the certificate is valid.³¹⁸

The text suggests that encryption vendors saw the greatest utility and profit from using the public key encryption subsystem was not from "personal, non-commercial and U.S. Federal, state and local government" users, but from commercial royalties and "commercial services which certify a signature's authenticity." These services were electronic libraries that users could obtain the public keys of signatories to verify the authenticity of their digital signatures. Thus by 1993, actors in the Encryption Technology Group realized that certificate authorities for public key encryption provided a valuable service, which commercial users would pay for.

In contrast to using the government's Digital Signature Algorithm that had commercial value, the private sector did not adopt the government's Escrowed Encryption Standard hardware designs because they were not utility maximizing

³¹⁸ U.S. Department of Commerce, National Institute of Standards and Technology, "Notice of Proposal for Grant of Exclusive Patent License," *Federal Register* 58, no. 108 (8 June 1993): 32106.

solutions. These hardware designs, which were often referred to as the CLIPPER or CAPSTONE chip, appealed to privacy and security conscious users because the underlying 80-bit SKIPJACK algorithm was much stronger than the mainstay 56-bit DES. While the 112-bit effective encryption key strength of Triple DES was available to users, the lower efficiency of triple encryption reduced the utility of this option. Competitive alternatives to the Escrowed Encryption Standard were stronger and more flexible commercial designs that could gain the trust of users. One company using a commercial design was Atalla, which supplied encryption equipment for United States automated teller machines. In 1996, Robert G. Garcus, President of Atalla Corporation, testified and gave a prepared statement to Congress on the issue of trust:

In general any key escrow scheme is unacceptable on a worldwide basis. For example, US citizens and corporations will not allow the US government or some designated agency to act as a trusted third party. This bias is cultural and is based on strong beliefs in the rights of privacy of the individual. Some other countries may or may not have this cultural or constitutional basis. In any case, it is very clear through our experience with Clipper that any escrow scheme in which the US government plays any role is almost uniformly unacceptable among both governments and corporations around the world. The result would be that US products would be commercially unacceptable. In today's global economy it is impossible to develop a product that only has US market potential. This means the technology would wither and die.³¹⁹

The text indicates that encryption users would “not allow the US government or some designated agency to act as a trusted third party.” Mr. Garcus’ rationale for this claim was that “culture” and “strong beliefs in the rights of privacy” decreased the utility of

³¹⁹ Senate Committee on Commerce, Science, and Transportation, Subcommittee on Science, Technology and Space, *S. 1726, Promotion of Commerce Online in the Digital Era Act of 1996, or PRO-CODE” Act*, 26 June 1996, 122.

government encryption solutions. If the United States government forced escrowed-key encryption onto the market, then “US products would be commercially unacceptable.” Mr. Garcus proved to be prophetic in his “wither and die” statement as information technology solutions based on the Escrowed Encryption Standard were in market decline by the end of the Competitive Period. What is particularly poignant about his testimony was that the usual detriments to value, such as monopolistic costs from government-sponsored vendors and the loss of software flexibility that would foster competition, played lesser roles than the loss of trust did. Thus, competitive commercial systems dominated the encryption markets in both the private and non-defense government sectors because they were perceived to be more trustworthy.

The favoring of utility maximizing solutions by actors in the Encryption Technology Group matched Allison’s RAM general proposition that decreasing the utility value of a solution “decreases the likelihood of that action being chosen” and his corollary that increasing the utility value of a solution “increases the likelihood of that action being chosen.”³²⁰ The actors in the Encryption Technology Group rallied together against encryption systems based on the government’s Escrowed Encryption Standard. Encryption users perceived such systems to be untrustworthy for use in the private sector, despite the use of these systems in the national security arena for information security and to satisfy counterintelligence and security countermeasure requirements. Thus, information security technology vendors did not face an effective government competitor

³²⁰ Allison and Zelikow, *Essence of Decision*, 25.

and competed among themselves for users desiring lower cost and higher utility solutions. I assigned a Favored Alternative valance of "0" to the Encryption Technology Group for defeating government solutions and for generating utility maximizing solutions to solve the information security problem.

D. Decision Timing Valance

Actors in the Encryption Technology Group were able to use available secret key encryption solutions, such as the government's Data Encryption Standard, during the majority of the Competitive Period. They bought time using this baseline technology and competed against the government's hardware-based Escrowed Encryption Standard with their development of software-based alternatives. Early in the Competitive Period, actors from the Encryption Technology Group had to resist decision initiatives to change the approved encryption technology baseline according to the government's timeline. In 1987, the security arm of the banking industry complained to Congress about the timing of NSA's decision to abandon DES:

This development certainly put the banks in a difficult position. Years of work and many millions of dollars have been devoted to encryption and message authentication efforts and were thus jeopardized. The ABA Data Security Management Committee initiated dialog with the National Security Agency in October 1985 on this issue and we finally reached agreement just last week that NSA would continue to support the financial industry's use of DES-based technology until an acceptable replacement is available.

While we are pleased with that development and that agreement, 16 months have elapsed while we worked to educate NSA about our business. Our industry has lost valuable momentum in adopting improved security technology, and it still

remains to be seen if we can overcome the damage that has been done to the perceived security of DES-based techniques.³²¹

The text shows that the banking industry selected DES as its mainstay encryption algorithm and sought stability after making this choice. According to the text, the instability caused by NSA's suggestion of using a newer encryption solution put at risk "[y]ears of work and many millions of dollars." In addition, the text notes that it took "16 months" for the banking industry to "educate NSA" on the requirements of the banking business. Encryption systems built and updated to satisfy national security requirements were unsatisfactory to the business community. The requirements for an "acceptable replacement" of DES diverged between the government and private sectors early in the Competitive Period.

The Office of Technology Assessment (OTA) did not believe that the private sector could perform the required research and development to produce advanced alternatives to the government's DES. Allegedly, the private sector had the technical talent, but not the organizational influence required to develop universally accepted encryption systems. In 1987, OTA testified before Congress about their concerns on the encryption development monopoly held by government:

The lack of certified cryptographic algorithms, other than those provided by the Government, also limits the flexibility of the private sector. Because DES is certified, vendors and users produce and use it. Now, however, with the prospect of Federal certification being withdrawn, the attractiveness of DES is in serious

³²¹ Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 113-4.

question, and there are no alternative certified algorithms other than offered by NSA. Nor is research underway to develop alternative systems in an open forum in the same way in which DES was developed. Yet, since there are no provably secure cryptographic systems, the only national source for systems to replace those now in use will be NSA. Thus, the pattern now in place is likely to become permanent.³²²

The text suggests that the government controlled the timing on the advancement of encryption technology by withdrawing support for older solutions and by introducing new alternatives. The main rationale for this assessment by OTA was the perceived inability of the private sector to “develop alternative systems in an open forum.” In theory, the competition among encryption vendors would result in secretive and proprietary solutions that would be less secure than a government solution and would not be interoperable. In addition, the text shows that OTA believed NSA’s encryption monopoly and agenda-setting power was “likely to become permanent.” Encryption technology developments in the private sector proved that these beliefs were wrong.

Electronic rights activists in the Encryption Technology Group took actions to release software-based encryption that put the government in a reactionary position. As noted earlier, some encryption vendors tried to gain monopoly positions by controlling the major patents on public key encryption. While this feature of the market seemed to justify OTA’s concern about the inability of the private sector to produce encryption systems open to public scrutiny, the real competition was between the government’s closed Escrowed Encryption Standard and open encryption systems that were in the

³²² *Ibid.*, 224.

public domain. Without open systems, international and domestic consumers would not trust encryption irrespective of its government or commercial origin. In 1991, Mr. Zimmermann decided to demonstrate the relative ease of open development. With an undergraduate degree in computer science, he was able to develop and release source code for a complete encryption system. In his 1993 testimony to Congress, Mr. Zimmermann presented his views on why the private sector should take the initiative and create a replacement for the aging DES:

As word of his results spread throughout the crypto community, you can be sure that the reaction of the world business community is going to be that DES is dead. DES is essentially useless for serious data security applications and we are going to see all of our rivals switching to triple DES, which is a variation using twice as many bits in the key and takes far longer to crack.

That means that if Congress acts now to enable the export of full DES, it is going to be a date late and a dollar short in doing so. Where if we do enable the export of full DES, by the time that happens, all of the overseas rivals will be doing it with triple DES and we will still be in the position we are in right now.

We have to allow the export of as much cryptography as people feel like writing.³²³

The text suggests that people in the early 1990s believed that encryption systems aged precipitously and new systems needed to be continuously developed. With the proclamation “DES is dead,” the text suggests that decisions had to be made on a replacement for DES. One replacement predicted by Mr. Zimmermann was the wholesale “switching to triple DES.” While such a shift suggests that the government could have driven the decision timing with the availability of its Triple DES algorithm,

³²³ House Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade and Environment, *Export Controls on Mass Market Software*, 22-23.

this was not the case, as the government was committed to its hardware-based escrowed-key encryption solution. Mr. Zimmermann's last statement, "We have to allow the export of as much cryptography as people feel like writing," revealed that encryption choices were dependent on the people who developed software. Control of encryption software would result in the control of encryption choices.

The international vetting of encryption algorithms, as instantiated in software code, allowed users and vendors to decide on what type of encryption would be required and when to implement change. The global availability of encryption algorithms and source code transferred control of the decision timing from the United States government to actors in the Encryption Technology Group. One individual from this group, Mr. Bruce Schneier, published the definitive reference on encryption algorithms and source code. The preface of Mr. Schneier's *Applied Cryptography: Protocols, Algorithms, and Source Code in C* lauded the power of open source encryption algorithms:

This book is being published in a tumultuous time. In 1994, the Clinton administration approved the Escrowed Encryption Standard (including the Clipper chip and Fortezza card) and signed the Digital Telephony bill into law. Both these initiatives try to ensure the government's ability to conduct electronic surveillance....

The lesson here is that it is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics. Encryption is too important to be left solely to governments.

This book gives you the tools you need to protect your own privacy; cryptography products may be declared illegal, but the information will never be.³²⁴

The text indicates that Mr. Schneier was concerned about government policies on encryption control. The Digital Telephony bill he referenced was the *Communications Assistance to Law Enforcement Act*, which encouraged telecommunications providers to assist with government wiretap efforts. His statement, "Encryption is too important to be left solely to governments," suggests that the initiative for encryption decisions should be with the private sector. One method to take the initiative was the distribution of information about "the tools you need to protect your own privacy." Mr. Schneier was using his First Amendment rights to provide information on encryption. When electronic rights activists tried to extend this right to source code and digital source code, the government reacted.

Realizing that a loss of initiative for making encryption decisions was occurring, the government mounted legal attacks and counterattacks on electronic rights activists seeking to release digital versions of source code for encryption algorithms. Three major federal court cases on encryption control, *Bernstein v. United States Department of State*, *Junger v. Daley*, and *Karn v. United States Department of State*, had their origins in the Competitive Period. As noted earlier, only the Bernstein case produced a significant ruling in that the First Amendment protected source code. The issue regarding digital source code was trivial in the sense that some one could legally type the source code into

³²⁴ Schneier, *Applied Cryptography*, xx.

a computer from Mr. Schneier's book, but could not export a computer diskette with the source code in digital form. From an organizational behavior perspective, government agencies saw exported digital source code as possible violations of the *Arms Export Control Act*, the *Export Administration Act of 1979*, and numerous presidential directives and orders. A definitive ruling by the United States Supreme Court would have decided the control of software-based encryption technology. However, the courts cycled these cases between the circuit and appellate levels and made and unmade decisions:

It should be emphasized that with the exception of its conclusions that source code is speech for the purposes of the First Amendment and that this case is justiciable, the court makes no other substantive holdings.³²⁵

The text indicates the firmness of the "source code is speech" finding and the reluctance to adjudicate a challenge to executive branch regulations, even on the trivial aspect of digital source code. These court cases did deter information control efforts by the executive branch, because national security and public safety concerns prevented summary dismissals of these cases and perpetuated cycling of these cases between lower and higher federal courts. Likewise, these cases did not stop the development of new encryption technology in the private sector. However, by the end of the Competitive Period, actors from the Encryption Technology Group dominated the creation of encryption technology choices.

³²⁵ *Bernstein v. United States Department of State, et al.*, 922 F. Supp. 1439 (N.D. Cal. 1996).

The timing of decisions by actors in the Encryption Technology Group matched Allison's RAM general proposition that the "likelihood of any particular action" is dependent upon the "perceived alternative courses of action."³²⁶ These actors realized that the government had the decision initiative with the retirement of DES because of the first-mover trust placed in government encryption standards. Thus, these actors fought the blind acceptance of government standards with public testimony and activism. They were able to gain the initiative when the government made mistakes by developing a hardware-based escrowed-key encryption alternative and by using a closed development process that aroused public suspicion. Actors in the Encryption Technology Group countered with software-based encryption alternatives that were developed in the open. Mr. Zimmermann's giveaway of Pretty Good Privacy and the claim by electronic rights activists that encryption source code was a form of protected speech forced the government to use the judicial system in an attempt to regain the decision initiative. Ambiguous rulings wasted time, and the more liberal courts sided with the electronic rights activists. Time, a distrust of government solutions, and the inability of a democratic government to control information about encryption technology allowed the private sector to produce encryption choices that out competed the government's escrowed-key encryption offering. I therefore assigned a Decision Timing valance of "0" to the Encryption Technology Group for setting their own decision timing by creating their own encryption technology choices.

³²⁶ Allison and Zelikow, *Essence of Decision*, 25.

Executive Group

In the Competitive Period, the primary actors in the Executive Group affecting information and encryption control policies were the president, the Assistant to the President for National Security Affairs (National Security Advisor), the Secretaries of Commerce, Defense, and State, and the Attorney General. The president and his National Security Advisor used executive orders and directives as information control policies that generally favored national security and public safety requirements over economic and privacy concerns. During this period, dramatic changes in the international environment, such as the end of the Cold War, were the causes of inconsistent executive branch actions and decisions. Thus, the federal departments implemented their best guesses at information control policies in a dynamic environment and without the support of specific laws from Congress. While the executive branch introduced the complex concept of unclassified but sensitive information near the end of the First Mover Period, it took several years before the ramifications of this concept became apparent. The Competitive Period ended with an encryption policy crescendo predicated on the success of escrowed-key encryption. The government would provide all users with a complete encryption system that featured a strong encryption algorithm. This algorithm was of military strength and was used to secure classified national security information. The qualifier was that the government would have guaranteed access to information by keeping copies of the encryption keys. Executive orders, directives, international arrangements, and congressional testimony from leaders in all sectors provided the data

for analyzing the actions of the Executive Group. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

The administrations of Presidents Reagan, George H. W. Bush, and Clinton used the national security importance of information control to instigate governmental actions. While the constitutional prerogative of the president to ensure national security sometimes drove presidential actions, more often, technically astute members from the National Security Council System originated information control policies for the president. President Reagan's National Security Decision Directive 145 (NSDD-145) was significantly expanded to cover information control by his National Security Advisor, Rear Admiral Poindexter. This directive and its expansion did not produce significant effects in the First Mover Period, as it took several years before these decisions affected the non-defense federal and private sectors. Dr. Christie D. Vernon, representing the American Library Association, discussed this delay in her testimony before Congress:

Mr. HORTON. Why do you think it's taken so long for people such as yourself to respond to NSDD-145?

Dr. VERNON. Well, of course, it was promulgated secretly, as all the other people have testified they didn't know anything about it....

Mr. HORTON. Was it on a library computer system?

Dr. VERNON. It wasn't. And then, of course, they gave assurances that it really didn't mean what we thought it said it meant. Then we had to wait another year and a half until this NTSSIP [NTISSP – National Telecommunications and Information System Security Policy] No. 2 came out. We found that it means not

only what we thought it meant, but other things in addition that we are just now beginning to be able to respond to, as the others are.³²⁷

The text shows that Admiral Poindexter's National Telecommunications and Information System Security Policy No. 2 followed NSDD-145 by over a year.³²⁸ While this testimony explains the latency of the effects caused by NSDD-145 and NTISSP No. 2, few people in the non-defense government sector and the private sector appreciated the threats posed by digital information.

NSDD-145 drove government forays into information control efforts during the first three years of the Competitive Period until this policy was modified in 1990. In its introductory paragraph, NSDD-145 tasked national security actors within the executive branch with the responsibility for protecting sensitive but unclassified information in all sectors:

Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation.³²⁹

³²⁷ Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 199.

³²⁸ *Ibid.*, 604-607.

³²⁹ Ronald Reagan, National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security," 17 September 1984: 1.

The text shows that NSDD-145 portrayed the “foreign exploitation” efforts on “[g]overnment systems as well as those which process the private or proprietary information of US persons and businesses” as principal threats to national security. Irrespective of the credibility of these threats, NSDD-145 was a source of suspicion by Congress and the private sector because of the extent of executive branch power that would be required to control information in all sectors.

In 1990, President George H. W. Bush issued National Security Directive 42 (NSD-42), National Policy for the Security of National Security Telecommunications and Information, which restricted NSDD-145 activities to the national security arena and rescinded the broad information protection mission. The new introductory paragraph reflected this change:

Telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. A comprehensive and coordinated approach must be taken to protect the government's national security telecommunications and information systems (national security systems) against current and projected threats.³³⁰

The text suggests that the Bush administration viewed government information control as pertaining to “national security systems” or systems containing classified information. This change of perception agreed with the *Computer Security Act of 1987* in that the

³³⁰ George H. W. Bush, National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” 5 July 1990: 1. Redacted version, April 1992.

Department of Commerce was in charge of computer security for protecting unclassified information. In a parallel fashion, the Bush administration was satisfied with the Secretary of State controlling exports of information security tools containing encryption technology, in accordance with national security requirements. The Clinton administration perceived a different role for the government.

The Clinton administration believed that the government should manage information access and information security requirements for the government and private sectors. In 1993, Presidential Decision Directive / National Security Council 5 (PDD/NSC-5) stated the government's policy for "Public Encryption Management" in an open manner and without hiding the government's intent behind a national security classification barrier:

Advanced telecommunications and commercially available encryption are part of a wave of new communications and computer technology. Encryption products scramble information to protect the privacy of communications and data by preventing unauthorized access. Advanced telecommunications systems use digital technology to rapidly and precisely handle a high volume of communications. These advanced telecommunications systems are integral to the infrastructure needed to ensure economic competitiveness in the information age.

Despite its benefits, new communications technology can also frustrate lawful government electronic surveillance. Sophisticated encryption can have this effect in the United States. When exported abroad, it can be used to thwart foreign intelligence activities critical to our national interests. In the past, it has been possible to preserve a government capability to conduct electronic surveillance in furtherance of legitimate law enforcement and national security interest, while at the same time protecting the privacy and civil liberties of all

citizens. As encryption technology improves, doing so will require new, innovative approaches.³³¹

This text acknowledges that “in the past,” the government was able to “preserve a government capability to conduct electronic surveillance.” This statement applied to the uses of the Data Encryption Standard and equivalent technologies and suggested a government capability to defeat 56-bit DES. The text also implies that government action was required to maintain this information access capability into the future when “encryption technology improves.” No presidential directive prior to PDD/NSC-5 had documented a requirement for guaranteed access to protected information residing in the private sector. While such access requirements are common in the government sector to facilitate communications security monitoring and counter-intelligence activities, PDD/NSC-5 applied to all sectors, produced divisive effects in Congress, and caused deep suspicion with actors in the Encryption Technology Group.

PDD/NSC-5 made it more difficult to pass export control legislation because addressing the subject of encryption exports often hindered the legislative process. Congress had allowed export legislation to lapse, and the executive branch believed that government intervention was necessary to maintain past precedents. The standard method of government intervention was to use national security considerations as justification for the continuance of past regulations. As an example, in 1994 President

³³¹ William J. Clinton, Presidential Decision Directive / NSC 5, “Public Encryption Management,” 15 April 1993: 1. Copy obtained from the National Security Council archives by the Air University Library, Maxwell Air Force Base, Alabama.

Clinton had to intervene when Congress failed to update the *Export Administration Act of 1979*:

By the authority vested in me as President by the Constitution and the laws of the United States of America, including but not limited to section 203 of the International Emergency Economic Powers Act ("Act") (50 U.S.C. 1702), I, WILLIAM J. CLINTON, President of the United States of America, find that the unrestricted access of foreign parties to U.S. goods, technology, and technical data and the existence of certain boycott practices of foreign nations, in light of the expiration of the Export Administration Act of 1979, as amended (50 U.S.C. App. 2401 *et seq.*), constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States and hereby declare a national emergency with respect to that threat.³³²

The text demonstrates how President Clinton used the *International Emergency Economic Powers Act* and threats to the "national security, foreign policy, and economy of the United States" to declare a "national emergency." By doing so, the president was able to direct the regulatory activities of government while Congress worked on renewing export legislation. In addition to direct actions by the president, other actors in the Executive Group attempted to steer Congress away from laws that would relax government control of allegedly dangerous technologies.

In 1997, Attorney General Janet Reno sent a letter to Congress warning about the government's responsibility in the encryption control area:

We fully recognize that encryption is critical to communications security and privacy, and that substantial commercial interests are at stake. Perhaps in recognition of these facts, all the bills being considered allow market forces to

³³² President, Executive Order 12923, "Continuation of Export Control Regulations," 30 June 1994, *Federal Register* 59, no. 127 (5 July 1994): 34551-2.

shape the development of encryption products. We, too, place substantial reliance on market forces to promote electronic security and privacy, but believe that we cannot solely rely on market forces to protect the public safety and national security. Obviously, the government cannot abdicate its solemn responsibility to protect public safety and national security.³³³

The text shows that an influential member of President Clinton's cabinet believed that "market forces" could not "protect public safety and national security." Attorney General Reno succinctly placed this protection responsibly with the government. The text is also purposefully ambiguous in that the Attorney General is simultaneously arguing for the use of encryption to ensure information security and for government access to information protected by encryption.

The view of the government as the lead actor by the Executive Group matched Allison's GPM organizing concept of "Players in Positions."³³⁴ In this concept, actors in the Executive Group are individuals that "become players in the national security policy game by occupying a position in the major channels for producing action."³³⁵ During three administrations that spanned the Competitive Period, presidents and their national security staffs consistently acted to control unclassified but sensitive information in the same manner used to control classified national security information. While Congress believed that they had the lead in protecting government information through laws, actors in the Executive Group took actions to control information in all sectors and to control the encryption tools that could deny government access to information. The failure of

³³³ U.S. Department of Justice, Office of the Attorney General, Letter to Congress by Janet Reno. Washington, D.C., 18 July 1997, 1.

³³⁴ Allison and Zelikow, *Essence of Decision*, 296.

³³⁵ *Ibid.*, 296.

Congress to pass export legislation on encryption technology reinforced the activities of the executive branch in controlling domestic information security technology through a series of directives. I therefore assigned a Lead Actor valance of "2" to the Executive Group for perceiving a government responsibility to protect national security and to ensure public safety by securing and accessing unclassified but sensitive information.

B. Problem Perception Valance

Actors in the Executive Group perceived a complex information control problem that had national security, international, economic, public safety, and technology leadership dimensions. The National Security Advisor to President Reagan, Rear Admiral Poindexter, was accused by Congress of extending NSDD-145 to cover information in the private sector. Admiral Poindexter did not answer questions on the national security threat to unprotected information, but his assistant, Kenneth E. deGraffenreid did. In his 1987 testimony to the House Legislation and National Security Subcommittee, Mr. deGraffenreid discussed the problem posed by sensitive but unclassified information:

Today, I will address briefly the threat to our national security that we see from hostile intelligence services in the context of its relation to computer and telecommunications security. After touching on why NSDD 145 was written, what NSDD 145 is, and also what it is not, I would be happy to attempt to respond to any questions you may have.

We have some difficulty in this country talking about the hostile intelligence threat in recent years. It is important to comment on this difficulty and tell how this administration came to perceive the problem. First of all, we have difficulty talking about this threat because of a basic American aversion to what might be called the seamier side of international politics. Treason, subversion,

subordinations, betrayal, theft, reading other people's mail, intercepting their communications and sneaking into computers are not pleasant subjects. They are, however, very much a part of international politics, and particularly of the intelligence threat that faces our country.³³⁶

The text indicates that the perceived threat to national security was primarily from "hostile intelligence services" and that this threat was "very much a part of international politics." Also revealing in this text was the promised explanation of "how this administration came to perceive the problem," because some of the words used in the text suggest that people on the inside were committing treasonous acts. The perception that insiders posed a major threat to national security was downplayed, but not eliminated by the administration of President George H. W. Bush.

President Bush signed National Security Directive 42 on July 5, 1990. Under continued pressure from Congress to limit government information control activities in the private sector, NSD-42's objectives were focused on the information security problem found in the national defense government sector:

1. Objectives. Ensuring the security of national security systems is vitally important to the operational effectiveness of the national security activities of the government and to military combat readiness. I therefore, direct that the government's capabilities for securing national security systems against technical exploitation threats be maintained or, if inadequate, improved ...³³⁷

³³⁶ U.S. House, Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 407.

³³⁷ George H. W. Bush, National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," 5 July 1990: 1.

The redacted text uses the term “national security systems” in the “Objectives” paragraph, and the NSD-42 definition of this term was “telecommunications and information systems operated by the U.S. Government, its contractors, or agents that contain classified information.”³³⁸ NSD-42 appeared to address a legitimate national security problem within the policy purview of the executive branch. However, a classified directive issued four months after NSD-42 showed a dramatic broadening of this information control policy.

National Security Directive 47 (NSD-47) covered the counterintelligence (CI) and security countermeasures (SCM) areas, which involved activities used to catch spies, foreign agents, and their proxies operating in the United States. An examination of a declassified version of NSD-47 showed that this document covered offensive and defensive aspects of CI and SCM. On the offensive side, NSD-47 directed the following activities:

- Enhance our ability to make early identification of U.S. persons who volunteer to commit espionage and refer those cases to the appropriate agency to pursue investigation and prosecution. (C)
- censored
- censored
- censored
- Use our control of the domestic environment to anticipate, detect, and disrupt efforts by foreign intelligence services to exploit new operational opportunities in the United States. (C)
- censored

³³⁸ *Ibid.*, 9.

- Improve the focus and integration of CI analysis into operational targeting programs. (S)
- Build new Automated Data Processing capabilities using expert systems and artificial intelligence to better support interagency analytical exploitation of data bases. (S)
- Mount aggressive programs to enable us to identify and operate against foreign government-sponsored or government-subsidized operations targeted against U.S. technological and economic competitiveness. (S)³³⁹

The declassified text suggests that in order to protect national security, the government required access to information from all the sectors in the United States. Two controversial information control activities in NSD-47 are found in the phrases “control of the domestic environment” and “analytical exploitation of data bases.” These phrases coupled with the targets of espionage, which were “U.S. technological and economic competitiveness,” implied that CI and SCM activities included intelligence gathering within the United States and against the private sector. President Clinton’s administration did not hide the requirement for these activities in a classified document.

Starting in the domestic area, President Clinton directed the Attorney General and the Secretary of Commerce to follow his policy on the information access and security problem. In 1993, President Clinton issued PDD/NSC-5, which was unclassified and available to the public. PDD/NSC-5 directed the enforcement and implementation of escrowed-key encryption solutions in the government and private sectors:

INSTALLATION OF GOVERNMENT-DEVELOPED MICROCIRCUITS

³³⁹ George H. W. Bush, National Security Directive 47, “Counter Intelligence and Security Countermeasures,” 5 October 1990: 2-3. Declassified copy dated December 1996.

The Attorney General of the United States, or her representative, shall request manufacturers of communications hardware which incorporates encryption to install the U.S. government-developed key-escrow microcircuits in their products. This fact of law enforcement access to the escrowed keys will not be concealed from the American public....

PROCUREMENT AND USE OF ENCRYPTION DEVICES

The Secretary of Commerce, in consultation with appropriate U.S. Agencies, shall initiate a process to write standards to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits in federal communication systems that process sensitive, but unclassified information.³⁴⁰

The text indicates that the executive branch viewed itself as being responsible for solving the domestic encryption control problem. The text also indicates the desire of President Clinton to have "U.S. government-developed key-escrow microcircuits" dominate the domestic market. One method to ensure the spread of government-preferred encryption technology was to have the "Secretary of Commerce, in consultation with appropriate U.S. Agencies," create a government encryption standard. The resulting Escrowed Encryption Standard would be the subject of great suspicion because of the mandated participation by the National Security Agency. With the complex domestic information control problem apparently solved by a simple escrowed encryption solution, the executive branch thought it could work on the more difficult international aspects of this problem.

With the collapse of the Soviet Union and the rise of unipolar United States power, the Clinton administration was in a position to drive global information control policy

³⁴⁰ William J. Clinton, Presidential Decision Directive / NSC 5, "Public Encryption Management," 15 April 1993: 2.

through the network effects produced by standardized United States encryption. The global legacy of the Data Encryption Standard could have been repeated, thereby globally suppressing the use of competitive encryption systems. However, President Clinton perceived the information control problem to be an international responsibility. This perception change from the two prior administrations reflected President's Clinton's liberalist international relations approach that favored multilateral actions and international laws over a power-based realist approach. For example, in his 1997 National Security Strategy of the United States, President Clinton touted his multilateral approach to control dual-use technologies such as encryption:

The Administration also seeks to limit access to sensitive equipment and technologies through participating in and fostering the efforts of multilateral regimes, including the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, the Australia Group (for chemical and biological weapons), the Missile Technology Control Regime (MTCR), and the Nuclear Suppliers Group. We are working to harmonize national export control policies, increase information sharing, refine control lists and expand cooperation against illicit transfers.³⁴¹

The text shows a dramatic shift in direction with the executive branch moving away from unilateral control of unclassified information, such as dual-use technology information, and toward regime control of dual-use technology information and information security technologies. Hence, this National Security Strategy treated dual-use information technology exports, chemical and biological weapons, missiles, and nuclear weapons in a combined fashion. Securing multilateral agreements among interacting actors and

³⁴¹ The White House, *A National Security Strategy for a New Century* (Washington, D.C.: GPO, May 1997), 8.

organizations in a process known as “regime building” added to the complexity of the information control problem. Internal to the United States, these international actions partially addressed national security concerns but did not address public safety concerns on information control.

Attorney General Janet Reno followed President Clinton’s lead by openly writing to Congress in 1997 about requirements for encryption control legislations. The Attorney General perceived an encryption control problem that threatened public safety as well as national security:

In sum, while encryption is certainly a commercial interest of great importance to this Nation, it is not solely a commercial or business issue. Those of us charged with the protection of public safety and national security, believe that the misuses of encryption technology will become a matter of life and death in many instances. That is why we urge you to adopt a balanced approach that accomplishes the goals mention above. Only this approach will allow police departments, attorneys general, district attorneys, sheriffs, and federal authorities to continue to use their most effective investigative techniques, with court approval, to fight crime and espionage and prevent terrorism.³⁴²

The text focuses on encryption as a tool of information control and the hazards of relying on business and market controls for this tool. Attorney General Reno called for a “balanced approach” which involved legalized encryption key management and key recovery schemes run by the government.³⁴³ These proposed solutions favored the government’s side and overlooked the complex problem of satisfying private sector requirements for trustworthy, competitive, and marketable encryption products. With a

³⁴² U.S. Department of Justice, Office of the Attorney General, Letter to Congress by Janet Reno. Washington, D.C., 18 July 1997, 4.

³⁴³ *Ibid.*, 3-4.

lack of congressional support for Attorney General Reno's plea, the executive branch was on its own in ensuring policy congruency between the international and domestic aspects of encryption control.

The view of a complex problem by the Executive Group matched Allison's GPM organizing concept of the "Rules of the Game" where "rules constrict the range of governmental decisions and actions that are acceptable."³⁴⁴ During the Cold War administrations of Presidents Reagan and Bush, actors in the Executive Group perceived a dominant national security threat to the United States caused by international and domestic access to sensitive but unclassified information. While information security tools such as encryption could have alleviated this problem, an underlying government information access problem for counterintelligence and security monitoring purposes dominated policy decisions. Following the rules directed by laws such as the *Computer Security Act of 1987*, actors in the Executive Groups found it impractical to classify all sensitive but unclassified information at the appropriate national security level and lost easy access to privacy information. Domestic information access would have to be achieved through secretive rules issued by the president.

The end of the Cold War allowed the Clinton administration to create and follow a new set of international technology and information control rules. However, on the domestic side of the information control problem, the Clinton administration sided with satisfying national security and public safety requirements over market control of

³⁴⁴ Allison and Zelikow, *Essence of Decision*, 302.

information security technologies such as encryption. The public acknowledgment of the information access dilemma faced by the government did not convince actors in Congress and the private sector that new rules were required. Public acknowledgement did galvanize opposition to government information control activities. Thus, the Attorney General and the Secretary of Commerce had to face a complex information control problem with the same rules used by the two prior administrations. They now also faced hostile actors from the Encryption Technology Group. I therefore assigned a Problem Perception valance of "2" to the Executive Group for perceiving a complex information control problem with different international and domestic dimensions and with an elusive information access and security balance.

C. Favored Alternative Valance

Actors in the Executive Group believed that presidential directives and orders based on past precedents were required to protect unclassified national security information, while preserving government access to this information for counterintelligence and law enforcement purposes. Instead of working with Congress for laws to support the control of sensitive but unclassified information, the executive branch gambled on a single escrowed-key encryption alternative. During the Competitive Period, the buildup to this gamble started with actions by President Reagan's National Security Advisor.

Actors in the Executive Group preferred to use presidential directives as policy tools because such directives followed historical precedence and did not require congressional approval. The congressional examination of NSDD-145 and its extensions

by the National Security Advisor provided an example of the unilateral power found in executive branch directives. In a committee hearing, members analyzed NSDD-145 and its peripheral policies such as NTISSP No. 2, National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems:

SECTION II – DEFINITION

Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. government by its citizens.³⁴⁵

This policy by the System Security Steering Group was signed by Admiral Poindexter and was included in the record of the congressional hearing for scrutiny. The text shows the broad definition of a new class of information as being “related, but not limited to the wide range of government or government derived economic, human, financial, industrial, agricultural, technological, and law enforcement.” With such a broad definition, the committee questioned the potential for over-control of information.

Chairman Brooks directly asked Assistant Secretary of Defense Latham a question on the expanse of this new class of information:

³⁴⁵ Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 606.

Question: Given the expansiveness of the Poindexter Directive, what information would be excluded from the definition of sensitive information?

Answer: Sensitive but unclassified information, as defined by the “Poindexter Directive,” is not classified and is not subject to the procedures and safeguards applied to classified information. Individual department and agency heads are given the discretion of deciding which of their respective department’s or agency’s information is sensitive and should be protected.³⁴⁶

The text shows that Congress scrutinized even a benign section on the definition of sensitive but unclassified information in an attempt to determine the policy implications. In addition, the text demonstrates how executive branch policy directives influenced “department and agency heads” and how broadly defined policy authority or “discretion” caused congressional alarm.

In response to the Reagan administration issuance of NSDD-145 and questionable executive branch promulgations of subsidiary policies, a report by the Congressional Research Service (CRS) in support of the *Computer Security Act of 1987* highlighted concerns about presidential directives:

Legislative and judicial scrutiny is undermined when the administration announces policy not by Executive Order but by instruments that are not made public. Whether these instruments are called Presidential Directives (PD’s), National Security Decision Directives (NSDD’s), or designated in some other manner is unimportant. The significant fact is that these directives skirt public, congressional, and judicial controls.

In addition, secret executive directives can lead to inconsistencies and noncompliance within the administration. Although the presidency was created to supply unity to the government, the adoption of secret policies produces disunity

³⁴⁶ *Ibid.*, 307.

and fragmentation within the administration. The executive branch ends up operating at cross-purposes because one part knows not what the other is doing.³⁴⁷

The text shows that the CRS found sufficient evidence in the historical record to dissuade the Reagan and future administrations from using presidential directives. Despite the CRS warning of possible “disunity and fragmentation within the administration,” successive administrations have followed past precedents and continue to use directives as expedient, but potentially divisive, policy tools.

The administration of President George H. W. Bush favored separate policy directives that focused on one issue at a time. National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information, focused on protecting national security systems:

This Directive establishes initial objectives of policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation. It is intended to ensure full participation and cooperation among the various existing centers of technical expertise throughout the Executive branch, and to promote a coherent and coordinated defense against the foreign intelligence threat to these systems. This Directive recognizes the special requirements for protection of intelligence sources and methods.³⁴⁸

The text shows that the Bush administration favored a policy alternative that would “secure national security systems” and not information in the non-defense federal and private sectors. The text also shows that this directive was targeted to “centers of

³⁴⁷ *Ibid.*, 442.

³⁴⁸ George H. W. Bush, National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” July 5, 1990: 1.

technical expertise throughout the Executive branch,” which under the *Computer Security Act of 1987* meant the Commerce Department’s National Bureau of Standards and the Defense Department’s National Security Agency.

President Bush selected another directive, NSD-47, to focus the counterintelligence (CI) and security countermeasures (SCM) activities in the government and private sectors. However, NSD-47 suffered the fragmentation consequences predicted by the Congressional Research Service by not vetting all the policy tasks and information with actors both inside the executive branch and in Congress. According to NSD-47, actors in the executive branch had to “work closely with Congress on CI and SCM legislation seeking to improve U.S. Government capabilities in these areas.”³⁴⁹ The detailed tasking directive placed the Director of Central Intelligence (DCI) in charge of implementing NSD-47 in accordance with the results of another policy document: “I hereby direct the recipients of this memorandum [NSD-47] to implement the recommendations cited in NSR-18 and charge the Director of Central Intelligence, under guidance from the National Security Council, with coordinating interagency effort toward these goals.”³⁵⁰ National Security Review 18 (NSR-18) was a study effort launched a year before NSD-47 and did not contain recommendations.³⁵¹ This coupling of directives and reviews was a potential source of confusion within the executive branch and obfuscated law-making information required by external actors such as Congress.

³⁴⁹ George H. W. Bush, National Security Directive 47, “Counter Intelligence and Security Countermeasures,” 5 October 1990: 4.

³⁵⁰ *Ibid.*, 5.

³⁵¹ George H. W. Bush, National Security Review 18, “Counter Intelligence and Security Countermeasures,” 22 June 1989: 1-2.

President Clinton favored presidential decision directives to set policy and continued to use separate paths for directives and reviews. To alleviate fragmentation concerns, the Clinton administration better communicated policy documents by publishing them in an unclassified format when possible. Presidential Decision Directive / NSC-5 was the first unclassified directive that publicly set United States Government encryption policy:

In the area of communications encryption, the U.S. government has developed a microcircuit that not only provides privacy through encryption that is substantially more robust than the current government standard, but also permits escrowing of the keys needed to unlock the encryption. The system for this escrowing of keys will allow the government to gain access to encrypted information only with appropriated legal authorization.

To assist law enforcement and other government agencies to collect and decrypt, under legal authority, electronically transmitted information, I hereby direct the following action to be taken:³⁵²

The text shows explicitly the presidential direction to use a “microcircuit” that “permits escrowing of the keys needed to unlock the encryption.” While this direction did not have the force of law, it alerted and motivated actors in the executive branch to support the ongoing development of the Escrowed Encryption Standard. The explicit and public nature of PDD/NSC-5 alienated much of Congress, but not to the extent of responding with legislation to ban federally mandated escrowed-key encryption.

³⁵² William J. Clinton, Presidential Decision Directive / NSC 5, “Public Encryption Management,” 15 April 1993: 1.

As Congress periodically allowed export legislation to lapse, the Clinton administration took advantage of these opportunities to change public policy through emergency executive orders. While such orders were supposed to create “interim rules” until Congress acted, the Clinton administration used Executive Order 13026 to change statutory and regulatory responsibilities. This order transferred control of encryption technology from the Department of State to the Department of Commerce, and Congress did not challenge the results with timely intervention:

(b) Executive Order 12981, as amended by Executive Order 13020 of October 12, 1996, is further amended as follows:

(1) A new section 6 is added to read as follows: “Sec. 6. *Encryption Products*. In conducting the license review described in section 1 above, with respect to export controls of encryption products that are or would be, on November 15, 1996, designated as defense articles in Category XIII of the United States Munitions List and regulated by the United States Department of State pursuant to the Arms Export Control Act, 22 U.S.C. 2778 *et seq.*, but that subsequently are placed on the Commerce Control List in the Export Administration Regulations, the Departments of State, Defense, Energy, and Justice and the Arms Control and Disarmament Agency shall have the opportunity to review any export license application submitted to the Department of Commerce. The Department of Justice shall, with respect to such encryption products, be a voting member of the Export Administration Review Board described in section 5(a)(1) of this order and of the Advisory Committee on Export Policy described in section 5(a)(2) of this order. The Department of Justice shall be a full member of the Operating Committee of the ACEP described in section 5(a)(3) of this order, and of any other committees and consultation groups reviewing export controls with respect to such encryption products.”³⁵³

The text shows that a complex sequencing of Executive Orders 12981, 13020, and 13026, was required to change the regulation of encryption technology from the Department of

³⁵³ President, Executive Order 13026, “Administration of Export Controls on Encryption Products,” 15 November 1996, *Federal Register* 61, no. 224 (19 November 1996): 58767-8.

State's "United States Munitions List" to the Department of Commerce's "Commerce Control List." While some researchers may consider this change to be a new encryption control regulation, the text indicates that Congress did not instigate this rearrangement and that the executive branch followed the past precedent of issuing emergency executive orders to accomplish this change.

The failure of the executive branch to get congressional approval on encryption control made it difficult for the president to negotiate international treaties or agreements, as the likelihood of ratification in the Senate would be low. In 1996, President Clinton simply notified Congress of his actions when he negotiated the Wassenaar Arrangement on dual-use technology:

4. Since my last report to the Congress, there have been several significant developments in the area of export controls:

A. MULTILATERAL DEVELOPMENTS

Wassenaar Arrangement for Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The Bureau of Export Administration (BXA) of the Department of Commerce participated in several rounds of negotiations to establish a successor regime to COCOM. On December 19, 1995, 28 countries (former COCOM partners, cooperating countries, Russia, and the Visegrad states) agreed to establish a new regime, called the Wassenaar Arrangement, to control conventional arms and munitions and related dual use equipment. The Wassenaar Arrangement will be headquartered in Austria. The first plenary meeting of the new regime was held in Vienna in April 1996.³⁵⁴

The text shows that the Wassenaar Arrangement required the Department of Commerce to participate in "several rounds of negotiations," even though Congress failed to pass

³⁵⁴ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 80: S5758.

H.R. 361 authorizing this specific activity. The result was a negotiated supranational arrangement not directly supported by public law.

Actors in the Executive Group favored the use of directives and orders to solve the information control problem. Through the Reagan, Bush, and Clinton administrations, these directives and orders became more focused on encryption control solutions and more candid with the public on the rationale behind encryption control. These efforts were targeted to build public trust in the escrowed-key encryption alternative selected by President Clinton and to convince Congress to produce legislations that were required for the mandatory use of escrowed-key encryption. Without the force of law, the results of information control directives and orders were hardware implementations of escrowed-key encryption devices that were commonplace in the national security sector, but were not competitive in the private sector. This sequence of actions matched Allison's OBM general proposition that "Implementation Reflects Previously Established Routines" where the evolved alternative was not a "far sighted, adaptation to 'the issue.'"³⁵⁵ The continued issuances of directives and orders did not produce an encryption control solution that was acceptable to Congress or to the private sector. Congress saw the solution as a threat to its political power and the private sector favored cheaper and more flexible software encryption systems. I therefore assigned a Favored Alternative valance of "1" to the Executive Group for following past precedents, which culminated in the Escrowed Encryption Standard.

³⁵⁵ Allison and Zelikow, *Essence of Decision*, 178.

D. Decision Timing Valance

Actors in the Executive Group believed that urgent decisions were required to solve the information control problem. The sudden end of the Cold War and the gradual availability of private sector encryption systems drove the timing of executive branch decisions. NSDD-145 was issued in 1984, at the climax of the Cold War against what President Reagan described as an “Evil Empire.” Government and private sector ramifications of protecting sensitive but unclassified information drove Congress to pass the *Computer Security Act of 1987* as a partial response to NSDD-145. However, actors in the Executive Group saw this law as possibly supportive of the administration’s position. In March 1987, Howard H. Baker, Chief of Staff to President Reagan, sent an urgent letter to Committee Chairman Jack Brooks during a hearing on this act:

Frank Carlucci and I have discussed his letter that was sent to you last week on the matter of computer security policy.

He has moved promptly to rescind the policy directive which you cited as troublesome, and bearing in mind the point you have articulated so clearly, will act promptly to review the provisions of the NSDD [145] itself.

In addition, the Administration will propose certain changes to the legislation before your Committee, which if adopted, would satisfy our national security concerns.³⁵⁶

The text shows that “provisions of the NSDD” were related to “certain changes to the legislation” being considered. Thus, the *Computer Security Act of 1987* carried certain

³⁵⁶ House Committee on Government Operations, Legislation and National Security Subcommittee, *Computer Security Act of 1987*, 387.

parts of NSDD-145 and its subsidiary directives well into the 1990s. Figure 4-5 displays this propagation of President Reagan's information control policy.

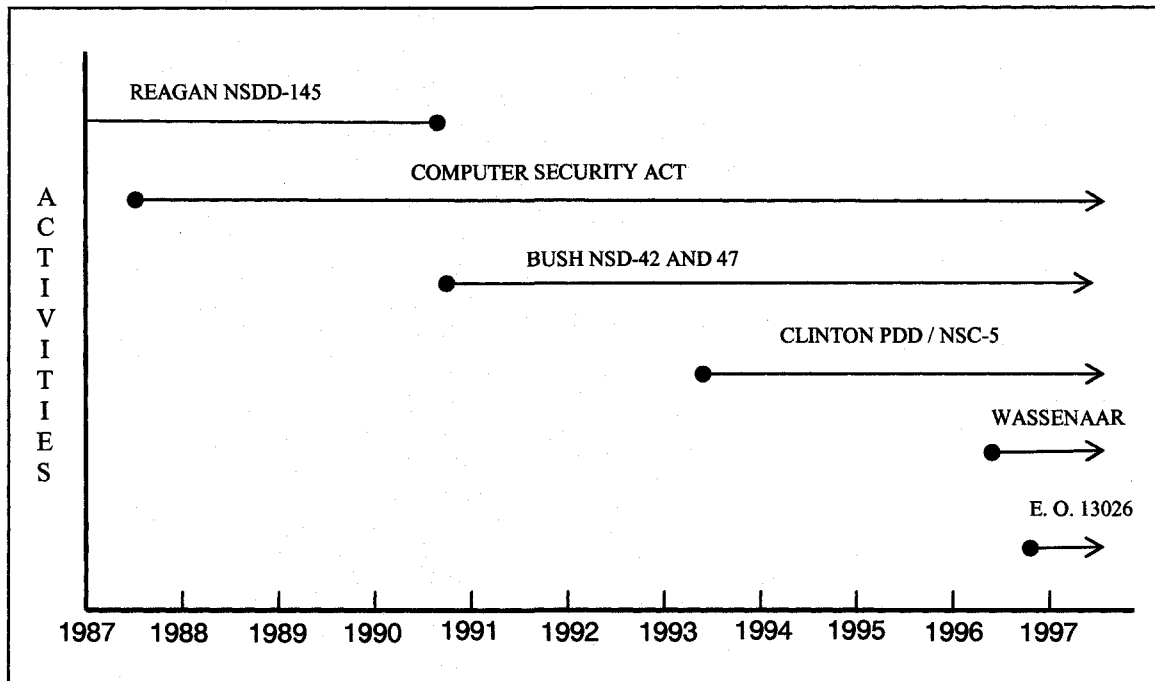


Figure 4-5 Timeline of executive branch activities on information and encryption control

At the end of the Cold War, President George H. W. Bush maintained information control for national security purposes by separating the problem into protecting classified national security information and ensuring information access for counterintelligence efforts. President Bush issued NSD-42 in July 1990 because he believed that “a comprehensive and coordinated approach must be taken to protect the government’s national security telecommunications and information systems (national security systems)

against current and projected threats.”³⁵⁷ In addition, NSD-42 continued the policies of NSDD-145 for national security systems, but did not control sensitive but unclassified information in the federal government because these systems were considered “within the purview of the Computer Security Act of 1987.”³⁵⁸ However, President Bush issued NSD-47 that strengthened counterintelligence and security countermeasures activities in the national security and private sectors. His rationale for this broad government interest in information was as follows:

By the end of the 1990s, we will probably see a markedly different threat environment. This dynamic situation requires thoughtful and systematic CI and SCM planning, resource commitment, and imaginative implementation. We must enhance our ability to anticipate the scope and pace of changing intelligence threats and to respond with successful operational initiatives. CI and SCM matters should continue to be handled in the 1990s as strategic issues requiring priority attention.³⁵⁹

The text shows that president Bush believed that “CI and SCM matters” were “strategic issues requiring priority attention.” Figure 4-5 shows the timings of NSD 42 and NSD-47 and the continued government control of information affecting national security.

In 1993, President Clinton issued PDD/NSC-5, which added a specific encryption control vector to the information control problem. PDD/NSC-5 identified encryption as a threat to “lawful government electronic surveillance,” because the government was conducting “foreign intelligence activities critical to [U.S.] national interests” outside and

³⁵⁷ George H. W. Bush, National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” 5 July 1990: 1.

³⁵⁸ *Ibid.*, 9.

³⁵⁹ George H. W. Bush, National Security Directive 47, “Counter Intelligence and Security Countermeasures,” 5 October 1990: 1.

inside the United States.³⁶⁰ President Clinton did not rescind President Bush's NSD-47 on counterintelligence, because encryption control was the next logical step in solving the information access problem that threatened national security and public safety. Figure 4-5 shows that NSD-47 and PDD/NSC-5 were in effect for the rest of the Competitive Period.

President Clinton negotiated the Wassenaar Arrangement to limit the export of dual-use technologies in early 1996, but required an executive order to fulfill the promised United States control of exported encryption products. Congress was not in a position to ratify or legitimize the Wassenaar Arrangement because of its successive failures to pass export legislation during the Competitive Period. President Clinton, acting under a declared "national emergency," notified Congress on 4 June 1996 about the pending the Wassenaar Arrangement.³⁶¹ Despite this notification, Congress still failed to pass export legislation.

President Clinton signed E.O. 13026 on 15 November 1996, which transferred encryption export controls from the Department of State to an agency in the Department of Commerce. E.O. 13026 specifically addressed the national security threat posed by encryption technology exported from the United States:

I have determined that the export of encryption products described in this section could harm national security and foreign policy interests even where

³⁶⁰ William J. Clinton, Presidential Decision Directive / NSC 5, "Public Encryption Management," 15 April 1993: 1.

³⁶¹ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 80: S5758.

comparable products are or appear to be available from sources outside the United States, and that facts and questions concerning the foreign availability of such encryption products cannot be made subject to public disclosure or judicial review without revealing or implicating classified information that could harm United States national security and foreign policy interests....

Appropriate controls on the export and foreign dissemination of encryption products described in this section may include, but are not limited to, measures that promote the use of strong encryption products and the development of a key recovery management infrastructure ...³⁶²

The text shows that President Clinton perceived a crisis in that exported encryption products “could harm national security and foreign policy interests even where comparable products are or appear to be available.” This perception would have been rational only if foreign “comparable products” were inferior to United States encryption products. No evidence was offered to support this perception. In addition, foreign encryption products could have used United States encryption algorithms that were already in the public domain. The text also indicates that encryption products developed under “key recovery management infrastructure” would be eligible for export. Thus, E.O. 13026 limited encryption exports, mainly from the private sector, and encouraged encryption exports based on the government’s Escrowed Encryption Standard.

Figure 4-5 shows the timing of the Wassenaar notification to the Senate and the subsequent issuance of E.O. 13026. This timing suggests that President Clinton used his emergency powers under the “International Emergency Economic Powers Act (50 U.S.C.

³⁶² President, Executive Order 13026, “Administration of Export Controls on Encryption Products,” 15 November 1996, *Federal Register* 61, no. 224 (19 November 1996): 58767.

1703(c)) and section 401(c) of the National Emergencies Act (50 U.S.C. 1641(c))” to implement his encryption control solution.³⁶³

During the Competitive Period, a continual sense of urgency surrounded the information control problem and warranted actions by three administrations. This sense of urgency matched Allison’s GPM general proposition of “Chiefs and Indians” where “policy issues with which the president can deal are limited primarily by his crowded schedule.”³⁶⁴ Information control policy issues involving international relations and having national security implications added to the busy schedule. President Reagan found that NSDD-145 was required to protect information in the government and private sectors from threats such as Soviet espionage. President Bush issued NSD-47 that asked for government access to information in order to perform counterintelligence activities. President Clinton went further by issuing PDD/NSC-5 that directed both the government and private sectors to use escrowed-key encryption. President Clinton’s domestic encryption policy scheme avoided the congressional paralysis on export legislation and allowed him to comply with the Wassenaar Arrangement on the export of dual-use technologies. This mandated encryption scheme guaranteed government access to information and made military strength encryption available to all users. However, this scheme alienated actors in the Encryption Technology Group and in Congress by imposing information control on the private sector through methods contrary to the *Computer Security Act of 1987*. I therefore assigned a Decision Timing valance of “2” to

³⁶³ *Congressional Record*, 104th Congress, 2d sess., 1996, 142, pt. 80: S5758.

³⁶⁴ Allison and Zelikow, *Essence of Decision*, 307-8.

the Executive Group for the urgent use of presidential directives and executive orders in setting information and encryption control policies without requiring congressional action.

Government Agencies Group

In the Competitive Period, the primary actors in the Government Agencies Group were the National Institute of Standards and Technology (NIST) and the Defense Department's National Security Agency (NSA). These actors worked together to first develop a Digital Signature Standard (DSS) that restricted public key encryption technology and then developed a complete encryption system to become the Escrowed Encryption Standard (EES). EES was unique in that NIST and NSA based this standard on prior national security encryption systems that provided for strong information security and government access to encryption keys. EES was different from legacy national security systems by separating the encryption key into two parts, which were stored in different key escrow facilities. Both key parts were needed to reconstruct the EES key. Since EES was a complete government encryption system using both public and secret key encryption algorithms, the Government Agencies Group did not take timely actions to replace the 1977 vintage federal Data Encryption Standard or to complete the development of a fully capable public key encryption standard. Congressional testimonies, Federal Information Processing Publications, memorandums of agreement, official notices published in the *Federal Register*, presidential directives, and United States patents provided the data for analyzing the actions of the Government

Agencies Group. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

Evidence shows that actors from the Government Agencies Group worked on two aspects of the information security problem while under the technical leadership of the National Security Agency and under the management of the National Institute of Standards and Technology. These actors were cognizant of the national security and public safety directives from three different administrations. A historical deference toward national security and law enforcement requirements existed in these technology-leading government agencies, which in turn fostered the development of restrictive encryption standards. The results were two encryption controlling standards, the Digital Signature Standard and the Escrowed Encryption Standard. The government's emergent role in the 1991 development of DSS is often obscured by the voluminous research on the dominant role of the government in the development of EES. The emergence of encryption control occurred during the development of DSS and became readily apparent with the development of EES. In contrast to the development of the Data Encryption Standard eighteen years prior, the development of DSS appeared suddenly with a government announcement of a proposed standard.

NIST established government leadership over the Digital Signature Standard by skipping the proposal solicitation step that had previously allowed industry and academia to submit their designs. NIST, in an August 1991 *Federal Register* notice, published

their rationale for eliminating this step in the development of a new Federal Information Processing Standard (FIPS):

This proposed FIPS is the result of evaluating a number of alternative digital signature techniques. In making the selection, the NIST has followed the mandate contained in section 2 of the Computer Security Act of 1987 that NIST develop standards and guidelines to “* * * assure cost effective security and privacy of sensitive information in Federal systems.” In meeting this statutory responsibility, NIST has placed primary emphasis on selecting the technology that best assures the appropriate security of Federal information and, among other technologies offering comparable protection, on selecting the option with the most desirable operating and use characteristics.

Among the factors that were considered during this process were the level of security provided, the ease of implementation in both hardware and software, the ease of export from the U.S., the applicability of patents, impact on national security and law enforcement and the level of efficiency in both the signing and verification functions.³⁶⁵

The text shows that the government decided to design DSS alone and without external visibility into the design process. A list of the “alternative digital signature techniques” was not published in the *Federal Register*, thereby, supporting speculation that the government eliminated digital signature algorithms capable of encrypting information in order to satisfy “ease of export” and “national security and law enforcement” requirements. Subsequent discussions by NIST further established the motivation behind the government’s leadership role.

In a May 1994 *Federal Register* notice, NIST denied unusual activities or influences in the development and approval processes for the Digital Signature Standard:

³⁶⁵ U.S. Department of Commerce, National Institute of Standards and Technology, “A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS),” *Federal Register* 56, no. 169 (30 August 1991): 42981.

NIST also received many comments criticizing the adoption of the proposed DSS. Some of the arguments in opposition included: The selection process for the Digital Signature Algorithm (DSA) was not public; time provided for analysis of the DSA was not sufficient; the DSA may infringe on other patents; the DSA does not provide for secret key distribution ...

NIST considered all of the issues raised and believes that it has addressed them. The development of this standard was carried out through NIST's usual procedures including solicitation of input from different sources.³⁶⁶

The text shows that the actors in the Government Agencies Group were cognizant of the problems created by a lack of transparency in the selection process. However, the text was not convincing when it claimed that NIST used "usual procedures," as DSS did not follow the public solicitation procedures used in the development of the Data Encryption Standard, some eighteen years earlier. Another question generated by NIST's response was on the role played by the National Security Agency in generating encryption standards.

The belief that a lead actor could control encryption policy by developing a standard was demonstrated in the development of the Escrowed Encryption Standard. The development of EES came two years after DSS development and was extreme in its secretive nature and policy vector. In a pattern similar to DSS, NIST did not publicly solicit proposals for candidate encryption algorithms that supported NIST requirements. Instead, the public start of EES development came with a government announcement of a proposed standard for a complete and unique encryption system. EES has a permanently

³⁶⁶ U.S. Department of Commerce, National Institute of Standards and Technology, "Approval of Federal Information Processing Standard Publication 186, Digital Signature Standard (DSS)," *Federal Register* 59, no. 96 (19 May 1994): 26209.

built-in information access feature that uses a government key escrow. In a July 1993 *Federal Register*, NIST announced its proposed Federal Information Processing Standard (FIPS):

This proposed FIPS implements the initiative announced by the White House Office of the Press Secretary on April 16, 1993. The President of the U.S. approved a Public Encryption Management directive, which among other actions, called for standards to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits in Federal communication systems that process sensitive, but unclassified information.³⁶⁷

The text indicates that NIST was following directions from the Executive Office of the President to take the government lead in establishing a viable encryption standard that could balance information access and security requirements. Unlike DSS development, EES had to be explicit in its approach to encryption control, as the use of the term "key-escrow" clearly indicated the government's motivation for developing this new encryption standard. The lapse of three months between executive direction and the announcement of the proposed EES did not accurately reflect the time needed by NSA to develop the technology behind the proposed standard.

EES development reflected NSA's approach to information security and did not necessarily indicate a mischievous role that infringed upon the privacy rights of United States citizens. The 1984 National Security Decision Directive 145, discussed earlier, gave NSA the leadership role for all federal government encryption standards. Although

³⁶⁷ U.S. Department of Commerce, National Institute of Standards and Technology, "A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES)," *Federal Register* 58, no. 145 (30 July 1993): 40791-2.

this direction was partially countermanded by the *Computer Security Act of 1987*, NSA had put significant effort into replacing DES “Type III” encryption used to protect unclassified information with an EES “Type II” encryption system. In doing so, NSA may have adapted information security (INFOSEC) and communications security (COMSEC) principles learned from its signals intelligence (SIGINT) experiences and from its use of “Type I” encryption systems required to protect classified national security information gained through SIGINT.

A key NSA document of this period, which was previously classified, set the policy for collection and COMSEC monitoring by the United States SIGINT System (USSS). The 1993 United States Signals Intelligence Directive 18 (USSID 18) described the bounds of government information collecting and monitoring:

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS.* The USSS will not intentionally COLLECT communications from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID....

4.9 (U) COMSEC Monitoring and Security testing of Automated Information Systems. Monitoring for communication security purposes must be conducted with the consent of the person being monitored and in accordance with the procedures established in National Telecommunications and Information System Security Directive 600.³⁶⁸

³⁶⁸ National Security Agency Central Security Service, United States Signals Intelligence Directive 18, 27 July 1993, 2 and 9. Document was declassified and released under a FOIA request and contains excisions.

The text shows that NSA collects intelligence and monitors communications in a strictly regulated fashion. To perform these functions, NSA favored Type I encryption systems with government control of the encryption keys. This control facilitated collecting against persons suspected of insider espionage and for COMSEC monitoring of intelligence information leakages. Thus, the political decision to rely on NSA's technology leadership heavily influenced the production of the EES with its guaranteed government access to encrypted information.

The view of the government as the lead actor by the Government Agencies Group matched Allison's GPM organizing concept of "Players in Positions." The players were NIST and NSA and were the "major channels for producing action on national security issues."³⁶⁹ NSA following political direction from the executive branch used its technical leadership to control non-defense encryption technology in a manner similar to the way it controlled national security encryption systems. I therefore assigned a Lead Actor valance of "2" to the Government Agencies Group for being the government lead in ensuring access to information for national security purposes and for protecting digital information from unauthorized access.

B. Problem Perception Valance

Actors in the Government Agencies Group perceived a complex encryption problem with international, national security, law enforcement, privacy, and market

³⁶⁹ Allison and Zelikow, *Essence of Decision*, 296.

aspects. The development of the Digital Signature Standard addressed the international aspects of encryption control in a unique manner. Like the 1977 vintage Data Encryption Standard, DSS was a complete specification for an encryption subsystem that provided international actors with all the information required to build DSS hardware and software devices. While DES was on the United States Munitions List for export control, the Digital Signature Standard, a subset of public key encryption technology, was not:

Export Control: Implementations of this standard are subject to Federal Government export controls as specified in Title 15, Code of Federal Regulations, Parts 768 through 799. Exporters are urged to contact the Department of Commerce, Bureau of Export Administration for more information.³⁷⁰

The text shows that the cited sections of the Code of Federal Regulations did not include Part 732 that deals with encryption exports. The cited sections pertained to foreign availability and administrative determination, both of which made DSS export control largely ceremonial as the publication of DSS gave away this technology to all international actors. Thus, the purposeful inability of the DSS algorithm to encrypt information satisfied national security and law enforcement requirements for international and domestic encryption control and relieved DSS from being considered as a munition.

The decision by actors in the Government Agencies Group to eliminate the encryption capabilities of DSS solved a major encryption control problem. However,

³⁷⁰ U.S. Department of Commerce, National Institute of Standards and Technology, "Approval of Federal Information Processing Standard Publication 186, Digital Signature Standard (DSS)," *Federal Register* 59, no. 96 (19 May 1994): 26210.

fixing this perceived problem reduced the market value of DSS against competing commercial digital signature standards. To improve the competitiveness of DSS against encryption capable digital signature algorithms, NIST sought to patent the technology behind DSS in order to gain a technology monopoly:

This proposed standard adopts a public-key signature system that uses a pair of transformations to generate and verify a digital value called a signature. The government has applied to the U.S. Patent Office for a patent on this technique. The government will also seek foreign patents as appropriate. NIST intends to make this DSS technique available world-wide on a royalty free basis in the public interest.³⁷¹

The text shows that NIST planned to have its DSS-based technology dominate over alternative digital signature designs in both the international and domestic markets by under-cutting the presumed licensing fees charged by competitive alternatives. NIST took action by filing for a United States Patent in July 1991, and NIST received a patent in July 1993.³⁷² The patented technology also helped DSS create a niche not previously open to NIST encryption standards.

The use of unclassified Federal Information Processing Standards on encryption to protect classified information showed a convergence of information security problems from the unclassified public domain and from the classified national security domain:

³⁷¹ U.S. Department of Commerce, National Institute of Standards and Technology, "A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," *Federal Register* 56, no. 169 (30 August 1991): 42980.

³⁷² David W. Kravitz, "Digital signature algorithm," U.S. Patent # 5,231,668, 27 July 1993. Filed on 26 July 1991.

NIST has received agreement from the Department of Defense authorities that this digital signature technique may be used to sign unclassified data processed by "Warner Amendment" systems (10 U.S.C. 2315 and 44 U.S.C. 3502(2)) as well as classified data in selected applications.³⁷³

The text indicates that NSA's function of protecting classified national security information was technologically and organizationally adaptable to protecting information in general. NSA had to be a part of DSS development to ensure that DSS was secure against cryptographic attacks. This complex task could not be done by NIST alone, and thus, presented an opportunity for NSA design and policy inputs. How much of the DSS policy originated from NSA is not in the public record. In contrast to DSS development, the development of the Escrowed Encryption Standard had a clear NSA origin.

NSA spent years developing encryption systems and in doing so, developed unique perspectives on the information security and encryption control problems. NSA designed EES to solve both these problems in a manner consistent with prior government approaches used to secure classified data. Classified information requires so called "Type I" encryption for protection. The first element of Type I encryption is a secret key encryption algorithm of adequate strength. The second element of Type I encryption is to secure the physical cryptographic device in a tamper resistant container, which is often known by its military moniker as a "KG" unit. The third element of Type I encryption is a centrally generated and controlled encryption key, which is often loaded into the KG unit by a punched paper tape reader, crypto "ignition key," or a digital crypto key loader.

³⁷³ U.S. Department of Commerce, National Institute of Standards and Technology, "A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," *Federal Register* 56, no. 169 (30 August 1991): 42981.

The last two elements of Type I encryption reduced the chances of cryptographic failure by minimizing human tinkering with the KG device and by avoiding human limitations in generating and archiving encryption keys in the field. Thus, Type I devices were implemented as black boxes that relied on a flow of secret encryption keys from NSA's central repository. This repository also provided copies of encryption keys in case the original keys were lost or if the government needed access to the encrypted information for communications security and counter-espionage purposes. It is from this problem perception that NSA developed EES to assist the non-defense sector in protecting sensitive, but unclassified data.

The proposed EES shown in the 1993 *Federal Register* confirms that actors in the Government Agencies Group perceived that the information security problem required an NSA solution:

This proposed standard adopts encryption technology developed by the Federal government to provide strong protection for unclassified information and to enable the keys used in the encryption and decryption processes to be escrowed. This latter feature will assist law enforcement and other government agencies, under the proper legal authority, in the collection and decryption of electronically transmitted information.³⁷⁴

The text uses the phrase "adopts encryption technology developed by the Federal government" to signify the use of NSA developed "strong protection" encryption technology previously employed for Type I national security data. The use of a national

³⁷⁴ U.S. Department of Commerce, National Institute of Standards and Technology, "A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES)," *Federal Register* 58, no. 145 (30 July 1993): 40791.

security solution for protecting “unclassified information” brought along NSA’s key escrow solution that would allow “law enforcement and other government agencies” access to encrypted information. This planned access was consistent with NSA’s collection and COMSEC monitoring requirements of national security data and allowed law enforcement officials to circumvent otherwise unbreakable national security encryption. In these respects, EES use allowed sensitive data to be protected at a level previously reserved for classified information and continued the blurring of national security encryption systems and private sector encryption systems.

Instead of using private sector encryption developers, NIST selected NSA to implement EES because of the complexity of the encryption control problem. In his 1994 testimony to the House Subcommittee on Technology, Environment and Aviation, NIST Deputy Director Raymond G. Kammer discussed the domestic and national security motivations behind EES:

Counterbalanced against its benefits, encryption also can present many substantial drawbacks – to both the government and other users. First and foremost, encryption can frustrate legally authorized criminal investigations by the federal, state and local law enforcement agencies. As their representatives can better explain, lawful electronic surveillance has proven to be of the utmost benefit in both investigating and prosecuting serious criminal activity, including violent crime. Cryptographic technologies can also seriously harm our national security and intelligence capabilities. As I shall discuss, the Administration recognizes that the consequences of wide-spread, high quality encryption upon law enforcement and national security are considerable....

The National Security Agency, in consultation with NIST and the federal law enforcement community, undertook to apply voluntary key escrow encryption technology to voice-grade communications. The product of this effort was

announced in the April 16, 1993 White House release concerning the key escrow chip.³⁷⁵

The text shows that the Government Agencies Group perceived that encryption use presented a problem to domestic “federal, state and local law enforcement agencies” and that encryption use could “seriously harm [U.S.] national security.” These problems prompted NSA to “apply voluntary key escrow encryption technology to voice grade communications” that in turn resulted in a White House decision to push for the widespread use of escrowed-key encryption. The careful use of the term “voluntary” and the expansion in scope from protecting voice communications to protecting information security with the “key escrow chip” indicated the political incongruities required to sell a mandatory use encryption system. The system would not work if domestic users could elect to keep their secret encryption keys hidden. In addition, the national security problem could only be solved if foreign countries would submit control of their encryption keys to United States government.

Actors in the Government Agencies Group perceived the importance of exporting escrowed-key encryption systems to satisfy national security requirements and to enhance the global market advantages of cooperative United States encryption vendors. NIST Deputy Director Kammer spoke of the importance of exporting EES technology in his testimony to Congress:

³⁷⁵ House Committee on Science, Space, and Technology, Subcommittee on Technology, Environment and Aviation, *Communications and Computer Surveillance, Privacy and Security*, 103rd Congress, 2nd sess., 3 May 1994, 42 and 44.

In the recent months, the Administration has dramatically relaxed export controls on computer and telecommunication equipment. However, we have retained export controls of encryption technology, in both hardware and software. These controls strongly promote our national security. These export controls include mass market software implementing the Data Encryption Standard. The Administration determined, however, that there are a number of reforms the government can implement to reduce the burden of these controls on U.S. industry.

These reforms are part of the Administration's goal to eliminate unnecessary controls and ensure efficient implementation of those controls that must remain ... Lastly, after a one-time initial technical review, key escrow encryption products may now be exported to most end users.³⁷⁶

The text suggests the NIST's 1977 Data Encryption Standard technology faced export restrictions and claims that "key escrow encryption products may now be exported to most end-users." NIST perceived EES as a solution that could fix encryption control and export problems that had been previously unsolvable for fifteen years.

The view of a complex problem by actors in the Government Agencies Group matched Allison's GPM organizing concept of "Goals and Interests" where the perception of the main problem depends on the politically guided function of the government organization with the solution.³⁷⁷ NSA offered its escrowed-key encryption solution to solve the complex international, domestic, and economic problems posed by strong encryption solutions being made available by the United States government. By developing EES under the auspices of NIST, NSA solved an encryption control problem left open by the 1977 Data Encryption Standard. I therefore assigned a Problem

³⁷⁶ *Ibid.*, 47.

³⁷⁷ Allison and Zelikow, *Essence of Decision*, 298.

Perception valance of “2” to the Government Agencies Group for perceiving a complex problem.

C. Favored Alternative Valance

Actors in the Government Agencies Group realized that the Digital Signature Standard and Escrowed Encryption Standard required the force of law or regulations to ensure compliance and to minimize competition from commercial encryption systems. The evidence shows that NIST and NSA developed DSS to be a regulatory standard designed to achieve the government’s encryption control agenda. This agenda eventually failed because DSS was not a market-based standard and was a sub-optimum regulatory standard that covered too many conflicting requirements. The following EES failed because it lacked the required legal and regulatory backing to be successful.

An examination of the *Federal Register* notice for the proposed DSS revealed the mechanism by which NIST planned to enforce this standard:

Applicability: This standard is applicable to all Federal departments and agencies for the protection of unclassified information that is not subject to section 2315 of Title 10, United States Code, or section 3502(2) of Title 44, United States Code. This standard shall be used in designing and implementing public-key based signature systems which Federal departments and agencies operate or which are operated under contract. Adoption and use of this standard is available to private and commercial organizations.³⁷⁸

³⁷⁸ U.S. Department of Commerce, National Institute of Standards and Technology, "Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS)," *Federal Register* 59, no. 96 (19 May 1994): 26210-11.

The text shows the use of the stringent “shall be used” phrase in the DSS applicability section. Other encryption standards, such as the 1977 DES and the 1999 DES update, employed the more common “will be used” phrase in their applicability sections.³⁷⁹ In the terminology of government regulations, “shall” means required and “will” means recommended. In addition to effectively requiring the use of DSS, the text uses citations from the United States Code defining unclassified data in order to bolster the forcefulness of the applicability section. These citations are not necessary and are not found in other federal encryption standards such as the 1977 DES and the 1999 DES update.³⁸⁰ The text expands the requirement to use DSS by extending its applicability to vendors working under government service contracts. The text then recommends the “adoption and use” of DSS by the private sector and shows the government's desired end state as the pervasive use of DSS technology. NIST's motivation behind the development of a regulatory DSS was to dominate the government and private sectors by gaining a first mover advantage in public key encryption.

The Digital Signature Standard was a restrictive public key encryption standard and used a unique approach to regulate digital signature encryption capabilities. In contrast to the DSS, commercial public key encryption subsystems performing digital signature functions could also perform encryption functions. An examination of the entire 1991

³⁷⁹ U.S. Department of Commerce, National Bureau of Standards, *The Data Encryption Standard (DES), Federal Information Processing Standard Publication 46* (Washington, D.C., July 1977), 1.

U.S. Department of Commerce, National Institute of Standards and Technology, *Data Encryption Standard (DES), Federal Information Processing Standards Publication, FIPS PUB 46-3* (Washington, D.C., 1999), 2

³⁸⁰ *Ibid.*

Federal Register notice revealed that NIST purposefully avoided the use of the term “encryption” even though their proposed algorithm was technically part of the public key encryption subsystem. This specific avoidance of language indicated that the Government Agencies Group required a DSS with the ability to perform authenticity, integrity, and non-repudiation functions and without the ability to perform encryption for confidentiality purposes. Other competitive digital signature algorithms, such as RSA from RSA Security, could perform all four functions. User comments on the inability of DSS to encrypt secret keys as part of a complete encryption systems prompted a terse response from NIST on this limitation of its patented digital signature algorithm (DSA). “The DSA does not provide for secret key distributions since it is not intended for that purpose.”³⁸¹ A technical review of the 1993 government patent on DSA revealed an algorithm specifically designed to sign digital documents efficiently and to be ineffective in encrypting and decrypting messages.³⁸² The advantages of a government sanctioned, royalty free, and efficient DSS were forms of control over the encryption capable public key encryption subsystems offered by information technology vendors.

Two actions in 1997 confirmed that actors in the Government Agencies Group used DSS to control public key encryption. After being pressured for three years to change DSS to allow other public key encryption subsystems, actors in the Government

³⁸¹ U.S. Department of Commerce, National Institute of Standards and Technology, “Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS),” *Federal Register* 59, no. 96 (19 May 1994): 26209.

³⁸² David W. Kravitz, “Digital signature algorithm,” U.S. Patent # 5,231,668, 27 July 1993.

Agencies Group revealed their rationale for pursuing a standard that restricted encryption capabilities in a 1997 *Federal Register* notice revising DSS:

The Administration policy is that cryptographic keys used by Federal agencies for encryption (i.e., to protect the confidentiality of information) shall be recoverable through an agency or third-party process and that keys used for digital signature (i.e., for integrity and authentication of information) shall not be recoverable. Agencies must be able to ensure that signature keys cannot be used for encryption. Any algorithms proposed for digital signature must be able to be implemented such that they do not support encryption unless keys used for encryption are distinct from those used for signature and are recoverable.³⁸³

The text shows that “cryptographic keys” were used in public key encryption and digital signatures, despite the avoidance of the “encryption” word in the DSS documentation by actors in the Government Agencies Group. More importantly, the text suggests that the encryption capabilities of the DSS were restricted because these actors believed that government digital signature algorithms “must be able to be implemented such that they do not support encryption.” This restriction was done in accordance with policy from the executive branch.

The second action was the attempted generation of a public key encryption standard that was never completed. By insisting on a separation of digital signature and public key encryption standards, NIST could continue to separate its regulatory DSS alternative from commercial public key encryption solutions that were encryption capable. In this manner, NIST could maintain the information control power of an updated DSS.

³⁸³ U.S. Department of Commerce, National Institute of Standards and Technology, "Announcing Plans to Revise Federal Information Processing Standard 186, Digital Signature Standard," *Federal Register* 62, no. 92 (13 May 1997): 26293.

Although this separation was artificial, as the same mathematical properties enable both DSS and public key encryption, NIST published a separate *Federal Register* notice on developing a standard for a public key encryption subsystem:

NIST is planning to develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange. This notice solicits comments regarding techniques for consideration specifically including RSA, Diffie-Hellman, and Elliptic Curve techniques. This standard will be used for designing and implementing public-key based key agreement and exchange systems which Federal departments and agencies operate or which are operated for them under contract....

The Administration policy is that cryptographic keys used by Federal agencies for encryption (i.e., to protect the confidentiality of information) shall be recoverable through an agency or third-party process and that keys used for digital signature (i.e., for integrity and authentication of information) shall not be recoverable. Agencies must be able to ensure that signature keys cannot be used for encryption. Any algorithms proposed for digital signature must be able to be implemented such that they do not support encryption unless keys used for encryption are distinct from those used for signature and are recoverable.³⁸⁴

The text uses the weaker "will be used" phrase that implies the development of a voluntary public key encryption standard. The cautionary text on encryption keys was the same text used in the DSS notice, thus further demonstrating that DSS and public key encryption were parts of the same public key encryption subsystem and were separated for regulatory purposes. The next encryption standard after DSS was the Escrowed Encryption Standard, which specified a complete encryption system.

³⁸⁴ U.S. Department of Commerce, National Institute of Standards and Technology, "Announcing Plans to Develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange," *Federal Register* 62, no. 92 (13 May 1997): 26294.

The Escrowed Encryption Standard was a novel type of standard and was developed by actors in the Government Agencies Group as a competitive alternative to solve a complex problem. The executive and legislative branches had different perspectives on encryption control, and this difference resulted in an encryption alternative without the required regulatory or legal power for enforcement of its use. Adding to this problem were the requirements for public trust in the technology behind EES and in the choice of key escrow agents. Guided by a 1989 Memorandum of Understanding that selectively interpreted the *Computer Security Act of 1987*, NIST and NSA produced a complete encryption system alternative that relied heavily upon NSA's expertise and technology:

4. Develop telecommunications security standards for protecting sensitive unclassified computer data, drawing upon the expertise and products of the National Security Agency, to the greatest extent possible, in meeting these responsibilities in a timely and cost effective manner.³⁸⁵

The use of NSA's "expertise and products" appeared reasonable to actors in the Government Agencies Group. NIST Deputy Director Kammer commented to Congress on the complexity of complying with the *Computer Security Act of 1987* to make computers more secure and with administration directions to ensure encryption control for national security and public safety purposes:

Before leaving the subject of the Computer Security Act, however, let me briefly comment on the Escrowed Encryption Standard. I strongly believe that NIST and

³⁸⁵ Raymond G. Kammer and Vice Admiral W.O. Studeman, "Memorandum of Understanding between the Director of the National Institute of Standards and Technology and the Director of the national Security Agency Concerning the Implementation of Public Law 100-235," 24 March 1989.

NSA have complied with the spirit and intent of the Act. At the same time, this issue underscores the complex issues which arise in the course of developing computer standards, particularly cryptographic-based standards for unclassified systems.³⁸⁶

The text indicates that NIST and NSA were satisfied with EES as a pragmatic and legal encryption control alternative for use in the "unclassified" or non-defense federal and private sectors. NSA had previously satisfied the encryption requirements for the national security community and had earned the trust of this community. This level of trust in an encryption alternative was assumed to exist in the private sector.

The 1993 *Federal Register* notice announcing the proposed EES differed radically from previous encryption standards in that EES did not contain any technical specifications:

Summary: A Federal Information Processing Standard (FIPS) for an Escrowed Encryption Standard (EES) is being proposed. This proposed standard specifies use of a symmetric-key encryption/decryption algorithm and a key escrowing method which are to be implemented in electronic devices and used for protecting certain unclassified government communications when such protection is required. The algorithm and key escrowing method are classified and are referenced, but not specified in this standard.³⁸⁷

The text describes the secret or "symmetric-key" aspects of EES but does not describe the key escrow method. This method, which was revealed by NSA in 1998, used a form of

³⁸⁶ House Committee on Science, Space, and Technology, Subcommittee on Technology, Environment and Aviation, *Communications and Computer Surveillance, Privacy and Security*, 103rd Congress, 2nd sess., 3 May 1994, 50.

³⁸⁷ U.S. Department of Commerce, National Institute of Standards and Technology, "A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES)," *Federal Register* 58, no. 145 (30 July 1993): 40791.

public key encryption for distributing parts of the key to the key escrow facilities.³⁸⁸

Thus, EES was a complete encryption system built into tamper-resistant modules in order to preclude reverse engineering of the system. In 1993, NIST and NSA had to protect their operational systems from exploitation by classifying the algorithms behind EES.

Users of EES could not inspect or test EES and had to trust the government.

In order to gain the trust of potential EES users, EES was advertised as a voluntary standard. The 1994 *Federal Register* notice approving EES made this point by answering concerns from the public sector about mandatory use of this new government encryption standard:

(1) Five industry organizations and 200 individuals said that guarantees are needed to assure that this standard is not a first step toward prohibition against other forms of encryption. In response, NIST notes that the standard is a specification for voluntary use by the Federal government in the acquisition of devices for escrowed encryption. There is no requirement that the public use this standard. Further, the Administration has announced that it will not propose new legislation to limit the use of encryption technology.³⁸⁹

The text indicates that EES was a voluntary standard and that no laws required its use.

Without a legal requirement to use EES, trust-building mechanisms would be required to build an adequate user base. However, the publication of the complete specification for EES was restricted because of security considerations. NSA was using similar systems

³⁸⁸ U.S. Department of Defense, National Security Agency, "Press Release: NSA Releases FORTEZZA Algorithms," 24 June 1998.

³⁸⁹ U.S. Department of Commerce, National Institute of Standards and Technology, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)," *Federal Register* 59, no. 27 (9 February 1994): 5998.

for national security purposes and operational security required that the details of encryption systems be kept secret.

Although advertised as a voluntary Federal Information Processing Standard, the absence of technical details hindered users from making a rational choice between EES and commercial encryption standards. NIST's explanation for this lack of technical details was not satisfactory and was circular:

Four Federal government organizations and two individuals said the standard is not an interoperability standard, that it does not specify parameter lengths and formats and placements in communications, and that the standard provides insufficient technical detail for implementation. NIST added information to the standard to explain that is not an interoperability standard. It does not provide sufficient information to design and implement a security device or equipment.³⁹⁰

In the text, NIST explains that EES was "not an interoperability standard," but this explanation contradicts their definition of a standard. In retrospect, NIST's concerns about protecting the Escrowed Encryption Standard's SKIPJACK algorithm and Diffie-Hellman public key exchange algorithm were not warranted. Equivalent technology, such as Pretty Good Privacy, was already commercially or freely available. EES as a voluntary encryption control alternative did not provide technical details to generate user trust and therefore was not competitive with other encryption systems.

Although actors in the Government Agencies Group attempted to make the Digital Signature Standard a regulatory standard through legalistic prose and by using a crippled

³⁹⁰ *Ibid.*, 6001.

encryption algorithm, DSS was still voluntary and users could choose a more capable commercial standard. Next, these actors made the voluntary Escrowed Encryption Standard a secretive standard to protect it from misuse and exploitation. By doing so, these actors inadvertently sacrificed the trust relationships required by encryption users in the non-defense federal and private sectors. These actions matched Allison's OBM general proposition that "Existing Organized Capabilities Influence Government Choice."³⁹¹ In the case of out-competing the private sector, NIST and NSA required legal and regulatory standards. Without the combined support from the executive and legislative branches, NIST and NSA developed and tried to implement voluntary standards in accordance with the precedent set by the successful Data Encryption Standard. I therefore assigned a Favored Alternative valance of "1" to the Government Agencies Group for developing DSS and EES as government standards that favored national security and public safety requirements over privacy and economic concerns.

D. Decision Timing Valance

Actors in the Government Agencies Group believed that there were urgent requirements for encryption controlling standards. One standard would limit the public key encryption subsystem to perform only digital signatures. The second standard would specify the use of a complete encryption system with a mandatory key escrow. Competition from the private sector was the driving force behind this sense of urgency. In 1991, Zimmermann released PGP as a functional product, while NIST was just

³⁹¹ Allison and Zelikow, *Essence of Decision*, 176-177.

announcing its proposed Digital Signature Standard. Actors in the Government Agencies Group recovered from this lag with the Escrowed Encryption Standard, which NIST proposed in 1993 and approved in 1994. The ability to overcome numerous DSS and EES development obstacles serves as evidence for the urgent requirement to beat the competition.

The sense of urgency for encryption control originated from the executive branch and drove the actions of the Government Agencies Group. NIST Deputy Director Kammer spoke of this urgency in his testimony before Congress:

Encryption use world-wide affects our national security. While this matter cannot be discussed in detail publicly without harm to this nation's intelligence sources and methods, I can point to the Vice President's public statement that encryption has "huge strategic value." The Vice President's description of the critical importance of encryption is important to bear in mind as we discuss these issues today.³⁹²

The phrase "critical importance of encryption" meant that actors in the Government Agencies Group were taking immediate actions to control encryption through technology standards. NSA's representative testifying before Congress, Dr. Clinton C. Brooks, commented on the opportunity to be the first country to have a standard for an encryption system acceptable to disparate policy actors:

The U.S., with its key escrow concept, is presently the only country proposing a technique that provides its citizens very good privacy protection while maintaining the current ability of law enforcement agencies to conduct

³⁹² House Committee on Science, Space, and Technology, Subcommittee on Technology, Environment and Aviation, *Communications and Computer Surveillance, Privacy and Security*, 103rd Congress, 2nd sess., 3 May 1994, 47.

lawful electronic surveillance. Other countries are using licensing or other means to restrict the use of encryption. We have gone to great lengths to provide for both individual privacy and law enforcement interests, and I think we have developed the best technical approach. When you think that most people currently use no encryption, the key escrow encryption concept presents a system that actually enhances privacy protections. Widespread use of CLIPPER will make it easy for people to take advantages of the benefits offered by high quality encryption.³⁹³

The text uses the phrase “very good privacy,” which is similar to the name of Zimmermann’s Pretty Good Privacy encryption system, to indicate that the desired end state was the “[w]idespread use of CLIPPER.” CLIPPER was the NSA name for a hardware version of one of its escrowed-key encryption schemes. EES is also considered to be one of NSA’s escrowed-key encryption schemes. The text indicates that NSA’s most urgent concern was not with EES use in the federal government, but with being the first to supply an encryption control solution that would satisfy “both individual privacy and law enforcement interests.”

The rapidity of both the DSS and EES development processes was indicative of the urgency displayed by actors in the Government Agencies Group. In contrast to the Data Encryption Standard that took over four years to develop, DSS took just under three years to develop, as measured by its August 1991 *Federal Register* announcement and its May 1994 standard approval dates. EES was much faster, as measured by its July 1993 *Federal Register* announcement and its February 1994 approval dates. To make these dates, actors in the Government Agencies Group had to remove obstacles hindering

³⁹³ *Ibid.*, 33.

development and had to take technical risks. DSS and the EES were subjects of patent infringement claims. Inventor Claus Schnorr obtained a patent for a digital signature algorithm in 1991, well before NIST's patent award in 1993.³⁹⁴ Public Key Partners (PKP), a California-based patent holding company, obtained several public key encryption patents including Schnorr's patent and challenged NIST. This challenge forced NIST to grant PKP exclusive licensing rights to the government's digital signature algorithm when used for commercial purposes.³⁹⁵ This extreme compromise was a retreat from NIST's original position of making the "DSS technique available world-wide on a royalty free basis in the public interest" and reflected the urgency in which NIST acted.³⁹⁶ EES also had patent infringement problems.

By 1994, NIST and NSA decided that the Escrowed Encryption Standard should use two key escrow agents as a privacy protection measure. In doing so, they may have infringed upon Dr. Silvio Micali's secret sharing patents that he filed for in 1992 and 1993, and received both in 1994.³⁹⁷ Dr. Micali's idea of separating a secret into pieces such that any one piece cannot reconstruct the secret was similar to the final key-splitting scheme used by NIST and NSA. Despite the closed development used by NIST, Dr.

³⁹⁴ Claus P. Schnorr, "Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system," U.S. Patent # 4,995,082, 19 February 1991.

³⁹⁵ U.S. Department of Commerce, National Institute of Standards and Technology, "Notice of Proposal for Grant of Exclusive Patent License," *Federal Register* 58, no. 108 (8 June 1993): 32105-6.

³⁹⁶ U.S. Department of Commerce, National Institute of Standards and Technology, "A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," *Federal Register* 56, no. 169 (30 August 1991): 42980.

³⁹⁷ Silvio Micali, "Fair cryptosystems and methods of use," U.S. Patent # 5,276,737, 4 January 1994. Filed in April 1992.

Silvio Micali, "Fair cryptosystems and methods of use," U.S. Patent # 5,315,658, 24 May 1994.

Micali knew enough of the design to challenge the government. The EES design used a Law Enforcement Access Field (LEAF) to perform parts of the secret sharing and key escrowing functions, and Dr. Micali believed that the similarities with his secret sharing patent warranted a claim against government for compensation. Five months after EES approval, NIST issued a press release on an agreement with Dr. Micali:

This license agreement eliminates concerns Micali raised about possible infringements of his patents in key escrow encryption. It also removes a perceived barrier to the Administration's voluntary key escrow encryption program for telecommunications security and other new encryption approaches potentially covered by Micali patents....

NIST plans to purchase the patent rights from Micali in formal procurement actions now under way.³⁹⁸

The text shows that by negotiating with Micali, NIST eliminated a "perceived barrier" to a "voluntary key escrow encryption program." What made this press release unusual was its publication before "procurement actions" were completed. The government thus had to negotiate from a position of urgent need and Micali from a position of a sole supplier. The final settlement amount was never formally published, perhaps as part of the condition for quick settlement.

Other manifestations on the urgent need for encryption standards were rushed developments and subsequent technical flaws. While not fatal, these flaws cast doubt upon the government's closed development process and technical competence. The first

³⁹⁸ U.S. Department of Commerce, National Institute of Standards and Technology, "NIST 94-28: Patent Agreement Removes Perceived Barrier to Telecommunications Security System," 11 July 1994.

flaw was with the DSS and its supposed inability to encrypt information. This inability allowed DSS to escape export restrictions faced by commercial public key encryption systems. However, experts in cryptography found that encryption was possible by adjusting the parameters used in DSS software and signing a message twice.³⁹⁹ The result was a slow, but strong, public key encryption subsystem that was contrary to administration policy. Cryptographers also uncovered a flaw in EES that allowed users to send a bogus LEAF value to fool the key escrow system. Thus, a pair of “rogue” users could communicate using NSA’s strong SKIPJACK secret key encryption, without the government having access to the session key.⁴⁰⁰ Both these technical flaws were accepted by the actors in the Government Agencies Group as part of expedited development processes required to satisfy policy directives. Other actor groups would attack this decision timing as being irrational because the government’s trust relationship based on technical excellence was sacrificed for expediency.

The sense of urgency by actors in the Government Agencies Group to produce encryption-controlling standards matched Allison’s GPM general proposition of “Problems and Solutions” where actors are more concerned about “the decision that must be made today or tomorrow” than about “the total strategic problem.”⁴⁰¹ NIST and NSA, as action channels for a political agenda, quickly produced the Digital Signature Standard and the Escrowed Encryption Standard in attempts to gain first mover advantages over

³⁹⁹ Schneier, *Applied Cryptography*, 490-91.

⁴⁰⁰ Matt Blaze, “Protocol failure in the Escrowed Encryption Standard,” in *Proceedings of the 2nd ACM Conference on Computer and Communications Security* (New York: ACM Press, 1994), 59-67.

⁴⁰¹ Allison and Zelikow, *Essence of Decision*, 307.

competitive encryption systems offered by the private sector. Being first was the only way to solve the strategic problem of international and domestic encryption control. However, direction by the administration forced accelerated development processes and focused decisions on overcoming short-term obstacles such as hiding development from technical scrutiny and quickly settling allegations of patent infringements. This short-term focus on solving urgent problems affected the strategic outcome by producing secretive, commercially restrictive, and technically handicapped standards. I therefore assigned a Decision Timing valance of "2" to the Government Agencies Group for its sense of urgency in developing DSS and EES.

Competitive Period Summary

The four actor groups investigated during the Competitive Period made decisions and undertook actions that can be described using Allison's models. Table 4-2 summarizes these findings and shows that the Congressional, Executive, and Government Agencies Groups followed patterns of behavior that were a mix between the Governmental Politics and the Organizational Behavior Models. These three groups had Lead Actor and Problem Perception valances that matched the Governmental Politics Model. However, these groups diverged with regard to their Favored Alternative valance. The actions of Congressional Group matched a Favored Alternative valance suggested by the GPM, while the actions of the Executive and the Government Agencies Groups matched a Favored Alternative valance suggested by the OBM. A result of these

dissimilarities was the failure of the government's Escrowed Encryption Standard, which required the force of law to work.

Table 4-2 Competitive Period Summary

Analysis Unit	Lead Actor	Problem Perception	Favored Alternative	Decision Timing	Allison Model
Congressional Group	2 government sector	2 complex	2 laws / regulations	1 incremental / tacit	GPM OBM
Encryption Technology Group	0 private sector	0 simple	0 utility maximizing	0 contingent on choices	RAM
Executive Group	2 government sector	2 complex	1 precedents / routines	2 urgent	GPM OBM
Government Agencies Group	2 government sector	2 complex	1 precedents / routines	2 urgent	GPM OBM

The behaviors of the Executive and Government Agencies Groups exactly matched the Lead Actor, Problem Perception, and Decision Timing valances suggested by the GPM. However, the Congressional Group exhibited a Decision Timing valance that matched the OBM. While actors in the Executive and Government Agencies Groups perceived the need to make urgent decisions on the information control problem, actors in the Congressional Group were more likely to make incremental and tacit decisions on legislations required to solve the problem. This mismatch in Decision Timing valance hindered the agenda setting and timeliness of the policymaking process, thereby helping actors in the Encryption Technology Group.

The initiative in this period shifted to the Encryption Technology Group as their actions matched the behaviors suggested by the Rational Actor Model. This group perceived that the private sector could solve a simple problem of ensuring information security and did not perceive an equivalent problem regarding information access concerns. Their resulting utility maximizing encryption solutions could not be controlled by uncoordinated government actions and, in time, would out compete the government's Escrowed Encryption Standard. The appeal of RAM behaviors would change the behavior of the Government Agencies Group in the next period, while the Congressional and Executive Groups would exhibit more cooperative and convergent decision behaviors.

Status Quo Period: 1998-2004

The Status Quo Period spans seven years and starts with the passage of the *Digital Millennium Copyright Act*, which encouraged the use of information technology solutions to protect intellectual property. During the first half of this period, economic growth and domestic concerns dominated the information and encryption control agendas. A fully established Internet in the United States enhanced the domestic productivity and global value of the information service sector, which now required protection. Encryption was the method of choice to protect economically valuable information, and this protection created market complaints from trading partners. A World Trade Organization (WTO) press statement on the trade policies of the United States noted that restrictions placed on the encryption components of its global goods distribution system and airline computer reservation system were unfair trade practices.⁴⁰² Within the United States, the reliance on the Internet for private and government transactions was causing increased public concern. An August 2000 current population survey (CPS) data from the Census Bureau showed that 64% of adults were concern about “Internet confidentiality.”⁴⁰³ The capabilities of United States encryption systems to protect valuable information and privacy were threatened by the use of the obsolete Data Encryption Standard.

⁴⁰² World Trade Organization, Trade Policy Reviews: United States, July 1999, Press Release Press/TPRB/108, 1 July 1999, <http://www.wto.org/english/tratop_e/tpr_e/tp108_e.htm>, accessed October 2004.

⁴⁰³ United States Census Bureau, August 2000, “Computer Ownership Supplement Variable, HESIU20, <<http://ferret.bls.census.gov>>, accessed October 2004.

The requirement to replace DES was leftover from the Competitive Period, and the lack of action was a target for electronic rights activists and the news media. A 1998 *Washington Post* article by John Schwartz amplified this requirement by touting the exploits of a DES cracker built by the Electronic Frontier Foundation (EFF): “One of the most common systems for scrambling sensitive digital data has been defeated in a 56-hour attack by a custom-built computer costing just \$250,000.”⁴⁰⁴ To focus blame on the government’s lack of progress, Mr. Schwartz claimed that he contacted the United States Department of Commerce and the National Security Agency and did not receive an answer on the significance of cracking DES.⁴⁰⁵ I will analyze the actions of the Encryption Technology Group as they forced the development of more capable encryption systems.

The National Institute of Standards and Technology realized the requirement to replace DES with a much stronger 128-bit or better secret key encryption algorithm. After an international development competition, NIST selected the Belgian Rijndael encryption algorithm as the new Advanced Encryption Standard (AES). John Schwartz, now writing for the *New York Times*, noted NIST Director Ray Kammer’s praise for the new algorithm: “Rijndael provided ‘the best balance of robustness and versatility’ of all the finalists, since it can be used on puny personal computers and even microchip-

⁴⁰⁴ John Schwartz, “One High-End PC Cracks Data-Scrambling System Privacy Groups Say Export Curbs Undercut,” *Washington Post*, 121, no. 225 (18 July 1998): A9.

⁴⁰⁵ *Ibid.*

enabled smart cards.”⁴⁰⁶ Also in his article, Mr. Schwartz extolled the strength of AES with the following claim: “The standard institute estimates that today’s computers would take approximately 149 trillion years to decrypt such a message.”⁴⁰⁷ The secret key encryption requirement for information security tools appeared to be solved with AES, while national security and public safety concerns on information access were not addressed. I will analyze the actions of the Government Agencies Group as they developed new encryption standards such as AES.

The September 11, 2001 attack on the United States brought recriminations of intelligence failures, which were blamed in part on encryption use. While the Clinton administration and some members in the legislative branch tried to control encryption use in the Competitive Period, the attack now provided the impetus for action. AP Internet writer Anick Jesdanun captured this sentiment in an on-line article written shortly after the attack: “In a terror-induced climate of heightened electronic vigilance, debate is brewing over whether makers of electronic software should be obliged to provide law enforcement with the keys to open scrambled messages.”⁴⁰⁸ With the collapse of the Escrowed Encryption Standard several years earlier, the government knew that it would be impossible to mandate an encryption system upon a citizenry distrustful of a powerful central government. However, the threat of future attacks could be used to reach an

⁴⁰⁶ John Schwartz, “Technology; U.S. Selects New Encryption Technique,” *New York Times* 110, no. 51,530 (3 October 2000): C12.

⁴⁰⁷ *Ibid.*

⁴⁰⁸ Anick Jesdanun, “Attacks Renew debate Over Encryption Software,” *Chicago Tribune* Online Edition, 28 September 2001, <<http://www.chicagotribune.com/technology/local/sns-worldtrade-encryptionsoftware,0,4922753.story>>, accessed October 2004.

unwritten compromise with encryption users and vendors. I will analyze the actions of the Congressional Group and the Executive Group in protecting the global information infrastructure and for tacitly satisfying national security and public safety requirements threatened by the misuse of encryption technology.

Congressional Group

In the Status Quo Period, the primary actor in the Congressional Group was Congress as a whole in passing the *Digital Millennium Copyright Act* in 1998, the *Electronic Signatures in Global and National Commerce Act* in 2000, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, and the *Cyber Security Research and Development Act* in 2002. These laws did not challenge the executive branch and, except for the broad powers found in the *USA PATRIOT Act*, focused on solving legal, economic, and research issues associated with information security. Laws on the use of encryption to protect intellectual property and to facilitate electronic transactions demonstrated that Congress could solve the economic and information security pieces of the problem.

Although the *USA PATRIOT Act* satisfied national security and public safety concerns, this law did nothing to control the use of encryption. The failure to renew the *Export Administration Act* in 2001 showed that Congress did not have the required political consensus for decisions in areas such as the export of dual-use technology. The inability of Congress to pass tough encryption control provisions in the *USA PATRIOT Act* or encryption liberalizing laws such the proposed 1999 *Security and Freedom*

through Encryption Act (SAFE Act) demonstrated the divisive, but static nature of encryption control problem. While the majority of Congress supported encryption liberalization laws, powerful congressional leaders and committees would not explicitly compromise national security and public safety requirements for information privacy and economic gains.

Other active members of the Congressional Group during this period were the research services and congressional committees that helped Congress investigate the information control dilemma, and then to screen, markup, and track legislations. The text found in the laws just mentioned, proposed encryption and export legislations, the *Congressional Record*, and committee and Congressional Research Service reports provided the data for analyzing the actions of the Congressional Group. I analyzed this data according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

Actors in the Congressional Group believed that government action in conjunction with private sector technology and marketing advancements produced optimum solutions for the information control problem. In addition, actors in this group believed that unilateral government actions, which guaranteed information access for national security and public safety reasons, were counter-productive to their economic goals. The first public law determining the use of encryption in the Status Quo Period was the *Digital Millennium Copyright Act* (common nickname is *DMCA*). This law focused on the global protection of intellectual property in the Information Age. A consequence of

negotiating the 1996 World Intellectual Property Organization (WIPO) copyright treaties required the United States to pass a public law that would ensure domestic enforcement of these treaties. More importantly, government and private sector behaviors directed by this new domestic law were supposed to produce reciprocal behaviors with other WIPO members. In September 1997, Representative Howard Coble (R-North Carolina) chaired the House Committee on Courts and Intellectual Property, which held hearings on the WIPO compliance law. He opened the hearing with a claim that the United States did not require big changes in its copyright laws:

The treaties do not require the United States change the substance of our domestic copyright rights or exceptions. They do require we address the problems posed by the possible circumvention of technologies, such as encryption, which will be used to protect copyrighted works in the digital environment and for the development of secure on-line licensing systems.⁴⁰⁹

The text shows Representative Coble believed that the focus of governmental action was on “the problems posed by the possible circumvention of technologies, such as encryption.” In addition, he believed that once the United States acted to limit circumvention technologies with laws, global actors would do the same in their home countries. After the opening remarks by Representative Coble, the government agenda in the hearing soon expanded beyond creating a WIPO compliance law and protecting encryption technology.

⁴⁰⁹ House Committee on the Judiciary, Subcommittee on Courts and Intellectual Property, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 105th Congress, 1st sess., 16-17 September 1997, serial no. 33, 26.

Other members of the committee believed that a new law had to consider the actions of intellectual property creators and the telecommunications service industry. Representative Rick Boucher (D-Virginia) saw merit in broadening the debate as the government was not the only actor involved:

It is essential, Mr. Chairman, in my view that these issues be joined; not just for the purpose of these hearings, but that they be joined in a single bill prior to the presentation of legislation by the House Judiciary Committee to the full House of Representatives. By joining these issues together, parties on all sides will preserve their maximum leverage, and therefore I think will be more forthcoming in the discussions and the negotiations that lie ahead. And the opportunity for us to achieve a balanced agreement that protects the concerns of content owners and on-line service provider individuals, as well as those who manufacture equipment, will be best enhanced in the event that we are able to join these issues together.⁴¹⁰

The text shows that there were “parties on all sides” of these issues and that “discussions and negotiations” would actually take place in the hearings. The three parties according to the text were equipment manufacturers, “content owners,” and “on-line service provider[s].” The common element among these parties was economic gain, thus leaving public policy issues, such as fair-use of digital content and reverse engineering of protection systems for research, without a strong champion. Electronic rights activists attempted to fill this void at the hearings, but the government and business sector consortium was too strong. The same consortium also passed a digital signature law to satisfy global e-commerce concerns.

⁴¹⁰ *Ibid.*, 28.

While federal control over diverging state laws was a large motivator for Public Law 106-229, the *Electronic Signatures in Global and National Commerce Act (E-SIGN)*, the government also had global technology leadership and economic motives. Senator Robert F. Bennett (R-Utah) opened a March 1998 hearing on the predecessor to the *E-SIGN Act*, which was S. 1594, *The Digital Signature and Electronic Authentication Law [SEAL] of 1998*. Senator Bennett discussed the economic importance of digital signature technology:

Putting pen to paper to sign a document has served us well over the centuries, but as we move toward the 21st century and the digital age, something other than looking at the handwriting of an individual is necessary to certify and authenticate transactions.

The technology for electronic authentication is readily available. In fact, many different technologies have been developed and are competing for the vast potential business anticipated as electronic banking and commerce develops. Several of those technology vendors have submitted statements for the record today, and we are very grateful to them for helping us to understand what is taking place.

Unfortunately, financial institutions and other businesses across the country have hesitated to fully invest in these available technologies. The question, obviously, is, why?⁴¹¹

The text suggests that Senator Bennett believed that new technology was needed to replace the process of “looking at the handwriting of an individual” in order to “certify and authenticate transactions.” One candidate technology was public key encryption based digital signatures. Senator Bennett also noted, “[M]any different technologies have been developed and are competing for the vast potential business.” In theory, the market

⁴¹¹ Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on Financial Services and Technology, *The Digital Signature and Electronic Authentication Law [SEAL] of 1998—S. 1594*, 105th Congress, 2nd sess., 11 March 1998, Senate Hearing 105-896, 1.

would eventually select the utility maximizing technology as the standard, but Senator Bennett's rhetorical question implied that government intervention in the private sector could hasten the process. He answered his own question with a statement: "We believe the answer is because the law on electronic authentication does not currently provide the support necessary to justify such a substantial investment."⁴¹² His choice of the word "support" instead of the word "leadership" suggests that the government was coequal with the business sector in promoting electronic signatures. During the hearing, Senators on the committee did not debate the national security and public safety aspects of encryption-based digital signature technology, which indicated that a dominant government leadership role was not required. A year later, members from the House attempted legislation to codify the government's consortium status with the business and technology sectors.

In 1999, Representative Coble chaired a House committee hearing on the *Security and Freedom through Encryption (SAFE) Act*, H.R. 850. This act would have ended most domestic and international restrictions on the use and export of encryption:

Mr. COBLE. As you know, encryption is the process of encoding data communications in a form that only the intended recipient can understand. Once the exclusive domain of the national security agencies, encryption has become increasingly important to persons and companies in the private sector concerned with the security of the information they transmit. H.R. 850 seeks to provide a means of ensuring protection for confidential communications transmitted in this

⁴¹² *Ibid.*, 2.

information age. It also seeks to lift restrictions on the exportation of advanced encryption so U.S. information companies will remain the world leader.⁴¹³

The text shows that H.R. 850 acknowledged a shift in encryption technology leadership from being the “exclusive domain of the national security agencies” to now being a shared responsibility with “persons and companies in the private sector concerned with the security of the information they transmit.” In addition, the text suggests a congressional desire that “U.S. information companies remain the world leader.” This consortium view of government technology leadership had popular support in that the bill had “over 200 cosponsors, including both Republicans and Democratic leadership.”⁴¹⁴ This bill did not pass, because the sentiment of Congress was that no encryption control crisis threatened national security and public safety and that the government and private sectors together were adequately addressing information technology leadership and economic issues.

The September 11, 2001 attack on the United States shocked congressional actors into the realization that the lack of encryption control had jeopardized intelligence collection on terrorists. On September 12, 2001, Senator Judd Gregg (R-New Hampshire) addressed the whole Senate on intelligence failures:

Mr. GREGG....

In fact, at three different hearings that I know of when I was chairman of the appropriations subcommittee that has jurisdiction over the Justice and State

⁴¹³ House Committee on the Judiciary, Subcommittee on Courts and Intellectual Property, *Security and Freedom through Encryption (SAFE) Act*, 106th Congress, 1st sess., 4 March 1999, Serial No. 34, 6-7.

⁴¹⁴ *Ibid.*, 7.

Departments, it was clearly stated by our intelligence community that they anticipated a significant terrorist act sometime in the future. No one was specific as to when. We now know when. It has occurred.

How do we prepare so it does not occur again or so we can mitigate the damage? ...

We have electronic intelligence of immense capability. It needs to be improved, especially in the area of encryption. But specifically, we need more people involved in intelligence efforts. We have to, as a nation, recognize that this is, for all intents and purposes, a war, and that it is going to take soldiers, and that some of those soldiers are going to have to participate in counterintelligence activities that are covert and personal, something from which we have shied away as a society. We are going to need to commit significant resources to this.⁴¹⁵

The text shows that, although the United States had “electronic intelligence of immense capabilities,” the specific area of defeating encryption was an intelligence weakness.

Like President Reagan’s public warning on Soviet encryption being used to hide missile telemetry seventeen years prior, Senator Thompson was warning Congress on the continuing intelligence perils posed by hostile encryption use. While several other congressional hearings heard similar encryption warnings, Congress did not take action to control encryption.

The *USA PATRIOT Act* became Public Law 107-56 on 26 October 2001 and expanded *FISA* powers, but did not include legal mechanisms to obtain encryption keys.⁴¹⁶ A review of the House Judiciary Committee report on the *USA PATRIOT Act* shows why this act did not contain encryption controlling legislation:

⁴¹⁵ *Congressional Record*, 107th Congress, 1st sess., 2001, 147, pt. 118: S9301.

⁴¹⁶ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, U.S. Statutes at Large* 115 (2001): 272-402.

VOTES OF THE COMMITTEE

(1) An amendment was offered by Mr. Boucher (for himself, Mr. Goodlatte, and Mr. Cannon) to insert language at the end of title I that states “Nothing in this Act shall impose any additional technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities, services or technical assistance.” The amendment passed by voice vote.⁴¹⁷

The text shows that Representative Goodlatte, the author of the *SAFE Act*, and two other legislators effectively limited the government’s ability to get encryption keys from private sector telecommunications service providers. The phrase “any additional technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities, services or technical assistance” was similar to the one used in the 1996 *Communications Assistance to Law Enforcement Act*. Thus, the government could not place extra technical demands on the private sector for assistance with intelligence gathering that satisfied national security and public safety requirements.

Less than a year after the September 11, 2001 attack, actors in the Congressional Group perceived that ensuring digital information security was a consortium effort. A report of the Committee of the Whole House on the *Cyber Security Research and Development Act* documented their thoughts on leadership in this area:

While private industry has rapidly advanced many aspects of information technology, it has had little incentive to focus on the development of cyber security. The market demands faster, cheaper, more powerful products, not more

⁴¹⁷ House Committee on the Judiciary, *Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001*, 107th Congress, 1st sess., 11 October 2001, Report 107-236, Part I, 42.

secure ones. In the wake of the September 11th attacks, security has a slightly higher profile in the private sector, but real advances in information assurance will still rely on efforts by the Federal Government.⁴¹⁸

The text indicates that Congress saw the private sector as producing “faster, cheaper [and] more powerful products,” but not products responsive to security requirements of the post attack period. Thus, the government had to assist the private sector with developing “real advances in information assurance.” This approach seemed sensible as government agencies, when properly directed and funded, could perform the required information assurance tasks and produce information security standards for all sectors.

The view that actors in the Congressional Group had to work in conjunction with the private sector matched Allison’s OBM organizing concept of “Organizational Actors.” According to this concept, encryption policy actors did not work as a “monolithic nation or government but rather a constellation of loosely allied organizations.”⁴¹⁹ During the Status Quo Period, Congress as a whole assisted the private sector with intellectual property protection schemes, legalization of digital signatures, and information security research funding. After the attack on September 11, 2001, Congress did not take the lead to balance information security and information access requirements. This left satisfaction of these requirements to a government and private sector consortium. I therefore assigned a Lead Actor valance of “1” to the Congressional

⁴¹⁸ House Committee on Science, *Cyber Security Research and Development Act*, 107th Congress, 2nd sess., 4 February 2002, Report 107-355, Part I, 5.

⁴¹⁹ Allison and Zelikow, *Essence of Decision*, 166.

Group for being part of a consortium that was focused on economic, security, and technology leadership issues.

B. Problem Perception Valance

The Congressional Group perceived the information control issue as a complex problem with international and domestic dimensions and with economic, national security, public safety, and technology leadership requirements to satisfy. The hearings on the *Digital Millennium Copyright Act* demonstrated that the initial preference of Congress was to solve the economic and technology pieces of the problem. The *DMCA* hearings covered H.R. 2281, *WIPO Copyright Treaties Implementation Act*, and H.R. 2180, *Online Copyright Liability Limitation Act*, in order. Representative John Conyers, Jr. (D-Michigan) questioned the relationship between a bill that affected an international treaty and a bill that protected the domestic liabilities of telecommunications service providers:

Mr. CONYERS. Say what I need to know here.

Mr. COBLE. I say to you there are two separate bills, each free standing.

Mr. CONYERS. Right. Oh, okay. So, they are two freestanding bills, but you have 57 bills in your committee. Was it accidental? You just reached into the basket and pulled these two and coupled them?

One bill we could almost go tomorrow, after we hear the witnesses, to markup. We are implementing a treaty that has been asked by 60 nations. The other bill, this liability bill, there are going to be some more hearings, unless I misjudged my reading of this hearing.⁴²⁰

⁴²⁰ House Committee, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 94.

The text shows Chairman Coble of the Subcommittee on Courts and Intellectual Property believed that there were “two separate bills,” while Representative Conyers questioned the Chairman’s coupling of the treaty implementing H.R. 2281 with the liability limiting H.R. 2180. In addition, Representative Conyers claimed that H.R. 2281 could go “to markup,” while H.R. 2180 required “more hearings.” Subsequent debates on H.R. 2180 and H.R. 2281 proved Representative Conyers was not correct.

Both bills were interrelated and required because the global protection of digital intellectual property started with solving the complex problems of domestic use, sharing of intellectual property, and the liabilities incurred by the developers and providers of telecommunications technologies and services. Representative Sonny Bono (R-California) noted that within the allegedly mature H.R. 2281, domestic content providers were accorded differing definitions and protections of their intellectual property:

What bothers me is that we take one industry or one portion of that industry and conduct ourselves in one manner, and then we go into the music business and conduct ourselves in another manner. And I, Mr. Chairman, frankly do not understand it, and I am concerned about approaching the whole issue in this manner, which is we all agree that technology is now becoming the product of America, and that intellectual property is connected to that, so it has to be protected. We are going two ways on the same specific issue with intellectual property. Intellectual property is intellectual property.⁴²¹

The text indicates that the contentious part of the hearing was the domestic protection of intellectual property against advances in information technology. Representative Bono believed that separating copyright issues according to their information contents and

⁴²¹ *Ibid.*, 32-33.

types of enabling technologies was like “going two ways on the same specific issue with intellectual property.” He believed that legislative actions should have focused more on telecommunications technologies that enabled music and software theft and less on the contents of stolen material. Congressional supporters of the telecommunications industry perceived the problem to be with the ubiquitous nature of digital intellectual property and believed that technology solutions such as encryption could solve the problem.

Others actors in the Congressional Group believed that advances in information technology would not threaten digital intellectual property, but would overly protect such property to create a “fair use” of information problem. Representative Zoe Lofgren (D-California) believed this to be true and stated the following during the hearing: “There is encryption technology that basically will wall off digital transmissions, absent appropriate interface with the content provider.”⁴²² She went on to bring up questions on “Fair Use doctrine,” where users could make copies of information they owned and “reverse engineering” concerns, where users and industry could create devices to decrypt and use protected information.⁴²³ These additional domestic concerns proved the complexity of the information control problem by eventually affecting the international enforceability of H.R. 2281. Other WIPO countries had their own definitions of digital intellectual property and their own views on fair use and reverse engineering rights. These issues were not solved before Congress attempted to legislate an international definition for digital signatures, including public key encryption based signatures.

⁴²² *Ibid.*, 110.

⁴²³ *Ibid.*, 144.

During Senate hearing on the proposed *SEAL Act*, Chairman Bennett showed the complex nature of this bill by citing the international, domestic, and economic reasons for the law. In his introductory remarks, Senator Bennett explained his goals:

One aspect of the electronic age is that it does not recognize geographic borders and many times involves people who do not have a face-to-face kind of relationship, so the need for legal certainty extends beyond the borders of States, and also beyond the borders of this country. Internet transactions take place globally and instantly. Countries around the world are getting their own laws and systems in place. We need, at the least, to get Federal legislation enacted that would allow us to negotiate with other countries from a common base and on a comprehensive global scheme.

This is what drove me to introduce, on February 2, 1988, the Digital Signature and Electronic Authorization Law, or SEAL. We look for acronyms around here that can give us some distinction and that is what we came up with for this bill. This legislation would authorize financial institutions to use electronic authentication, and further provide that when the parties to a transaction agree to use electronic authentication, the electronic signature, under law, would be considered as valid as the one created with pen and paper.⁴²⁴

The text describes the international and domestic reasons for a legalized global authentication scheme among “people who do not have a face-to-face kind of relationship.” If executed properly, then this authentication “would be considered as valid as the one created with pen and paper.” These phrases are similar to ones used by Diffie and Hellman in their 1977 explanation of the requirement for a public key encryption subsystem. The information security linkage between authentication and confidentiality was not discussed by Senator Bennett, but was introduced by a witness.

⁴²⁴ Subcommittee on Financial Services and Technology, *The Digital Signature and Electronic Authentication Law [SEAL] of 1998—S. 1594, 2.*

Actors in the Congressional Group were silent on the relationship between digital signature technologies and encryption policy even though witnesses brought up the issue. In the hearing, Mr. Harris N. Miller, President of the Information Technology Association of America, responded to the apparent liberties that the financial sector enjoyed in exporting United States encryption products:

Senator BENNETT. Thank you.

Mr. Miller, your body language says you want to respond.

Mr. MILLER. I'm glad that Mr. Nugent [Citibank counsel] brought up the example of encryption. We're very pleased that the financial institutions are able to export software with high encryption, but, again, that's an example of hanging together or hanging separately.

Because the financial services industry has been hived off, Congress and the Administration so far have been able to resist the entreaties of the information technology industry to more broadly allow the export of higher strength encryption.⁴²⁵

The text indicates that actors in the Congressional Group solved complex problems in the past by focusing on the international and domestic concerns of a specific industry.

Although Mr. Harris' claim on the "export of higher strength encryption" pertained to the secret key encryption subsystem and not the public key encryption subsystem used in digital signatures, his notion that the financial services industry had "been hived off" by Congress from encryption export restrictions was not debated by Senator Bennett. Actors in the Congressional Group did consider export restrictions and information access requirements for all industries in subsequent legislation.

⁴²⁵ *Ibid.*, 19.

While the *SEAL Act* debate avoided the national security and public safety aspects of encryption use, actors in the Congressional Group attempted to pass legislation that satisfied information access requirements to encrypted data. The Senate Committee on Commerce, Science, and Transportation issued a report on S. 798, the *Promote Reliable On-line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999*, which countered the encryption liberalizing *SAFE Act*, H.R. 850. The committee had its own intertwined views on how regulating encryption use could balance information access and information security requirements:

THE PROTECT ACT ENSURES THE PROTECTION OF NATIONAL SECURITY INTERESTS

The greatest guarantor of U.S. national security interests in a digital age is the complete dominance of the United States encryption producing industries. The PROTECT Act puts into place procedures to allow such industries to effectively compete for such dominance. However, the PROTECT Act reflects the legitimate concerns of both law enforcement and national security. The Act clarifies that the U.S. government may continue to impose export controls on all encryption products to terrorist countries, and embargoed countries; that the U.S. government may continue to prohibit exports of particular encryption products to specific individuals, organizations, country, or countries; and that encryption products remain subject to all export controls imposed for any reason other than the existence of encryption in the product.⁴²⁶

The text suggests that the Senate committee perceived a complex relationship between technology leadership and national security when it used the following statement: “The greatest guarantor of U.S. national security interests in a digital age is the complete dominance of the United States encryption producing industries.” Countering this simple

⁴²⁶ Senate Committee on Commerce, Science, and Transportation, *The Promote Reliable On-line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999*, 106th Congress, 1st sess., 05 August 1999, Senate Report 106-142, 8.

view of the problem was the subsequent idea that “the U.S. government may continue to prohibit exports of particular encryption products to specific individuals, organizations, country, or countries.” The report did not detail the rectification of these suggested approaches to encryption control, but the Senate’s support of encryption control differed significantly from the House’s version, H.R. 850, which specified more encryption liberalization as the solution.

House committee members knew that encryption control was a complex problem that would be difficult to solve. During the 1999 *SAFE Act* hearing, the opening remarks of ranking minority member, Representative Howard L. Berman (D- California), went directly to this point:

I congratulate you on having this hearing and for your decision to get to the issues underlying this legislation very quickly in the beginning of this Congress. The issues surrounding encryption are very complex, and it remains one of the most serious and complicated issues that our subcommittee will address this year.⁴²⁷

The *SAFE Act*, H.R. 850, treated the information control problem in the opposite manner of the *PROTECT Act* by promoting the use of encryption to ensure information security. In this way, private sector information vital to national security and public safety could be protected from foreign governments and criminals. During the March 1999 *SAFE Act* hearing, Representative Lofgren offered her perception of the information control problem:

⁴²⁷ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 7-8.

Much has been said recently about our vulnerability to attack by terrorists and by rogue individuals, by those who would harm our Nation. One of the best ways to protect our system of information, our computer system [, which] is basic infrastructure [,] is through strong encryption. So I am hopeful we can get past this together, for the benefit of both law enforcement and our economy.⁴²⁸

Her idea represents a new approach to the information control problem whereby “basic infrastructure” would be protected “through strong encryption.” Thus, encryption use was now perceived as being beneficial to “both law enforcement and our economy” and as having an ambiguous effect on national security and public safety. Actors in the Congressional Group now faced an intertwined relationship between potential encryption controlling and liberalizing laws and their resulting complex national security and public safety effects. Encryption use simultaneously helped and hurt the United States.

The September 11, 2001 attacks polarized perceptions of the problem by actors in the Congressional Group. Within a few days of the attack, Senator Judd Gregg (R-New Hampshire) addressed the Senate on the need for encryption control:

I have ideas how to do this so we do not undermine their activity to sell their [encryption] product, and ideas that will allow us as a nation that wants to protect the civil rights of individuals and constitutional rights of individuals to do that, yet still allow our law enforcement community, when it sees a need, to be able to break a code.⁴²⁹

Within a few months after the attack, Representative Connie Morella proposed the *Computer Security Enhancement Act of 2001*, H.R. 1259. This act would have liberalized encryption use in order to enhance security:

⁴²⁸ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 15.

⁴²⁹ *Congressional Record*, 107th Congress, 1st sess., 2001, 147, pt. 122: S9469.

(4) The development and use of encryption technologies by industry should be driven by market forces rather than by Government imposed requirements.⁴³⁰

These two texts suggest that a demonstrated national security and public safety threat did not alter the perceptions of a complex problem by members of the Senate and the House.

A 2002 House report on the *Cyber Security Research and Development Act*, H.R. 3394, showed that the problem perception on information security remained complex after September 11, 2001. Actors in the Congressional Group perceived that information security vulnerabilities now threaten the United States government and an information dependent society:

VULNERABILITIES OF THE NATIONAL INFORMATION INFRASTRUCTURE

The Internet has been a tremendous success—connecting more than 100 million computers and growing—far outstripping its designers’ wildest expectations. Yet the Internet was not originally designed to control power systems, connect massive databases of medical records or connect millions of home appliances or automobiles, yet today it serves these functions. It was not designed to run critical safety systems but it now does that as well. We now heavily rely on an open network of networks, so complex that no one person, group or entity can describe it, model its behavior or predict its reaction to adverse events.⁴³¹

The text shows that House members were concerned that the “Internet was not originally designed to control power systems, connect massive databases of medical records, or connect millions of home appliances or automobiles.” In addition, these members perceived a growing information security problem in that the United States was using “an

⁴³⁰ *Congressional Record*, 107th Congress, 1st sess., 2001, 147, pt. 161: H8351.

⁴³¹ House Committee on Science, *Cyber Security Research and Development Act*, 2.

open network of networks, so complex that no one person, group or entity [could] describe it, model its behavior or predict its reaction to adverse events.” This new perception of protecting national security and public safety through information security tools added a complex dimension to the countervailing perception of protecting national security and public safety through guaranteed information access by the government.

The view of a complex problem by the actors in the Congressional Group matched Allison’s GPM organizing concept of “Parochial Priorities and Perceptions,” where perceptions are “colored by the position from which the question is considered.”⁴³² Starting with the 1998 *DMCA*, actors in the Congressional Group perceived that increasing global economic gains through technology leadership required the protection of intellectual property using such measures as encryption. Some congressional actors feared the opposite in that encryption use by content providers would present an information access problem to the public. The *E-SIGN Act* gave legal status to the public key encryption subsystem in order to assist the United States financial services sector in global and domestic competitions. While the Congressional Group considered the security and public safety aspects of encryption use, a reversal of perceptions changed encryption use from being a threat to national security and public safety to actually protecting these areas. The September 11, 2001 attack reinforced the bifurcated perceptions of congressional members with the Senate generally perceiving an information access problem for the government sector and the House generally

⁴³² Allison and Zelikow, *Essence of Decision*, 298.

perceiving an information security problem for all sectors. The 2002 *Cyber Security Research and Development Act* added to these differing perceptions by favoring information security research over information access research. I therefore assigned a Problem Perception valance of “2” to the Congressional Group for perceiving complex and intertwined problems.

C. Favored Alternative Valance

Actors in the Congressional Group favored digital information control laws that satisfied treaty obligations, maintained United States technology leadership, and promoted international and domestic economic goals. In the areas of protecting national security and public safety, the House and Senate tried but could not reach an agreement on an encryption law that would balance information access with information security requirements. During the House hearing on the *Digital Millennium Copyright Act*, Representative Howard L. Berman (D-California) spoke in disagreement with his fellow minority member, Representative Boucher, on the key purpose of the hearing:

Mr. BERMAN. Mr. Chairman, I do not have an opening statement. It seems to me that it is a key priority for this Congress to act on the implementing legislation submitted by the Administration on the not so recently concluded WIPO treaties, dealing with the digital technology and copyright protection.

We are talking here about industry—the export and protection of copyrighted works which produces tens of billions of dollars in surplus balance of

trade for this country, with very significant employment consequences, and additional strength to our economy.⁴³³

In the text Representative Berman believed that it was “a key priority for this Congress to act on the implementing legislation.” The executive branch had done its part in negotiating the WIPO treaties and Congress had yet to produce the ratifying legislation. In addition, the text shows that Representative Berman recognized the motivation behind the legislation as “the export and protection of copyrighted works.” He believed that the trade in intellectual property created a United States trade surplus of “tens of billions of dollars.” His fellow minority member on the committee agreed with the requirement for this export enhancing legislation, but favored legislation commensurate with the complex domestic nature of problem.

Representative Boucher believed that the final legislation had to control the interplay of digital information, information sharing technologies, and the roles and liabilities of digital intellectual property owners and telecommunications service providers. During the hearing, he presented his views to Chairman Coble:

During the course of the last Congress these issues were joined together in the draft legislation that we considered. We never quite got to the point of introducing a formal bill in all the various drafts the were considered by interested members and by various stake holders, the issues what we call the 1201 set of concerns—[circumvention] devices and conduct—and the issues related to on-line

⁴³³ House Committee, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 27.

service provider liability were joined. And I would respectfully suggest, Mr. Chairman, that this be done again in this Congress.⁴³⁴

The text shows that in order for the proposed *DMCA* to become law, “issues” had to be “joined together” and then “considered by interested members and by various stake holders.” Representative Boucher’s joining efforts were important to encryption policy in that the “[circumvention] devices and conduct” section of the law gave legal support to information security tools used to protect copyrighted digital content. A product of *DMCA* was that large media corporations could use encryption to protect their property such that users would be punished if they tried to break or circumvent this encryption. Encrypted material on Digital Versatile Disks (DVD) would have this specific protection, while unencrypted audio on Compact Disks (CD) would not.

The multifaceted *E-SIGN Act* showed that Congress favored laws to control the behaviors of fifty states in their acceptance of electronic signatures. Another facet of this law sought to advance the technology leadership and economic interests of the United States. A June 2000 report on S. 761, the Senate version of the *E-SIGN Act*, focused on the regulating role of Congress:

Presently, however, one of the greatest barriers to the growth of Internet commerce is the lack of consistent, national rules governing the use of electronic signatures. More than forty States have enacted electronic authentication laws, and no two of these laws are the same. This inconsistency deters businesses and

⁴³⁴ *Ibid.*, 29. Misuse of the anti-circumvention term was corrected.

consumers from using electronic signature technologies to authorize contracts or transactions.⁴³⁵

The text suggests that the Senate acted because of divergent state laws: “More than forty States have enacted electronic authentication laws, and no two of these laws are the same.” The more encompassing House bill H.R. 1714, the *E-SIGN Act*, added to the Senate bill by advancing the technology leadership and financial interests of the United States. During the June 1999 hearing by the House Subcommittee on Telecommunications, Trade, and Consumer Protection, Chairman Billy Tauzin (R-Louisiana) claimed the *E-SIGN Act* went beyond regulating the states:

Another important element of this legislation is that it provides this sector of Commerce with guidance in promoting American principles on electronic signature laws overseas. It would clearly harm American interests to have foreign nations enact laws that would, or could, discriminate against American products and companies; or create closed systems that do not recognize the technologies and systems used by American companies.⁴³⁶

The text suggests that the House created H.R. 1714 to promote “American principles on electronic signatures laws overseas.” In addition, the text shows that the intent of H.R. 1714 was to preempt the foreign creation of “closed systems that do not recognize the technologies and systems used by American companies.” Figure 4-6 shows the success of the *E-SIGN Act* over state laws and international conventions. The authority of the *E-SIGN Act* is demonstrated by the phrase, “Federal law authorizes electronic signature by

⁴³⁵ Senate report 106-131

⁴³⁶ House Committee on Commerce, Subcommittee on Telecommunications, Trade, and Consumer Protection, *The Electronic Signatures in Global and National Commerce Act*, 106th Congress, 1st sess., 9 June 1999, Serial No. 106-32, 2.

authenticated request.” However, the *E-SIGN Act* did not address the international use of encryption products to protect confidentiality. Figure 4-6 shows the additional use of an encryption system with the following notice: “All credit card information is encrypted for your protection.”

Payment Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://myieemembership.ieee.org/renewal/RenewalPayment.jsessionid=BD65Kv1Yv2JqLw7J1yrTnW7FvvhQCvJGGK54w>

Back Search Favorites 1087 blocked AutoFill Options

Google - Search Web

Pay now with your credit card or print your renewal form and mail it with payment. If you have subscribed to the IEEE Member Digital Library, you must pay on-line by credit card through the IEEE Web Renewal or IEEE Add Services applications.

Total Amount Due: US \$153.00

OPTION 1:

Pay By Credit Card Payment Secure by VeriSign

Federal law authorizes electronic signature by authenticated request from a customer over the internet as a valid substitute for a written signature.

Enter your credit card information below.
All credit information is encrypted for your protection.

Type: VISA MasterCard Diners Club AMEX
(IEEE or other) (IEEE or other)

Cardholder's Name: MARK DEVIRGILIO

Number: _____

Expiration Date(MM/YY): ____/____

5 digit Zip Code(US Only): _____

NOTE: After selecting "checkout", processing of your Credit Card payment may take up to 30 seconds. To avoid duplicate charges click "checkout" only once. Your "Receipt for Payment" and "Web Renewal Reference Number" will follow. Do not click STOP or follow any links until the transaction is complete.

Figure 4-6 Internet credit card transaction showing the use of electronic signatures for authentication and encryption for confidentiality.

The attack on September 11, 2001 did not force Congress to select between encryption controlling and liberalizing legislations that had been circulating in both houses for all of the Status Quo Period. The *Uniting and Strengthening America by*

Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

greatly expanded government surveillance powers, especially powers authorized by *FISA*. With regard to digital information and communications, the *USA PATRIOT Act* expanded access to unprotected information:

“§ 2703. Required disclosure of customer communications or records”; ...

“(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity ...”⁴³⁷

This extract shows that the *USA PATRIOT Act* allowed for the disclosure of “a record or other information pertaining to a subscriber to or customer of such service ... to a governmental entity.” In addition, the *USA PATRIOT Act* forced the disclosure of financial, immigration, and law enforcement information to the government.⁴³⁸ In the case of information being protected by encryption, this law was silent on circumventing information security to allow government access. Likewise, this law was silent on enhancing information security through mandatory encryption use. Protecting information from criminals, spies, and terrorists seemed like a logical task for the *USA PATRIOT Act*, but such considerations would have hindered passage.

⁴³⁷ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, U.S. Statutes at Large* 115 (2001): 272-402.

⁴³⁸ *Ibid.* This was determined using a word search for “data access” or “information access” to find the relevant sections.

After the *USA PATRIOT Act*, Congress passed the *Cyber Security Research and Development Act*, H.R. 3394, which sought technology solutions to the information security problem:

II. BACKGROUND AND NEED FOR LEGISLATION

The terrorist attacks of September 11, 2001 brought into stark relief the Nation's physical and economic vulnerability to an attack within our borders. The relative [e]ase with which terrorists were able to implement their plans serves as a pointed reminder of the need to identify critical "soft [spots]" in the nation's defenses. Among the Nation's vulnerabilities are our computer and communications networks, on which the country's finance, transportation, energy and water distribution systems, and health and emergency services depend. These vulnerabilities have called into question whether the Nation's technological research programs, educational system, and interconnected operations are prepared to meet the challenge of cyber warfare in the 21st century.⁴³⁹

The text shows that House members realized the potential for terrorists to exploit "the Nation's physical and economic vulnerability," especially in "computer and communications networks." One problem perceived by the House was a lack of technology leadership "to meet the challenge of cyber warfare in the 21st century." H.R. 3394 would fix this problem by making available money for research on "authentication and cryptography, computer forensics and intrusion detection, reliability of computer and network applications, and privacy."⁴⁴⁰ This law, however, did not have a commensurate funding increase for research on information access, which many national security actors believed was also required to ensure information security.

⁴³⁹ House Committee on Science, *Cyber Security Research and Development Act*, 2.

⁴⁴⁰ *Ibid.*, 57.

Actors in the Congressional Group exhibited behaviors that matched Allison's GPM general proposition of "The Face of the Issue Differs from Seat to Seat," where laws are passed to "obtain at least limited agreement on the face of the issue, at least for the moment."⁴⁴¹ Congress passed a series of legislations to solve the international and economic issues surrounding information security. Through the passage of the 1998 *Digital Millennium Copyright Act*, a majority of congressional actors believed that laws guaranteeing information security of intellectual property would advance the economic interests of the United States. Instead of solely relying on technology solutions, *DMCA* used laws to protect encryption systems that were subsequently used to protect intellectual property. *DMCA* also suppressed information access requirements for both the government and individuals. The *E-SIGN Act* advanced the technology leadership and economic interests of the United States by legalizing digital signatures, which were often implemented through public key encryption technology.

Before the terrorist attack on September 11, 2001, some actors in the Congressional Group saw the other face of the issue in that laws were required to guarantee information access. The denial of information access through encryption use still threatened national security and public safety requirements, and now, encryption use could legally deny access to purchased copyrighted material and stop the legal development of competitive information system through reverse engineering. This face of the issue was lost after the attack, which elevated the requirement to protect the critical information infrastructure of

⁴⁴¹ Allison and Zelikow, *Essence of Decision*, 309-10.

the United States. Congress passed the 2002 *Cyber Security Research and Development Act* to research information security solutions. However, this law did not address the information access face of the issue in a balanced manner. I assigned a Favored Alternative valance of “2” to the Congressional Group for passing laws to achieve their important information security goals at the sacrifice of information access requirements.

D. Decision Timing Valance

During the Status Quo Period, no integrated law determined information access or information security policy. Actors in the Congressional Group made incremental decisions on laws that avoided encryption control or liberalization extremes and made tacit decisions when policies could not keep pace with advances in encryption technology. Proposed laws that challenged these extremes were forced to a more central position or were killed by legislative processes. Beginning with the 1998 *Digital Millennium Copyright Act*, actors in this group created legislations that solved pieces of the information control problem. As noted earlier, House hearings on the *DMCA* considered protecting anti-circumvention technology such as encryption, allowing fair use of protected information, and permitting the reverse engineering of protection schemes. At the end of one hearing, Representative Lofgren used the testimony of Mr. Edward J. Black, President of the Computer and Communications Industry Association, to show that the *DMCA* achieved a balance between information security and access, while the executive branch’s encryption policy did not:

Ms. LOFGREN. Finally, this has been a long hearing, and we are down to just the hardy few, I did note your comment Mr. Black, about the inconsistency in the administration's view on encryption in this area as compared to its Big Brother takes over the world encryption policy. I'm wondering if you would like to address that issue for the remaining Members.

Mr. BLACK. Yes. I thought because there is the committee's involvement, it is worth mentioning. We do think that if you really approach encryption and this issue and keep them in perspective and together, that the idea of limiting the use of technology which is vital to the encryption process, the ability to encrypt, it makes no sense.⁴⁴²

In the text, Representative Lofgren believed that there was an "inconsistency in the administration's view on encryption in this area as compared to its Big Brother takes over the world encryption policy." The inconsistency arose when the administration wanted to limit the export of strong encryption so that the government could have information access through circumvention of United States encryption products. Under *DMCA*, this circumvention would be illegal, and "people who complied with their [executive branch] proposal would be violating the law."⁴⁴³ The failure of the next two laws showed that Congress had its own set of consistency problems.

The encryption liberalizing *SAFE Act* and the encryption controlling *PROTECT Act* both failed because a sense of urgency did not exist within Congress. In the case of the *SAFE Act*, urgency was lost because policy makers could not keep pace with technology. Former Congressman Dave McCurdy, president of the Electronic Industry Alliance made a point on legislating encryption strength during the 1999 House hearing on the *SAFE Act*:

⁴⁴² House Committee, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 292.

⁴⁴³ *Ibid.*, 292.

So it is moving at such a rapid pace that there is no way that the policy can catch up. That is why it is very difficult to put it in rigid statutory form. That is why, quite frankly, if I had my druthers, I would say to the Administration—whether it is a Democratic or a Republican Administration—you all have the obligation to have a flexible policy that fits the times rather than have Congress impose a standard, because you can't pick that data point out there that you have opened up.⁴⁴⁴

The text shows that Mr. McCurdy believed that a “flexible policy” would be better than having “Congress impose a standard” on encryption strength. His rationale for a flexible policy was that a congressionally selected “data point” on exportable encryption strength could not be rationally justified. However, if Congress waited, then the executive branch’s graduated encryption strength limit for exports would effectively become policy. If Congress had to act, then the *PROTECT Act*, S. 798, would be one way of taking an incremental action.

The *PROTECT Act* relied on international actors to limit their strong encryption technology exports to questionable countries, and this dependence caused hesitation in the Senate. The *PROTECT Act* would have codified the responsibilities of the United States in accordance with the Wassenaar Arrangement. Senator Ernest F. Hollings (D-South Carolina), the ranking minority member of the Senate Committee on Commerce, Science, and Technology added a concluding statement to the *PROTECT Act* report that suggested an incremental approach:

The international control of the powerful encryption technology will require a multinational effort with real and enforceable sanctions for violations of the

⁴⁴⁴ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 6-7.163.

international controls. This international effort recently received a boost from a multilateral agreement, the Wassenaar agreement, designed to place limits on the availability of such exports. To date, the effectiveness of this agreement to curb the export of strong encryption products is in question. If the international community is unable to enforce the Wassenaar agreement and place meaningful international controls on encryption products, the Committee may have to revisit this issue.⁴⁴⁵

The text shows that Senator Hollings voiced his concern by stating, "To date, the effectiveness of this agreement to curb the export of strong encryption products is in question." As noted earlier, a premise of the *PROTECT Act* was to ensure United States encryption technology dominance. Senator Hollings realized that any encryption voids created by United States export controls would be filled by uncooperative countries. Thus, the Senate was in no hurry to pass a bill that would require a "revisit to this issue." Congress followed Mr. McCurdy's idea of policy flexibility by deferring decisions on the encryption controlling *PROTECT Act* and the encryption liberalizing *SAFE Act*.

The 2000 *E-SIGN Act* incrementally solved the information security problem by legalizing the use of public key encryption-based digital signatures in the government and private sectors. By passing the *E-SIGN Act*, Congress tacitly decided that encryption technology supporting digital signatures could be exported and used around the world. In questioning a witness, Representative John Shimkus (R-Illinois) made the point that the *E-SIGN Act* assumed freely exportable encryption, while reality suggested otherwise:

Mr. SHIMKUS. Thank you, Mr. Chairman.

⁴⁴⁵ Senate Committee, *The Promote Reliable On-line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999*, 20-21.

I want to first direct my question to Mr. Engelberg. Based upon your response, you saw us all chuckling. Encryption is part of this issue, but we also have another big issue before us on encryption. I guess the question I want to ask, first, is our issue addressing the ease of export controls for encryption products. What is the role of that, in perspective? I will just ask for your comments.

Mr. ENGELBERG. [President Stamps.Com] Well, as a company, Stamps.Com does not have a formal position on export controls of encryption. We are working with international postal authorities to try and achieve a[n] international standard, along with the U.S. Postal Service, for the digital signature and two-dimensional barcode, so that this form of postage can be recognized worldwide. Right now, it is restricted for domestic use.⁴⁴⁶

In the text, Representative Shimkus believed that Congress had to address “the ease of export controls for encryption products” in order for the *E-SIGN Act* to have the desired international effects. The response of the industry witness, “Right now, it is restricted for domestic use,” corroborated Representative Shimkus’ concern that the *E-SIGN Act* was inconsistent with encryption export policy.

Since 1994, Congress has failed to reach agreement on a new export law, which shows both a lack of urgency and incrementalism in this area. For example, the whole text of Public Law 106-508, the *Export Administration Modification and Clarification Act of 2000*, contained the following:

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 20 of the Export Administration Act of 1979 (50 U.S.C. App. 2419) is amended by striking “August 20, 1994” and inserting “August 20, 2001”.*⁴⁴⁷

⁴⁴⁶ House Committee, Subcommittee on Telecommunications, Trade, and Consumer Protection, *The Electronic Signatures in Global and National Commerce Act*, 45.

⁴⁴⁷ *To provide for increased penalties for violations of the Export Administration Act of 1979, and for other purposes, U.S. Statutes at Large* 114 (2001): 2360.

The text shows that after years of technology advancements and changes in dual-use technology, Congress was only able to update the expiration date on an old export law. Congress' latest attempt was the *Export Administration Act of 2001*, S. 149. The Senate committee report on S. 149 suggested that committee members believed reactions of foreign nations would make United States export policy initiatives counter-productive, and this belief suppressed legislative initiative:

The Wassenaar Arrangement arguably is the least effective, largely because it does not contain a "no undercut" policy to prevent one regime member from exporting an item previously denied by another member to the same destination. In addition, non-regime members do not respect Wassenaar regime guidelines, further weakening its effectiveness. For example, China is making great inroads in the computer and semiconductor field, and India is producing high-quality encryption software; yet neither are members of the Wassenaar regime.⁴⁴⁸

The text mentions the recurring export problem of preventing "one regime member from exporting an item previously denied by another member to the same destination." In addition, the text specifically mentions the bigger issue of controlling non-regime members such as India, which was allegedly "producing high-quality encryption software." This perceived inability to affect the behaviors of international actors with respect to encryption policy also affected domestic policy.

The *USA PATRIOT Act* did not address encryption policy, although encryption control was a topic of several congressional debates after September 11, 2001. One reason could have been encryption policy fatigue caused by the failed *SAFE Act*,

⁴⁴⁸ Senate Committee on Banking, Housing and Urban Affairs, *Export Administration Act of 2001*, 107th Congress, 1st sess., 2 April 2001, Senate Report 107-10, 20.

PROTECT Act, and *Export Administration Act*. In a September 13, 2001 debate, Senator Bob Graham (D-Florida) used a *Washington Post* article on the NSA to suggest that indirect solutions to the encryption control problem were required:

Another challenge facing Hayden's NSA is to decode communications encrypted with powerful—and widely available—software. When Hayden became director, the deputy he inherited told Congress that the encryption software would make the job of decoding encrypted messages “difficult, if not impossible,” even with the world's largest collection of supercomputers. One alternative is to steal 1s and 0s before they are encrypted, or after they are decrypted. This requires classic [espionage]—as practiced by the Special Collection Service, the top-secret joint CIA–NSA operation. In the Code War, American spies recruited Soviet code clerks. Now the targets of choice—the people paid to sell out their governments or organizations—are systems administrators and other techies capable of providing encryption keys or planting electronic “trapdoors” in computer systems that can be accessed from computers on the other side of the world.⁴⁴⁹

This text, introduced into the *Congressional Record*, implied that a new approach to the encryption control problem would be to use “people paid to sell out their governments or organizations.” Thus, information access denied by unbreakable encryption had a non-technical solution. Senator Graham, as head of the Senate Select Committee on Intelligence, was able to talk around the espionage issue by using a *Washington Post* article to make his points. Actors in the Congressional Group realized that secretive and tacit decisions to use espionage to break encryption would have to be discussed by committee members in classified sessions.

⁴⁴⁹ *Congressional Record*, 107th Congress, 1st sess., 2001, 147, pt. 119: S9346-51.

Congress passed the 2002 *Cyber Security Research and Development Act* to focus federal money and effort on information security research. Actors from the Congressional Group were now focused on information security vulnerabilities after the terrorist attack:

We will not be able to address these vulnerabilities without conducting more research on cybersecurity. H.R. 3394 is designed to address four inadequacies with current research efforts:

- (1) The Federal Government has chronically underinvested in cybersecurity, an area in which the private sector has little incentive to invest.
- (2) This is true, in part, because no Federal agency has the responsibility of ensuring that the Nation has a robust cybersecurity research enterprise;
- (3) As a result, what little research has been done on cybersecurity has been incremental, leaving the basic approaches to cybersecurity unchanged for decades; and
- (4) As a field with relatively little money, few researchers and minimal attention, cybersecurity fails to attract the interest of students, perpetuating the problems in the field.⁴⁵⁰

In the text, the House committee believed that a law was required to conduct “more research on cybersecurity,” because there was no single government agency responsible for this area and because the “private sector” did not make the proper investments. Indirectly the committee was chastising NIST, NSA, and actors in the Encryption Technology Group for not producing technology solutions to solve the information control problem. More pointedly, the committee was taking some blame for the lack of policy direction, which resulted in research that was “incremental, leaving the basic approaches to cybersecurity unchanged for decades.” It had been almost three decades since the Data Encryption Standard was developed to solve the information security

⁴⁵⁰ House Committee on Science, *Cyber Security Research and Development Act*, 2.

problem. What was lacking was a technological approach to solve the information access problem in a manner that did not jeopardize information security. Thus, the passage of the *Cyber Security Research and Development Act* was a late start in the development of a technology solution that would support a balanced encryption policy.

In the Status Quo Period, actors in the Congressional Group exhibited behaviors that matched Allison's OBM general proposition of "Limited Flexibility and Incremental Change."⁴⁵¹ According to this proposition, once actors in this group found success in passing the 1998 *Digital Millennium Copyright Act*, subsequent laws would focus on extending the information security theme. The *E-SIGN Act* legalized the domestic and international use of digital signatures, most of which are based on public key encryption technology. Both these laws promised significant economic gains by advancing information security in the private sector. However, when alleged encryption use by terrorists threatened national security and public safety, Congress lacked the flexibility to address the information access problem in the *USA PATRIOT Act*. Instead of making a crisis decision that favored information access, Congress passed the *Cyber Security Research and Development Act* that studies solutions for the information control problem. I therefore assigned a Decision Timing valance of "1" to the Congressional Group for passing incremental laws that addressed the information security problem and tacitly avoided the information access problem.

⁴⁵¹ Allison and Zelikow, *Essence of Decision*, 180.

Encryption Technology Group

In the Status Quo Period, a majority of actors in the Encryption Technology Group had a common motivation for encryption liberalization. This group contained intellectual property vendors, information security and software vendors, established information technology associations, and a loose alliance of individuals and organizations that supported electronic privacy rights. During this period, the Internet-driven economic growth of the late 1990s reinforced a common notion among actors in this group that unimpeded private sector activities and market forces should determine information access and information security policies. The only valid reason for government action would be to foster technology neutral policies that advanced the efficiency of economic transactions. Encryption control to satisfy international relations, national security, and public safety requirements did not enter into the decision processes of these actors.

Despite the perturbations caused by the defeat of escrowed-key encryption, the ideological differences among actors in the Encryption Technology Group and actors in the Government Agencies Group dissipated quickly under a common goal of attaining the information technology leadership required for economic growth and market efficiency. The ubiquity of the Internet and e-commerce obscured the encryption control debate in the public sphere, and the debate moved to the technology world of communications, digital rights management (DRM), operating system protocols, public key infrastructure (PKI) management, and information assurance for the critical infrastructure. To users, the term information security took on a broad meaning to include secure “https://”

transactions, biometrics, virus scanning, spam and pop-up blockers, and regularized security patches. Normally, only technologists and activists debated issues on secret and public key encryption. Thus, the attack on September 11, 2001 did not produce a sudden public call to control encryption, but elevated requirements for even more information security tools. Actors in the Encryption Technology Group were ready to provide these tools. Company statements, congressional testimonies, court cases, engineering demonstrations, and *Federal Register* notices provided the data for analyzing the actions of the Encryption Technology Group. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

Actors in the Encryption Technology Group believed that the private sector, working towards an economic goal, was the lead actor in solving the related information and encryption control problems. Continuing into the Status Quo Period, this group believed that they had a decisive leadership role in the encryption policy debate. At the 1998 RSA Data Security Conference, a RSA press release described the actors in this debate:

The long-running battle in Washington over federal restrictions on the export of encryption technology and products promises to heat up in 1998, which various conference speakers called the most important legislative year yet for encryption technology. Congress is expected to be the battlefield as opponents of export controls, led by the computer and software industries and civil liberties groups,

continue the war against control supporters primarily federal law enforcement agencies and the Clinton Administration.⁴⁵²

Because of the perceived disagreement between the Clinton administration and Congress, the text indicates that 1998 was “the most important legislative year yet for encryption technology.” In addition, the text implies that the Encryption Technology Group had an initial leadership division between “computer and software industries and civil liberties groups” on the one side and unmentioned users, such as the digital content providers, on the other side. One reason for this omission can be traced back to the debate on using technology specific laws to advance the economic interests of a few technology users, such as the entertainment industry.

When it came to supporting a law to protect technology measures such as encryption from circumvention efforts, actors in this group were ambivalent about the value of government intervention. Conflicting testimony during congressional hearings on the *Digital Millennium Copyright Act* showed that intellectual property originators, such as the Recording Industry Association of America (RIAA) favored some government assistance in the form of targeted information security laws:

One, they make it absolutely clear that, consistent with current U.S. law, copyright holders are able to control the electronic delivery of their works to individual members of the public....

Three, the treaties require countries to prevent the circumvention of technical measures and interference with measures that copyright owners use

⁴⁵² RSA Security, “RSA Conference Ends With Push to Educate Business, Consumers and Policy Makers About Need for Data Security,” 20 January 1998 < http://www.rsasecurity.com/press_release.asp?doc_id=550&id=1034 >, accessed December 2004

themselves to protect themselves. These are key elements of a global Internet electronic commerce that has been a key focus of Members of Congress in this administration and U.S. competitiveness.⁴⁵³

In the text, RIAA believed that domestic copyright laws were adequate, but favored additional government help “to prevent the circumvention of technical measures” by other countries. In addition, the text suggests that the motivation behind RIAA’s effort was to gain an economic advantage through “global Internet electronic commerce.” Other actors in the Encryption Technology Group did not share this view.

Countering the testimony of the RIAA, Edward J. Black, the Computer and Communications Industry Association (CCIA) representative, believed that the private sector should be free to maintain the technology leadership of the United States:

We believe that any legislative changes to intellectual property law must vigilantly take into account the paramount interest of the intellectual property laws as provided for in the Constitution to promote the sciences and useful arts. The wisdom of this clause has been demonstrated over the years by providing the balanced underpinning of our nation's tremendous intellectual, technological and industrial growth.⁴⁵⁴

In the text, CCIA believed that the Constitution promoted intellectual property protection to advance “the sciences and useful arts” and not to guarantee technology-based monopolies. CCIA was worried that government intervention to protect intellectual property in the entertainment industry would hurt the larger information technology industry.

⁴⁵³ House Committee, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 201-202.

⁴⁵⁴ *Ibid.*, 257.

During the hearings on the proposed *SAFE Act* in 1999, Mr. Thomas Parenty representing the Business Software Alliance (BSA) submitted a prepared statement in favor of private sector leadership and against government controls on information security technology:

But we really are here today to speak on behalf of the tens of millions of users of American software and hardware products. The American software and hardware industries have succeeded because we have listened and responded to the needs of computer users worldwide. We develop and sell products that users want and for which they are willing to pay.

One of the most important features computer users are demanding is the ability to protect their electronic information and to interact securely worldwide. American companies have innovative products which can meet this demand and compete internationally. But there is one thing in our way—the continued application of overbroad, unilateral, export controls by the U.S. Government.⁴⁵⁵

The text indicates that BSA believed “American software and hardware industries” were responsive to “the needs of computer users worldwide.” In addition, the text shows BSA anticipated that users would need the “ability to protect their electronic information and to interact securely worldwide.” While American information technology industries could supposedly meet this need, BSA perceived that the United States government was the “one thing in [their] way.” Removing government technology leadership from the area of information security policy became a goal for the Encryption Technology Group after the failure of the *SAFE Act*.

The June 2000 passage of the *Electronic Signatures in Global and National Commerce Act* demonstrated that actors in the Encryption Technology Group were

⁴⁵⁵ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 73.

eventually successful in presenting a unified position on the value of private sector technology leadership. During the debates on the *E-SIGN Act*, Scott Cooper from Hewlett Packard cautioned a House committee on the perils of statutory technology direction that was occurring overseas:

The E-sign bill recognizes this need to harmonize international laws governing the use of electronic signatures so that electronic commerce can flourish globally. An important foundation to the creation of that seamless global marketplace must be the elimination of existing technology-specific national laws of electronic authentication and electronic signatures. Legal standing for electronic signatures should be performance based, i.e., that they are secure, easily available, and user friendly, not design based; that is, specifically mandated technologies. This reflects the need for technology neutrality in the development of a legal framework for electronic contracts.⁴⁵⁶

The text indicates that at least one information technology vendor believed that the “elimination of existing technology-specific national laws” was necessary to allow the private sector to develop “performance based” solutions. In the case of digital signatures, this idea of “technology neutrality” in laws would allow private sector versions of digital signature technology to compete against the government’s original Digital Signature Algorithm (DSA). As was noted in the Competitive Period, the government held the patent on DSA and tried to entice industry into compliance with the resulting Digital Signature Standard (DSS).

The inability of the government to market their DSS, despite its royalty free patent arrangements, showed that information security vendors were better able to develop and

⁴⁵⁶ House Committee on the Judiciary, Subcommittee on Courts and Intellectual Property, *Electronic Signatures in Global and National Commerce (E-SIGN) Act*, 30.

market information security products. Instead of relying on specific laws for assistance, these vendors successfully protected their economic positions through patents. One leading vendor, now renamed as RSA Security, held patents on both public key and secret key encryption subsystems. Two weeks before their critical public key encryption patent expired on September 20, 2000, RSA Security surrendered its main patent:

"So much misinformation has been spread recently regarding the expiration of the RSA algorithm patent that we wanted to create an opportunity to state the facts," said Art Coviello, chief executive officer of RSA Security. "RSA Security's commercialization of the RSA patent helped create an entire industry of highly secure, interoperable products that are the foundation of the worldwide online economy. Releasing the RSA algorithm into the public domain now is a symbolic next step in the evolution of this market, as we believe it will cement the position of RSA encryption as the standard in all categories of wired and wireless applications and devices. RSA Security intends to continue to offer the world's premier implementation of the RSA algorithm and all other relevant encryption technologies in our RSA BSAFE® software solutions and we remain confident in our leadership in the encryption market."⁴⁵⁷

In the text, RSA Security suggested that its stewardship of the RSA public key encryption patent enabled the "foundation of the worldwide online economy." With the statutory seventeen-year lifetime of the RSA patent expiring, RSA Security would have to compete with other encryption technology vendors that would be using this technology. Only the implementation details on the various public and secret key encryption subsystems would be protected by remaining patents held by information technology vendors. However, the text shows that RSA Security was confident in its "premier implementation of the RSA

⁴⁵⁷ RSA Security, "RSA Security Releases RSA Encryption Algorithm into Public Domain," 6 September 2000 < http://www.rsasecurity.com/press_release.asp?doc_id=261&id=1034 >, accessed December 2004.

algorithm” and in its “leadership in the encryption market.” This confidence in private sector technology leadership was high before the September 11, 2001 attack.

In the months before the attack, actors in the Encryption Technology Group told Congress that the private sector should develop information security solutions to protect the critical information infrastructure identified by President Clinton’s PDD/NSC-63. Mr. Harris Miller, representing the Information Technology Association of America (ITAA), testified before a Senate committee on the roles of industry and government:

MILLER: Now in many ways solutions to cyber security challenges are no different than any other Internet-related policy issue. Industry leadership, again, must be the hallmark, but government does have an important role. So let me review a few points that I believe government must focus on. First, I would like to reiterate the point Dr. Cerf made. The Congress must provide for what I call the Internet Hippocratic Oath. First, do no harm. Do not try to pass laws that seem to be ways of dealing with the challenge, but in fact miss the mark.⁴⁵⁸

In the text, ITAA explicitly claimed, “Industry leadership, again, must be the hallmark.” In addition, the text shows that Mr. Miller was critical of government leadership by admonishing the committee on past information security laws: “Do not try to pass laws that seem to be ways of dealing with the challenge, but in fact miss the mark.” This general attitude of the Encryption Technology Group softened, but did not change in the post-attack timeframe.

⁴⁵⁸ Senate Committee on Commerce, Science, and Transportation, Subcommittee on Science, Technology and Space, *Security Risks in Electronic Commerce*, 107th Congress, 1st sess., 16 July 2001. Available from Federal Document Clearing House, Inc., published by Lexis Nexis, < <http://web.lexis-nexis.com/congcomp/document> >, accessed December 2004.

During the October 2001 hearings on the *Cyber Security Research and Development Act*, Dr. Eugene Spafford representing the USACM reiterated concerns about government assistance in the information security area:

Experience has also shown that industry is concerned with information security certainly, and is willing to provide some funding for our research in this area. But it's usually tied to short-term deliverables and often has restrictions on publications of results, primarily because of information proprietary concerns. And as a result, our faculty have not been particularly interested in pursuing funding of that nature because it hinders their ability to progress in academia....

More recently, provisions of the Digital Millennium Copyright Act have led to faculty being threatened with lawsuits for publishing their security research. And some faculty, myself included, have had to stop our research in security forensics because of the potential for us to be arrested or sued because of our research.⁴⁵⁹

In the text, USACM believed that there were problems with industry funding for information security research and that there was a fear of government intervention through technology specific laws. In his example on *DMCA*, Dr. Spafford claimed that he had to stop his “research in security forensics” because of the fear of being “arrested or sued.” Thus, actors in the Encryption Technology Group appeared less worried about questionable government technology developments of the past and were now more worried about the unintended consequences of information security laws.

The perception of the private sector as the lead actor by the Encryption Technology Group matched Allison’s RAM organizing concept of a “Unified National Actor,” in

⁴⁵⁹ House Committee on Science, *Cyber Security: How Can We Protect American Computer Networks from Attack?*, 107th Congress, 1st sess., 10 October 2001. Available from Federal Document Clearing House, Inc., published by Lexis Nexis, < <http://web.lexis-nexis.com/congcomp/document> >, accessed December 2004.

which members of a group generally act as “unitary decision makers.”⁴⁶⁰ While some members in this group initially pushed for technology protection under *Digital Millennium Copyright Act*, others in this group consistently sought private sector leadership to solve the information security problem. The success of companies, such as RSA Security, over the federal government in patenting, developing, and marketing encryption technology reinforced the idea of private sector leadership. Even after the September 11, 2001 attack, actors in this group believed that the security of the critical information infrastructure depended upon tools researched and developed in the private sector. Actors in this group continued to show Congress that encryption export regulations and the technology specific legislation in *DMCA* were not market friendly and hampered United States efforts in the information security area. I assigned a Lead Actor valance of “0” to the Encryption Technology Group for acting as the leader in researching, developing, and marketing information security tools.

B. Problem Perception Valance

Well before the terrorist attack, actors in the Encryption Technology Group perceived that information security was a simple problem that could be solved by producing and using tools, such as encryption, to protect information. This group fought government attempts to ensure information access by challenging encryption export controls and specific information security solutions mandated by the government. The terrorist attack did serve to reinforce the importance of information security to this group

⁴⁶⁰ Allison and Zelikow, *Essence of Decision*, 24.

by highlighting the vulnerability of the critical information infrastructure in the United States to information warfare. However, during the Status Quo Period, actors in this group had to check government forays into encryption control. Continuing their efforts from the previous period, the Electronic Frontier Foundation (EFF) supported a position that information security was a simple problem and that bad government policy made the problem complex. In 1998, EFF built a Data Encryption Standard (DES) cracking machine to demonstrate that limiting exportable encryption strength to 56-bits threatened the information security of millions of DES users:

“Producing a workable policy for encryption has proven a very hard political challenge. We believe that it will only be possible to craft good policies if all the players are honest with one another and the public,” said John Gilmore, EFF co-founder and project leader. “When the government won't reveal relevant facts, the private sector must independently conduct the research and publish the results so that we can all see the social trade-offs involved in policy choices.”

The nonprofit foundation designed and built the EFF DES Cracker to counter the claim made by U.S. government officials that governments cannot decrypt information when protected by DES, or that it would take multimillion-dollar networks of computers months to decrypt one message. “The government has used that claim to justify policies of weak encryption and ‘key recovery,’ which erode privacy and security in the digital age,” said EFF Executive Director Barry Steinhardt. It is now time for an honest and fully informed debate, which we believe will lead to a reversal of these policies.⁴⁶¹

The text implies that the government would not “reveal relevant facts” on the security of DES encryption and shows that EFF believed it had to “independently conduct the research and publish the results” to produce these facts. More importantly, the text shows

⁴⁶¹ Electronic Frontier Foundation, “EFF DES Cracker” Machine Brings Honesty to Crypto Debate, 17 July 1998 <
http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html>, accessed December 2004.

EFF believed that government misstatements on DES were used to “justify policies of weak encryption and ‘key recovery,’ which erode privacy and security in the digital age.” By attempting to show that the government had reduced information security for many users in order to gain information access against suspected criminals, spies, and terrorists, EFF elevated the importance of the information security problem to Congress.

In addition to resisting information access requirements complicating the information security problem, actors in this group shunned the politicization of this problem. Proposed legislation to promote information security tended to have technology specifics that favored some industries and hurt others. During the House hearing on the *Digital Millennium Copyright Act*, Mr. Black representing the Computer and Communications Industry Association (CCIA) supported the intent of this bill, but not the technology specifics proposed by the Clinton administration:

If I do nothing else in this testimony today, I would like to make three points. First, we support passage of the WIPO implementing legislation in a comprehensive package that adequately addresses anti[-]circumvention and online service provider [(OSP)] liability.

Second, in order to implement the WIPO Treaty on the issue of anti[-]circumvention, the legislation should be amended to address actions and not devices, and to impose penalties for copyright infringement and not for non-infringing circumvention by itself. Unfortunately, the administration's bill, rather than implementing the WIPO Treaty, implements what the administration wanted the WIPO Treaty to be.

Third, legislation on OSP liability should be balanced to reflect the WIPO Treaty and should only impose liability on those in the private sector who have knowledge and control over the infringing material.⁴⁶²

The text shows that CCIA supported “WIPO implementing legislation,” but only legislation that would address “actions and not devices.” Specifically, CCIA believed that ensuring information security warranted “penalties for copyright infringement” and did not warrant a prohibition of circumvention activities. Some of these activities, such as fair use and reverse engineering, were legitimate under existing copyright laws. In addition, the text suggests that additional measures added to this bill were the result of trying to implement “what the administration wanted the WIPO Treaty to be.” As noted earlier, some intellectual property originators in the Encryption Technology Group supported these additional measures to help their industry.

Technology specific measures turned out to be problematic with the majority of the information technology industries. During the same hearing, Christopher Byrne representing the Information Technology Industry Council had a simpler view of the information security problem, whereby the private sector would focus on technical solutions and the government would “focus on conduct and behavior and not on technology.”⁴⁶³ Despite these recommendations, Congress passed the *DMCA* that included the problematic statutory protection against circumventing information security technology.

⁴⁶² House Committee, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 257.

⁴⁶³ *Ibid.*, 249.

A focusing theme to produce laws that controlled behaviors and not technologies permeated the hearings on the proposed *SAFE Act*. This bill was designed to limit government intervention with encryption technology policy and thereby simplify the information security problem. During a House hearing on the *SAFE Act*, Mr. Parenty representing the BSA used an example to show how a simple information security problem was made complex:

U.S. export controls still ignore the realities of mass-market software and hardware distribution. Mass-market hardware manufacturers and software publishers sell products through multiple distribution channels such as OEMs (*i.e.*, hardware manufacturers that pre-load software onto computers), value-added resellers, retail stores and the emerging channel of on-line distribution. Thus, mass market products are available to the general public from a variety of sources....

Uncontrollable products at 56-bits cannot suddenly become controllable products at 128-bits. The *SAFE Act* recognizes as a fundamental proposition that the United States should not try to control the export of something that is, by its very nature, uncontrollable. Trying to control the uncontrollable squanders the limited resources of companies trying to comply with unrealistic export controls as well as the resources of the government as it tries to enforce unenforceable export controls, undermining the credibility of the entire system of export controls.⁴⁶⁴

In the text, BSA claimed that the “realities of mass-market software and hardware distribution” meant that the spread of encryption was “by its very nature, uncontrollable.” Users would apply the best available encryption solutions to their information security problems. Thus, government actions to limit the exportable secret key encryption

⁴⁶⁴ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 80.

strength to 56 or 64-bits were in effect controlling technology availability and not the behaviors of hostile foreign actors.

The simple problem, as seen by BSA, was ensuring even information security on a global level. In his subsequent testimony, Mr. Parenty claimed, “[T]he protection of the infrastructures upon which our nation depends are not restricted to our nation’s borders.”⁴⁶⁵ His statement follows from the idea that interconnected systems require the application of simple and common information security measures to all the vulnerable points. Thus, Mr. Parenty believed that limiting the export of domestic encryption products to satisfy government information access requirements would complicate the global information security problem by favoring “foreign encryption over domestic-made.”⁴⁶⁶ The development and use of country specific encryption systems defeated the interoperability and common security protections required for good information security. Mr. Parenty also noted that the United States government was culpable in this matter “by requiring Americans to use key escrow, key recovery or recoverable encryption if they [wanted] to use an electronic signature.”⁴⁶⁷ Such country specific encryption schemes were unlikely to be used globally and would defeat interoperability requirements.

With parts of the *DMCA* and failure of the *SAFE Act* seen as setbacks, actors in the Encryption Technology Group continued to work against laws and regulations that compromised information security research, development, and publication. In the

⁴⁶⁵ *Ibid.*, 72.

⁴⁶⁶ *Ibid.*

⁴⁶⁷ *Ibid.*, 74.

culmination of a court case from the Competitive Period, EFF supported the legal efforts of Dr. Bernstein to publish and thereby export encryption software. The May 1999 decision by the United States Court of Appeals, Ninth Circuit, in favor of Dr. Bernstein caused a subsequent news release by EFF:

The case has been sponsored by EFF since 1995. "We sponsored Professor Dan Bernstein's case because of its importance to society, free expression, electronic commerce, and privacy in the digital world," said Tara Lemmey, EFF's President and Executive Director....

"The US government has wielded these export controls to deliberately eliminate privacy for ordinary people," said John Gilmore, co-founder of EFF. "The controls created wireless phones that scanners can hear, e-mail that's easy to intercept, and unsecured national infrastructures that leave us all vulnerable. Misguided national security bureaucracies use these controls everyday, to damage the nation they are sworn to protect, and to undermine the constitution they are sworn to uphold. Today's ruling is a giant step toward a sane policy."⁴⁶⁸

The text shows that EFF believed in the freedom to use encryption, which was important "to society, free expression, electronic commerce, and privacy." The complicating issue of satisfying information access requirements did not appear important to the EFF. In addition, the text implies that EFF believed the problem of "unsecured national infrastructures" was caused by "[m]isguided national security bureaucracies." This pre-attack belief by actors in the Encryption Technology Group on the importance of information security became coupled to a belief that government should control behaviors and not technology.

⁴⁶⁸ Electronic Frontier Foundation, US Export Control Laws on Encryption Ruled Unconstitutional, 7 May 1999 < http://www.eff.org/Privacy/Crypto_export/Bernstein_case/19990507_eff_pressrel.html >, accessed December 2004.

Success by actors in the Encryption Technology Group to keep the *E-SIGN Act* free of technology directives signaled a triumph of simplicity over complex information access and security schemes. During a House hearing on this bill, Mr. Thomas C. Quick of Quick & Riley / Fleet Securities explained the monopoly problem created by technical direction from the government:

Mr. QUICK. I believe that what this does is it prevents a monopoly because this is not dictating what you do, you know, how you are going to do it. It actually, I think promotes the spirit of entrepreneurship that you are able to come up—and some people can do it in house. My colleague here at the table, their firm is one of the best in the country for development of technology so Schwab might do it in house as opposed to our firm which has a tendency to want to—we say we are not in the technology business so we employ outside firms to come in and offer a solution to us. So I think this really truly does not give one particular company a monopoly on the whole process.⁴⁶⁹

The text indicates that users relying on information security solutions preferred “the spirit of entrepreneurship” instead of government direction. In addition, the text indicates that choices in the private sector allowed an “in house” solution and allowed “outside firms to come in and offer a solution.” Without the government directing information technology development, some actors in the Encryption Technology Group feared a drop in investments on the research and development of information security technologies.

The attack on September 11, 2001 did not produce Draconian information access laws, but did show the requirement for an information security program founded on a continuous research and development effort from the private sector. Actors in the

⁴⁶⁹ House Committee, *The Electronic Signatures in Global and National Commerce Act*, Serial No. 106-33, 35.

Encryption Technology Group were able to get government funding for part of this research and development effort. While government research funding may have targeted selected organizations and industries with political agendas, RSA Security gave Representative Boehlert an award for the *Cyber Security Research and Development Act*, which provided for government funding of private sector information security research and development:

Legislation introduced by Science Committee Chairman Sherwood Boehlert (R-New Hartford, New York) aimed at improving the nation's cyber security received final approval by Congress. "The Cybersecurity Research and Development Act" has been sent to the President, who is expected to sign it this year. This legislation strengthens efforts to attract top science and engineering talent to the Mohawk Valley in the field of cybersecurity and provide a powerful source of new ideas and innovation for the New York high-tech industry. The legislation would additionally expand federal funding for cybersecurity research and education.⁴⁷⁰

The text shows that RSA Security believed cyber-security legislation could improve the information security effort by funding "top science and engineering talent ... in the field of cybersecurity." Legislation that would help fund solutions to the information security problem appeared acceptable to RSA Security because the law focused on research and development behaviors and not on technical direction. Part of the *Cyber Security Research and Development Act* did allow for information access research on the "enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve piracy of intellectual property."⁴⁷¹ Actors in the

⁴⁷⁰ RSA Security, "RSA Conference Announces Sixth Annual Award Recipients," 14 April 2003 <http://www.rsasecurity.com/press_release.asp?doc_id=2445&id=1034>, accessed January 2005.

⁴⁷¹ *Cyber Security Research and Development Act*, *U.S. Statutes at Large* 116 (2002): 2368.

Encryption Technology Group found this language acceptable, as there were no political hot words such as key recovery or escrowed-key encryption mentioned in the legislation.

The perception of a simple problem by the Encryption Technology Group matched Allison's RAM organizing concept of "The Problem," whereby this group gained ownership of the information security problem by its common "response to the strategic situation."⁴⁷² Individuals, organizations, and corporations took actions to keep the information control problem simple by challenging government actions that added technical specificity and thus, complexity to this problem. Actors in the Encryption Technology Group challenged government suppositions on technical parameters for exportable encryption. EFF's DES cracker success showed that the security of 56-bit encryption was suspect and that government information access requirements may have limited development of stronger encryption systems. However, some actors in the Encryption Technology Group still trusted the government on specific technology issues, such as protecting intellectual property. The debate on the *Digital Millennium Copyright Act* divided this group on whether the government should prohibit circumvention technology or should prohibit behaviors such as information theft and espionage. The entertainment industry was in favor of technology control and the information technology industry worried that *DMCA* would inhibit research and development required for new information security tools.

⁴⁷² Allison and Zelikow, *Essence of Decision*, 24.

Believing in technological determinism, actors in the Encryption Technology Group supported court cases where individuals challenged government restrictions on the release of information on encryption technology designs and tools. As demonstrated by the 1999 Bernstein opinion from the Ninth Circuit, the statutory control of intangible technology, such as encryption software, violated the First Amendment. Actors in this group supported a minimalist approach to government control of behavior and not technology in the *E-SIGN Act*. With actors already focused on the information security problem, the September 11, 2001 attack served to boost research and development efforts as a better way to protect national security and public safety. I assigned a Problem Perception valance of “0” to the Encryption Technology Group for perceiving a simple information security problem that was not complicated by government technical direction or solving the information access problem.

C. Favored Alternative Valance

Actors in the Encryption Technology Group favored the development of utility maximizing alternatives from which users could choose. In support of market choice, these actors challenged laws and regulations that they viewed as market distorting. One way in which they challenged proposed laws and regulations was to expose the irrational information access and security logic used by the government. During the House hearing on the *Digital Millennium Copyright Act*, Mr. Black of the Computer and Communications Industry Association (CCIA) found that the government’s information security solution was not utility maximizing for private sector users:

There is a connection between copyright and encryption that needs to be mentioned because the Administration is more than just a little inconsistent in its treatment of encryption. Is encryption a good or bad thing? Is decryption good or bad? On the one hand, the Administration's encryption policy regards encryption as sufficiently dangerous to restrict its export. The FBI regards encryption as sufficiently dangerous to restrict its manufacture and use in the U.S., and too dangerous to import. Yet, in the copyright arena, the Administration treats encryption as a good thing, and seeks to impose criminal penalties for breaking through such encryption. On the one hand, the Administration's encryption policy treats encryption as a very powerful tool that is difficult to break. It requires the use of decrypting keys so that law enforcement can gain access to the plain text. Yet, in the copyright context, the Administration treats encryption as so weak that it imposes criminal penalties for those who circumvent it.⁴⁷³

The text demonstrates that the government and private sectors had opposing perceptions on the costs and benefits of using encryption to guarantee information access and security. As noted earlier, the government considered encrypted information as being “difficult to break” and favored weaker encryption technology solutions that allowed information access. When the private sector used “weak” solutions to protect information, the government had to help with information security by imposing “criminal penalties” on users circumventing weak protective measures. Thus, most actors in the Encryption Technology Group perceived that government developed or specified information security solutions did not provide the optimum security and thus, these solutions were not utility maximizing. One method to limit government influence was to develop and offer more choices for information access and security solutions. Another method to limit government influence was to remove technical specificity from proposed laws and regulations.

⁴⁷³ House Committee, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 261.

Actors in the Encryption Technology Group supported the proposed *SAFE Act* because this bill would have restricted government interference with user decisions on satisfying information access and security requirements. During the House hearing on this bill, Mr. Alan Davidson from the Center for Democracy and Technology (CDT) testified on the linkages among information security, privacy, and the requirement to use encryption:

Encryption gives people an easy and inexpensive way to protect that information. The need for encryption is becoming ever more acute as sensitive data is finding its way into electronic form:

- Individuals need encryption in order to trust the Internet with private data such as online banking, stock trades, medical records, electronic purchases, or personal communications.
- Businesses need encryption to protect their own proprietary information as it flows across vulnerable global networks.
- The country needs encryption to secure the critical information infrastructure governing such sensitive applications as our utilities, financial markets, or air traffic control networks.

If broad participation in electronic commerce and the information society is to become a reality, the adoption of encryption in most phases of electronic existence will be required.⁴⁷⁴

The text indicates that CDT believed users required encryption freedom “in order to trust the Internet with private data such as online banking, stock trades, medical records, electronic purchases, or personal communications.” The idea that users valued encryption freedom was not limited to users in the private sector. CDT believed that “the adoption of encryption in most phases of electronic existence” was a requirement. This was not a prophetic claim by CDT. Nine months earlier, the Social Security

⁴⁷⁴ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 99.

Administration decided that its millions of customers would use RSA Security encryption products and not the government specified Digital Signature Standard to provide information security and digital signatures for individual accounts.⁴⁷⁵ Because the *SAFE Act* failed, subsequent legislations had to be individually scrutinized to remove technology specificity and to allow user choice.

Actors in the Encryption Technology Group worked to ensure that the *E-SIGN Act* would allow users to choose their own information security solutions. During a 1999 House hearing on this legislation, Mr. W. Hardy Callcott, representing the brokerage firm of Charles Schwab, answered a question on the rationale of producing technology neutral legislation:

Mr. CALLCOTT. There is very exciting technologies that are emerging right now which would allow a computer basically to be locked unless somebody has a thumb print scan that unlocks it specifically for them. Those are the types of new technology that we would like to see legislation like this recognize. The European Union and some of the States have honed in on what is called public key, private key encryption technology, which is good technology but we don't think it is the only technology out there and one of the reasons we support this legislation is because it will allow the growth of new and very interesting and important technologies to protect consumer security.⁴⁷⁶

The text indicates that Charles Schwab, a user and developer of electronic signature technology, believed that legislation should allow other "types of new technology."

⁴⁷⁵ U.S. Social Security Administration, "The Chief Information Officer of the Social Security Administration Grants to the Social Security Administration a Waiver From the Use of Certain Federal Information Processing Standards," *Federal Register* 63, no. 108 (5 June 1998): 30794-5.

⁴⁷⁶ House Committee on Commerce, Subcommittee on Finance and Hazardous Materials, *The Electronic Signatures in Global and National Commerce Act*, 106th Congress, 1st sess., 24 June 1999, Serial No. 106-33, 34.

While Mr. Callcott's answer indicated that public key encryption was one available technology, he subsequent revealed that users would benefit from "the growth of new and very interesting and important technologies to protect consumer security." Thus, the search for utility maximizing choices to solve the information control problem went beyond encryption solutions and ultimately led to a search for supportive technologies. With the passage of the technology neutral *E-SIGN Act* in 2000, encryption vendors were able to competitively incorporate other identification technologies such as biometrics.

Actors in the Encryption Technology Group were willing to offer free propriety encryption solutions in order to capture the benefits of network effects. When NIST decided to have a full and open competition for the Advanced Encryption Standard, RSA Security submitted its patented RC5 secret key encryption subsystem as a candidate. Examining the RC5 patent shows that the algorithm could be tailored to meet the security requirements of different users:

It is another objective of the inventive cipher to have a variable-length cryptographic key. Since the cipher is symmetric, the same secret cryptographic key is used for both encryption and for decryption. By properly selecting the length of the key, the cipher can be tailored to provide the desired level of security that is appropriate for a particular application or other requirement. The key length "b" (in bytes) is the third selectable parameter of the cipher. By selecting a relatively-long key length "b", the resulting cipher application will have a relatively-high degree of security against an exhaustive search of each possible key. Similarly, a short key length is believed to provide a lesser degree of security.⁴⁷⁷

⁴⁷⁷ Ronald L. Rivest, "Block encryption algorithm with data-dependent rotations," U.S. Patent # 5,724,428, 3 March 1998.

The text indicates that this “inventive cipher” was developed to “provide the desired level of security.” Users could choose a higher level of information security by using “a relatively-long key length.” This increase in utility came at the expense of slower key generation speed and some reduction in encryption speed, both of which users would have to accept.

The idea of flexible encryption was tested in the AES competition by the submission of an improved RC5 algorithm called RC6. In 2000, RC6 lost to the winning Rijndael algorithm in large part because of slower key generation and higher resource loading characteristics of RC6.⁴⁷⁸ If RC6 had won the competition to become the Advanced Encryption Standard, then RSA Security would have had a technology monopoly on a complete encryption system, as it still had the technology lead with patented implementations of the RSA public key encryption subsystem.

Other actors in the Encryption Technology Group believed that an encryption technology monopoly could threaten the commercial viability of utility maximizing solutions. This concern was warranted as RSA Security maintained its general public key encryption patent until two weeks before patent expiration on September 21, 2000. These concerned actors were able to create competitive solutions using Diffie-Hellman and elliptic curve public key encryption technologies. Elliptic curve technology was a notable development in that this cryptosystem was not patented, unlike Diffie-Hellman

⁴⁷⁸ James Nechvatal, et al., *Report on the Development of the Advanced Encryption Standard* 2 October 2000 (Washington, D.C.: NIST, 2000), 91-92.

and RSA that were owned by Stanford University and RSA Security, respectively.⁴⁷⁹

Thus, actors in the Encryption Technology Group were relatively free to develop and patent their own implementations of elliptic curve public key encryption subsystems.

One such actor was SafeNet, which claimed to own a patent on an elliptic curve implementation that was better than RSA public key encryption implementation in several aspects:

One algorithm which has been used to encrypt unlocking codes is the well-known RSA algorithm. However, a problem arises when RSA is used for this purpose. In order to obtain a reasonable level of security, the output messages from RSA are quite long. For example, a typical message using RSA and providing a minimum acceptable level of security may be 45 digits in length. This is too long for use where users are obtaining keys over the telephone: they must record and enter messages of 45 digits in length with no errors. This is beyond the acceptable level of ease of use of most users. What is needed is an encryption method which provides an acceptable level of security, while at the same time allows the use of shorter messages.⁴⁸⁰

The text shows that the objective of competition was to produce a more suitable product, because RSA keys might have taken “too long for use where users are obtaining keys over the telephone.” In addition, one competitor claimed to have found an elliptic curve solution that would provide an “acceptable level of security” and would permit the use of “shorter messages” to pass encryption keys. Thus, the competitive environment among encryption technology vendors appeared sufficient to supply utility maximizing solutions to the market without government intervention.

⁴⁷⁹ RSA Security, “6.3.4 Are elliptic curve cryptosystems patented?,” Copyright 2004 < <http://www.rsasecurity.com/rsalabs/node.asp?id=2325> >, accessed January 2005.

⁴⁸⁰ Laszlo Elteto, et al., “Method and system for secure distribution of protected data using elliptic curve systems,” U.S. Patent # 5,737,424, 7 April 1988.

While the September 11, 2001 attack highlighted the requirement to protect the information infrastructure, the attack also increased the utility of electronic-business and electronic-government. Actors in the Encryption Technology Group, such as SafeNet, anticipated this change:

As we enter the New Year, government and business leaders must come to terms with the implications of the cataclysmic events of 2001. People are worried by the terrorist threats directed at air travel and paper-based mail leading to a definite movement for less face-to face meetings and less reliance on traditional mail. Insurance premiums are rising steeply, thereby forcing organizations to consider distributed operations. The outcome is a change in the way we conduct business and far greater use and dependence on electronic communications and networks.⁴⁸¹

The text shows that SafeNet anticipated a reduction in physical travel and transaction activities and a “far greater use and dependence on electronic communications and networks.” Heightened physical security risks and greater use of non-physical interactions would greatly increase the value of information security solutions.

As encryption technology vendors produced solutions to the information security problem, the more valuable solutions began to satisfy information access requirements. Instead of detracting from the perceived value of the solution, satisfying information access requirements suddenly appeared to be part of a balanced utility maximizing solution. Encryption technology vendor Entrust openly advertised their balanced solution that effectively had an encryption key recovery feature:

⁴⁸¹ SafeNet, The New Business Environment, August 2003 < http://www.safenet-inc.com/library/8/New_Business_Environment_WhitePaper.pdf >, accessed January 2005.

Entrust Authority™ Security Manager, the world's-leading public-key infrastructure (PKI), is designed to manage the digital keys and certificates that make up the digital identities required to transparently automate all security-related processes in an organization....

Entrust Authority Security Manager represents the centerpiece of the Entrust Authority products portfolio, built specifically to:

- securely store the certificate authority (CA) private key
- issue certificates for users and devices
- publish user and application certificate revocation lists (CRLs) to allow verifiable communications
- maintain an auditable database of users' private key histories for recovery purposes in the event that users lose access to their keys⁴⁸²

In the text, Entrust claimed to have produced the “world's-leading public-key infrastructure” management software, which performed the encryption key generation, distribution, and storage functions required of a “certificate authority.” The implied user trust placed in a certificate authority went so far as to include maintaining “private key histories for recovery purposes.” While actors in the Encryption Technology Group fought government attempts to mandate key recovery schemes, these same actors showed little hesitation in producing such solutions to satisfy user demand. From an economic perspective, encryption solutions had increased utility when they had provisions to cover human failings, such as forgetting one’s password. Without key recovery, encrypted information would be put at risk by the same technology used to secure the data.

By implementing key recovery solutions, actors in the Encryption Technology Group opened the possibility that the government could get access to encrypted

⁴⁸² Entrust, Entrust Authority Signature Manager, 2005 Copyright < <http://www.entrust.com/authority/manager/index.htm> >, accessed January 2005.

information. The implications of allowing or even charging the government for court-ordered access to private information have not been openly discussed by actors in this group. One company, VeriSign, specifically mentions to users the possibility of allowing government access to protected information:

Key Management Customers should be aware that law enforcement officials, litigants in civil cases, and others may seek information from VeriSign in an effort to obtain key recovery information by way of a search warrant, subpoena, request for production of tangible things, or other similar procedure. Although the VeriSign Key Recovery Service is never in possession of any subscriber's private key, VeriSign shall be entitled to comply appropriately with requests or demands for key recovery information pursuant to such judicial or administrative processes.⁴⁸³

The text indicates that although “VeriSign Key Recovery Service is never in possession of any subscriber's private key, VeriSign shall be entitled to comply appropriately with requests or demands for key recovery.” It is doubtful that the average encryption user reads the “fine print” on key recovery services, but such services are avenues for the government to use the *Communications Assistance for Law Enforcement Act* to gain access to encrypted information in the private sector.

The favoring of utility maximizing solutions over government solutions by actors in the Encryption Technology Group matched Allison’s RAM general proposition that increasing the utility value of a solution “increases the likelihood of that action being chosen.”⁴⁸⁴ Most of the actors in this group perceived that government technology

⁴⁸³ VeriSign, “Key Management,” 29 April 1999, <<http://www.verisign.com/repository/updates/entry1.2-05.html>>, accessed May 2005.

⁴⁸⁴ Allison and Zelikow, *Essence of Decision*, 25.

specification and protection, such as that mandated by the *Digital Millennium Copyright Act*, would hinder development of market-based information security systems. These actors were successful in freeing the *E-SIGN Act* of technology specificity, and thus, allowed users and the market to decide upon the better electronic signature technology. Encryption vendors soon had competitive technologies for secret key and public key encryption subsystems and produced software to manage complete encryption systems through certificate authorities. The trusted information security choices provided by the actors in the Encryption Technology Group allowed for a rational response before and after the September 11, 2001 attack. Users in the government and private sectors found market-based solutions available to protect the critical information infrastructure of the United States. With a choice of solutions, users in both sectors could also satisfy their perceived requirements for information access to include the ability to recover lost encryption keys, protect national security, and ensure public safety. I assigned a Favored Alternative valance of “0” to the Encryption Technology Group for resisting government solutions and for generating utility maximizing solutions to solve the information access and security problem.

D. Decision Timing Valance

During the Status Quo Period, actors in the Encryption Technology Group used encryption technology solutions when they became available and when global events and user demand supported a market for these solutions. With the Data Encryption Standard (DES) proven to be obsolete through cracking competitions, encryption technology

vendors were busy developing replacements for DES. A replacement was overdue, as presidential directives and laws continued to set policies for increased information security during this period. Figure 4-7 shows the timings of these policies. Just before President Clinton issued PDD/NSC-63 on critical infrastructure protection, the USPTO issued a patent to RSA Security for its RC5 secret key encryption algorithm, which had extensible key lengths and variable algorithm parameters. By being flexible, RSA Security could tailor its product to match or beat DES-level security:

As an example, one might reasonably choose a cipher algorithm in accordance with the current invention that is designated as “RC5-32/16/7” as a replacement the conventional block-cipher Data Encryption Standard (DES). The input/output blocks of the cipher algorithm are $2w=64$ bits long, as in DES. The number of rounds is also the same as in DES, although each of the “RC5-32/16/7” round is more like two DES rounds since all data registers are updated in one round, rather than just updating half of the registers as is done in DES. Finally, DES and the “RC5-32/16/7” algorithm each have 56-bit (7-byte) secret keys. Unlike DES, which has no parameterization and hence no flexibility, a cipher in accordance with the present invention may be upgraded as necessary by changing the variable parameters. The above exemplary cipher that is to be a DES replacement may be adjusted to an 80 bit key by moving to “RC5-32/16/10”.⁴⁸⁵

The text indicates that the inventors of RC5 targeted the lack of “parameterization” and hence the “flexibility” of DES. In addition, the text shows that DES-like capability could be reproduced by setting the parameters to “RC5-32/16/7.” The key length extensibility of the setting “RC5-32/16/10” produced a 10-byte or 80-bit key, which was the equivalent of NSA’s SKIPJACK algorithm. The choice of these parameters was not

⁴⁸⁵ Ronald L. Rivest, “Block encryption algorithm with data-dependent rotations,” U.S. Patent # 5,724,428, 3 March 1998.

coincidental and came at a time when the government's Escrowed Encryption Standard (EES) was supposed to be the dominant information access and security solution.

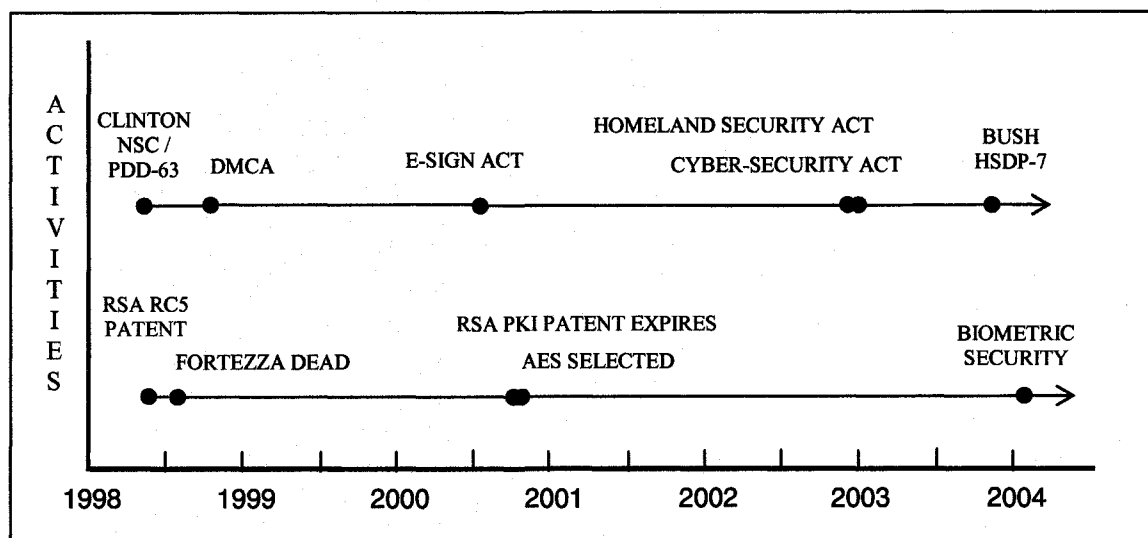


Figure 4-7 Timeline of policies and Encryption Technology Group activities

The failure of EES in the market opened the way for private sector developments of more trustworthy and secure solutions that could satisfy growing information security requirements. A June 1998 government press release showed that NSA would not use its EES compliant FORTEZZA algorithms as “candidates for the Advanced Encryption Standard (AES) competition” because the underlying 80-bit SKIPJACK algorithm was “not extensible to higher key lengths.”⁴⁸⁶ Figure 4-7 shows this event and the completion of the AES competition in October 2000. This competition involved the consideration of

⁴⁸⁶ U.S. Department of Defense, National Security Agency, “Press Release: NSA Releases FORTEZZA Algorithms,” (Washington D.C., 24 June 1998).

private sector candidates from the United States and several foreign countries. The eventual winner was the Belgian Rijndael encryption algorithm, which has extensible encryption key lengths from 128 to 256 bits.⁴⁸⁷ Encryption vendors designing information security solutions with the minimum AES key length could offer superior products when compared to products based on 56-bit DES and the interim 112-bit Triple DES algorithms.

While the ongoing AES competition was a significant technology high point for replacing DES, the 1998 passage of the *Digital Millennium Copyright Act* was a disappointment for the developers of information security choices. As noted earlier, the controversial part of *DMCA* was the legal protection provided to technically weak information security solutions. This perceived protection relieved content providers from the market pressure to produce information security solutions that would be adequate for the value of the intellectual property being protected. In their testimony to the U.S. Copyright Office, the Electronic Frontier Foundation (EFF) identified an effect this law had on developing information access and security solutions:

Contrary to the fears expressed by the publishing industry, it is possible to preserve Constitutional values without destroying the value behind creative expression. In its justification for greater control over creative expression, the industry claims the new found phenomena of digital technology leaves copyright holders at the mercy of massive unchecked piracy. While the industry has loudly over-stated any potential harm it might face resulting from digital technology, it quietly looks the other way without mentioning the unprecedented power

⁴⁸⁷ James Nechvatal, et al., *Report on the Development of the Advanced Encryption Standard* 2 October 2000 (Washington, D.C.: NIST, 2000), 7.

technology provides to copyright holders to control access and use over creative expression.⁴⁸⁸

The text shows that EFF believed that it was “possible to preserve Constitutional values without destroying the value behind creative expression.” In addition, the text implies that a technical solution could have been developed, but the “copyright holders” were not using “the unprecedented power” of technology in their solutions. Figure 4-7 shows that there was sufficient time between *DMCA* and the *E-SIGN Act* for actors in the Encryption Technology Group to realize the suppressive effect that technology specific laws had on the development of information security solutions.

Several months after the passage of the *E-SIGN Act*, the patent on the dominant RSA public key encryption subsystem expired. This expiration allowed other encryption technology vendors to develop their own implementations of the RSA algorithm, which was a concern to actors outside of the Encryption Technology Group. Without government direction, these outside actors feared that competition would cause a compatibility divergence between information security solutions. However, users demanded interoperable products especially when the underlying technology and algorithms were common. A RSA Security press release alleviated the need for government direction:

BEDFORD, MA., Wednesday, January 17, 2001 — RSA Security Inc. (NASDAQ: RSAS), the most trusted name in e-security, and Entrust

⁴⁸⁸ Robin D. Gross, Testimony of Electronic Frontier Foundation (EFF) before Copyright Office Public Hearings on Digital Millennium [Millennium] Copyright Act (DMCA), 19 May 2000 <http://www.copyright.gov/1201/hearings/robin_gross.pdf>, accessed January 2005.

Technologies Inc. (NASDAQ: ENTU), the global leader in solutions that bring trust to e-business, today announced their intent to further improve interoperability between their respective e-security solutions. Under the terms of a collaboration agreement, the two companies will work together to engineer, test and certify interoperability between Entrust/PKI™ software and RSA Keon® Advanced PKI software, RSA BSAFE® software and RSA SecurID® authentication technology....

“Interoperability is critical for the success of today's e-security enterprises,” said Scott Schnell, senior vice president of marketing at RSA Security. “Our relationship with Entrust Technologies is another proof point of our commitment to deliver on the value of interoperability to our customers and move the market forward by simplifying life for customers.”⁴⁸⁹

The text suggests that RSA Security and one of its leading competitors, Entrust, were motivated to work together under “a collaboration agreement” that would “improve interoperability between their respective e-security solutions.” Both companies believed that their cooperative solutions had the “value of interoperability” which would positively influence consumer choice. The cooperation required to generate the network effects of interoperable security solutions did not involve government direction.

Before the September 11, 2001 terrorist attack and without government intervention, actors in the Encryption Technology Group realized that it was an opportune time to provide users with an ability to satisfy information access requirements. By late 2000, users saw value in ensuring information access when encryption keys were lost or when information assurance activities required access to

⁴⁸⁹ RSA Security, “RSA Security and Entrust Technologies Commit to Work Towards Interoperability Among Their Market Leading e-Security Technologies,” 17 January 2001, <http://www.rsasecurity.com/press_release.asp?doc_id=100&id=1034>, accessed January 2005.

protected information. Information access requirements soon became important enough to warrant a metric in the analysis of business software solutions:

Based on a request for public-key infrastructure proposals from The Prudential Insurance Co. of America, eWeek Labs came up with a plan to test the implementation and management of a complete PKI installation.

The criteria used to assess products in this eValuation included the ability to set up a CA (certificate authority) and RA (registration authority), bulk key and certification generation, certificate revocation, key escrow and recovery, certificate renewal, and directory support and integration.⁴⁹⁰

The text shows that Prudential Insurance asked the *eWeek* laboratory staff to “test the implementation and management of a complete PKI installation.” One of the criteria was “the ability to set up ... key escrow and recovery.” In contrast to the perceived invasion of privacy caused by the development of the government Escrowed Encryption Standard, private sector security solutions were now perceived to be more valuable if they performed the equivalents of key escrow and recovery functions. The perplexing notion that users would wait for a private sector solution instead of using a government solution that was available seven years earlier suggests that encryption choice may increase the trust and value of a solution.

The terrorist attack on the United States generated the impetus behind the *Homeland Security Act*, the *Cyber Security Research and Development Act*, and HSPD-7 on critical infrastructure protection. The attack also motivated actors in the Encryption

⁴⁹⁰ Cameron Sturdevant, “PKI Tells 'Who Goes There?,'” *eWeek*, 11 December 2000, <<http://www.eweek.com/article2/0,1759,1282,00.asp>>, accessed January 2005.

Technology Group to develop encryption solutions in areas where there was distrust of government-developed solutions and where the government had previously specified technology solutions. One such area was the natural coupling of encryption and biometric technologies to produce competitive user identification and authentication systems. At the February 2004 RSA Convention, Memory Experts released a portable and secure computer hard drive for the transport and storage of sensitive information:

A biometric hard drive capable of delivering the storage power of a PC in a pocket-sized data device will launch at the RSA Conference in San Francisco.

Based on 128-bit AES (Advanced Encryption Standard) encryption, the Outbacker hard drive from Memory Experts activates only after a fingerprint is authenticated, said Mike Kieran, director of sales and marketing. Access to the hard drive is restricted to users whose fingerprints are registered in the hard drive....

An administrator can erase or add fingerprints to the device, said Kieran, who recommended that each user register at least two fingerprints. "If you scratch your finger while working in a garden, there will be no way to get in." ⁴⁹¹

The text demonstrates that Memory Experts developed a way to ensure information access and security by using "128-bit AES (Advanced Encryption Standard) encryption" in concert with fingerprints. The use of AES allowed users to protect their information and to prevent unauthorized access. In addition, the text shows that Memory Experts was concerned about satisfying information access requirements by recommending that administrators entice users to "register at least two fingerprints." This implies that a

⁴⁹¹ Agam Shah, "Memory Experts releases biometric hard drive," Computer Weekly, 24 February 2004, < <http://www.computerweekly.com/Article128629.htm> >, accessed January 2005.

trusted administrator could have access to protected information by allowing others to register their fingerprints in the access database. In effect, administrators would act as key escrow agents, but this role appeared acceptable to the attendees at the RSA Convention.

The decision timing exhibited by actors in the Encryption Technology Group matched Allison's RAM general proposition that the "likelihood of any particular action" is dependent upon the availability of "alternative courses of action."⁴⁹² Actors in this group realized that the cost of accepting the first available course of action often exceeded the cost of waiting for a better alternative, usually from the private sector. During the Status Quo Period, information security policies found in laws and directives evolved from being technology specific, as in the case of the *Digital Millennium Copyright Act*, to being more open to various alternatives, as in the case of the *E-SIGN Act*. Following this evolution, actors in this group coupled the development of the AES secret key encryption subsystem and the expiration of a critical public key encryption subsystem patent to produce competitive and interoperable encryption systems.

The September 11, 2001 attack increased requirements for information security solutions at the expense of information access considerations. Yet, by waiting for better private sector solutions, users found that solutions satisfying information access requirements were more valuable than solutions that only maximized information security. Waiting for choices generated user trust in key recoverable encryption systems,

⁴⁹² Allison and Zelikow, *Essence of Decision*, 25.

while earlier government direction to use similar systems caused widespread dissention. I assigned a Decision Timing valance of "0" to the Encryption Technology Group for resisting government directed alternatives and waiting for the convergence of secret key and public key encryption solutions to solve the information security and access problem.

Executive Group

In the Status Quo Period, the primary actors in the Executive Group affecting information control policies were two presidents, their National Security Councils, their federal department leaders, and their Offices of Management and Budget. The contrasting administrations of Presidents Clinton and G. W. Bush made little difference to their eventual and common views on information control policies. During the Clinton administration, the collapse of the escrowed-key encryption solution to solve the information access problem represented a turning point for domestic encryption policy. Attorney General Reno was an adamant supporter of information access requirements that satisfied her public safety goals, and her department regularly testified before Congress on this issue. Attorney General Ashcroft was silent on this issue, but as a senator, he supported information security requirements and encryption liberalization goals. Both administrations exercised de facto regulatory control of encryption exports that satisfied international agreements, as Congress was nearing its twentieth year of debate on export policy. The September 11, 2001 terrorist attack did not precipitate a crisis in information control policymaking and reaffirmed the Bush administration's policy focus on information security. Executive orders, directives, international

arrangements, and congressional testimony from leaders in the executive branch provided the data for analyzing the actions of the Executive Group. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

The successive administrations of Presidents Clinton and Bush rapidly transitioned away from supporting information access requirements to supporting information security requirements used to ensure national security and public safety. Although mindful of Attorney General Reno's desire for strong governmental action on information access, others on President Clinton's National Security Council envisioned a government and private sector consortium working together to increase national security. In May 1998, President Clinton released Presidential Decision Directive / NSC-63 (PDD/NSC-63) on critical infrastructure protection. According to this directive, the information economy was vulnerable to new forms of warfare:

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, we should, to the extent

feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.⁴⁹³

In the text, the Clinton administration perceived that “the targets of attacks ... would likely include both facilities in the economy and those in the government.” The administration’s “partnership” solution required the “coordinated effort of both the government and the private sector.” This government and private consortium approach also applied to the information subset of the nation’s critical infrastructure.

Actors in the Executive Group realized early on that the use of encryption was a primary solution to the information security problem. Following the policy of Vice President Al Gore’s “Reinventing Government” initiative, the government and private sectors would share the leadership role in guiding information security efforts. In September 1998, the Office of Management and Budget (OMB) published *Access with Trust* that specified the Clinton administration’s views on guaranteeing information security by using the public key infrastructure (PKI). PKI was the information technology sector’s rubric for modern encryption systems that included both secret key and public key subsystems and associated certificate authority infrastructure:

Access with Trust focuses on how the Federal government will promote and use a PKI to safeguard and protect electronic interactions internally (among Federal government employees and agencies) and externally (between the Federal government and its many trading partners — governments, businesses, and individuals). But the principles set forth here, and the steps and tasks identified, do not involve the Federal government alone. Our partners will be other

⁴⁹³ William J. Clinton, Presidential Decision Directive / NSC-63, “Critical Infrastructure Protection,” 22 May 1998: 3.

governments (domestic and foreign), colleges and universities, banks and other businesses, and non-profit organizations and advocacy groups. In particular, our partners will include those private sector technology providers from whose products and services the infrastructure is built.⁴⁹⁴

The text shows that the information security effort involved “partners” that were identified as “other governments (domestic and foreign), colleges and universities, banks and other businesses, and non-profit organizations and advocacy groups.” Although the financial and business sectors were mentioned together in the text, this grouping was not the most important PKI partner. Neither were citizens, as the largest PKI user group, the most important partner. The targeted partners for the government’s consortium effort were the “private sector technology providers,” which were presumed to be information technology vendors and encryption certificate authorities. This initial focus on technology groups did not persist, as actors in the Executive Group had to promote the PKI to a larger group of users and in a more convincing manner.

In December 2000, President Clinton released his *National Security Strategy for a Global Age* (2000 NSS), which in part, amplified PDD/NSC-63’s language on the partnerships involved in critical infrastructure protection:

Most importantly, the Federal Government cannot protect critical infrastructures alone. The private sector owns and operates the vast majority of these infrastructures. Protecting critical infrastructure, therefore, requires the Federal Government to build partnerships with the private sector in all areas — from business and higher education, to law enforcement, to R&D. The Secretary of Commerce and industry leaders — mostly from Fortune 500 companies — are leading the Partnership for Critical Infrastructure Security. The Attorney General

⁴⁹⁴ Office of Management and Budget, *Access with Trust* (Washington, D.C.: GITS, 1998), 3.

has teamed up with the Information Technology Association of America to promote industry-government cooperation against cyber crime through the Cyber Citizen project. The NIPC, meanwhile, is establishing cooperative relationships between industry and law enforcement through its InfraGard initiative.⁴⁹⁵

The text shows critical infrastructure protection requirements depended on the owners of “the vast majority of these infrastructures,” which was the “private sector.” In addition, the executive branch expected to form “partnerships with the private sector in all areas — from business and higher education, to law enforcement, to R&D.” This time, “business” partners received first mention.

The 2000 NSS used encryption as an example to show that businesses and citizens were important considerations along with satisfying the obligations of the Wassenaar Arrangement on dual use technology:

Encryption is an example of a specific technology that requires careful balance. Export controls on encryption must be a part of an overall policy that balances several important national interests, including promoting secure electronic commerce, protecting privacy rights, supporting public safety and national security interests, and maintaining U.S. industry leadership. After reviewing its encryption policy and consulting with industry, privacy and civil liberties groups, the Administration implemented significant updates to encryption export controls in January 2000 and concluded a second update in October 2000.

The text shows that “promoting secure electronic commerce, protecting privacy rights, supporting public safety and national security interests, and maintaining U.S. industry leadership” were important requirements and that electronic commerce for business transactions and privacy rights of citizens were mentioned before satisfying public safety

⁴⁹⁵ The White House, *A National Security Strategy for a Global Age* (Washington, D.C.: GPO, 2000).

and national security requirements. In addition, the 2000 NSS emphasized the importance of encryption users by mentioning their representation by “industry, privacy and civil liberties groups.” This group matched the Encryption Technology Group used in my analysis.

The terrorist attack on September 11, 2001 caused the Bush administration to put PDD/NSC-63’s language in a more authoritative form as Executive Order 13231. President Bush signed this order the month after the attack on October 16, 2001 and narrowed the critical infrastructure protection focus of PDD/NSC-63 to concentrate more on the information security area:

Section 1. Policy.

(a) The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. The protection program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.

(b) It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.⁴⁹⁶

⁴⁹⁶ President, Executive Order 13231, “Critical Infrastructure Protection in the Information Age,” *Federal Register* 66, no. 202 (18 October 2001): 53063-71.

The text shows the Bush administration believed that the “information technology revolution” created vulnerabilities in the government and private sectors. Both sectors relied on “an interdependent network of critical information infrastructures,” which required “a voluntary public-private partnership” to protect adequately. Thus, the Bush administration, like the Clinton administration, perceived that a government and private sector consortium was required to ensure information security. A difference between these administrations was that the Bush administration did not use the Office of Management and Budget to work out the policy details.

President Bush did not use his 2002 NSS to discuss information security, but instead used his December 17, 2003 Homeland Security Presidential Directive / HSPD-7 to set his policy. HSPD-7 superseded PDD/NSC-63 and made the Department of Homeland Security responsible for critical infrastructure protection, which included the information infrastructure:

The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations.⁴⁹⁷

The text shows that the Secretary of Homeland Security was now responsible for the “security of cyberspace,” which was an expansion of domestic information security requirements to include the global information domain. In addition, the text indicates

⁴⁹⁷ George W. Bush, Homeland Security Presidential Directive / HSPD-7, “Critical Infrastructure Identification, Prioritization, and Protection,” 17 December 2003: 4.

that controlling such a large domain would require the “interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations” to produce coherent actions. No dominant actors were identified, which suggested a consortium approach.

The Executive Group’s requirement for a consortium of lead actors matched Allison’s OBM organizing concept of “Central Coordination and Control.” According to this concept, the separate leadership roles played by the executive branch, the private sector, and international actors required “constraints,” which segment and deconflict the activities of consortium members according to their respective areas of competence or historical practice.⁴⁹⁸ During the Status Quo Period, the evolution of the information control problem into a cyberspace security problem subsumed the debate on encryption control by requiring the government, the private sector, and international actors to work together on a looming information security problem. The debate on information access and encryption control diminished in intensity during the Clinton administration and moved to the background in the Bush administration. This allowed the consortium to concentrate on satisfying information security requirements. I therefore assigned a Lead Actor valance of “1” to the Executive Group for being part of a consortium that was focused on information security issues.

⁴⁹⁸ Allison and Zelikow, *Essence of Decision*, 172-173.

B. Problem Perception Valance

Actors in the Executive Group perceived a complex information control problem that had international, economic, technology leadership, national security, and public safety dimensions. One input of the Clinton administration to the *Digital Millennium Copyright Act*, which implemented the negotiated WIPO treaties, was to restrict the global availability of circumvention technology. Assistant Secretary of Commerce Bruce A. Lehman testified before a House committee on a measure to ensure information security by outlawing circumvention devices. Such devices included illicit “ripping” tools used to read and copy DVDs, descramblers used to pirate television signals, and computer code used to circumvent proprietary information security schemes:

Mr. LEHMAN. Congressman, the treaty requires contracting parties to provide adequate legal protection and the effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this treaty or the Berne Convention. That is the test in the treaty. It really does not go to the issues that you just raised.

We in the Administration feel very strongly that it is important that other countries not have a loophole under which they can get out of their obligations under this treaty. To have a standard based on intent would very much permit that to happen.⁴⁹⁹

The text shows that actors in the Executive Group believed that “effective legal remedies against the circumvention of effective technological measures” were required because of the international problem of intellectual property theft. In addition, the text shows that “a

⁴⁹⁹ House Committee, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 62.

standard based on intent” to prevent the theft of intellectual property was less desirable than a law to prohibit the devices used to steal such property. This belief in restricting tangible devices was thought to be more applicable in coercing “other countries” that were facilitating the manufacture and distribution of these devices. Little thought was put into restricting intangible devices such as software ripping programs. The Clinton administration’s belief in protecting valuable economic information from aggressive nations and criminal activities was soon transformed into protecting the information infrastructure.

President Clinton’s 1998 critical infrastructure PDD/NSC-63 superseded parts of the defunct encryption management PDD/NSC-5. PDD/NSC-63 emphasized the global nature of the threats to the United States information infrastructure:

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems....

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.⁵⁰⁰

⁵⁰⁰ William J. Clinton, Presidential Decision Directive / NSC-63, “Critical Infrastructure Protection,” 22 May 1998: 1-2.

In the text, President Clinton believed that there were vulnerabilities in the nation's "cyber-based information systems" that could be exploited by "future enemies, whether nations, groups or individuals." This broad perception of the information security problem had an international dimension in the form of hostile nations and a domestic dimension in the form of hostile organizations and agents that could be operating in the United States. Both economic and military power would be the targets of these hostile actors. Defending against "non-traditional attacks on our infrastructure and information systems" would require intelligence about these hostile actors and their methods of attack and targets. Encryption use by these hostile actors could deny this intelligence, and thus, foreign and domestic encryption use had to be controlled.

The 1999 *Security and Freedom through Encryption (SAFE) Act* would have liberalized the use of encryption, and this law was contrary to the initial encryption control direction of the Clinton administration. During a 1999 hearing on the *SAFE Act*, the Deputy Director of the NSA and the Associate Deputy Attorney General discussed the complexities of gaining intelligence on foreign countries and obtaining information access on individuals operating within the United States. In her prepared statement, Deputy Director Barbara McNamara attempted to clarify the Clinton administration's policies on foreign and domestic encryption use:

Please do not confuse the needs of national security with the needs of law enforcement. The two sets of interest and methods vary considerably and must be addressed separately. The law enforcement community is concerned about the use of non-recoverable encryption by persons engaged in illegal activity

domestically. At NSA, we are primarily focused on preserving export controls on encryption to protect national security.⁵⁰¹

The text shows that NSA, under the Department of Defense, viewed the information access problem as an international issue that involved “preserving export controls” on encryption products. Presumably, limiting the exports of strong encryption would have simplified the job of NSA. The Department of Justice viewed the information access problem as a domestic issue that involved the “use of non-recoverable encryption by persons engaged in illegal activity.” With these positions, NSA and the Department of Justice appeared to challenge the evolving Clinton administration position on information security.

During a 1999 hearing on the *E-SIGN Act*, Deputy Associate Attorney General Ivan K. Fong discussed a Clinton administration policy that appeared to focus both on information security and on advancing the economy and e-commerce with digital signatures:

As the Nation’s litigator, legal advisor, and primary law enforcement agency, the Department of Justice strongly supports the administration’s efforts to encourage the healthy growth of electronic commerce.⁵⁰²

⁵⁰¹ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 46.

⁵⁰² House Committee on the Judiciary, Subcommittee on Courts and Intellectual Property, *Electronic Signatures in Global and National Commerce (E-SIGN) Act*, 106th Congress, 1st sess., 30 September 1999, Serial No. 3, 13.

While this text shows that, “the healthy growth of electronic commerce” was a dominant policy issue with the executive branch, Mr. Fong’s preparatory comments indicated otherwise:

Just last month, the President issued an executive order, Executive Order 13133, that directs the Attorney General to chair an Interagency Working Group on Unlawful Conduct Involving the use of the Internet.

This text questions whether the primary focus of the executive branch was with information security and economic growth or with information access and the ability to police the Internet to ensure public safety.

President Clinton’s 2000 NSS advanced the Wassenaar Arrangement on controlling the international spread of encryption, but did not advance the domestic information access requirements of the Department of Justice. The 2000 NSS did advance the domestic requirements of PDD/NSC-63 for infrastructure protection:

Critical Infrastructure Protection

An extraordinarily sophisticated information technology (IT) infrastructure fuels America's economy and national security. Critical infrastructures, including telecommunications, energy, finance, transportation, water, and emergency services, form a bedrock upon which the success of all our endeavors -- economic, social, and military -- depend. These infrastructures are highly interconnected, both physically and by the manner in which they rely upon information technology and the national information infrastructure. This trend toward increasing interdependence has accelerated in recent years with the advent of the Information Age.⁵⁰³

⁵⁰³ The White House, *A National Security Strategy for a Global Age*, 24.

The text indicates that the reliance on an “extraordinarily sophisticated information technology (IT) infrastructure” was perceived as a vulnerability. In addition, the text indicates that this vulnerability was growing with time as the “interdependence” of critical infrastructures had “accelerated in recent years with the advent of the Information Age.” This growing importance of the information security problem continued through the new administration.

The Bush administration did not continue the explicit discussions of encryption control and information infrastructure protection in their 2002 version of the NSS, but did address domestic information security issues in Homeland Security Presidential Directive / HSPD-7. This directive, like its predecessor PDD/NSC-63, tended to emphasize the challenges of protecting the critical information infrastructure, which was presumed to be the major vulnerability of the critical infrastructure:

To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, [] Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The organization will support the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law.⁵⁰⁴

⁵⁰⁴ George W. Bush, Homeland Security Presidential Directive / HSPD-7, “Critical Infrastructure Identification, Prioritization, and Protection,” 17 December 2003: 4.

The text indicates that the Bush administration considered the “Federal departments and agencies with cyber expertise” as key actors responsible for protecting “critical infrastructure information systems” in the United States. The last sentence in this text appears to encourage the Department of Justice to seek information access solutions so that it could continue to “investigate and prosecute threats to and attacks against cyberspace.” Thus, the Bush administration emphasized the domestic aspects of information access and security in a manner similar to that of the second Clinton administration, but remained purposefully vague on the specifics of the information access issue. This issue has moved underground as a political condition and not as a problem that could upset the national intelligence consolidation debate.

The view of a complex problem by actors in the Executive Group matched Allison’s GPM organizing concept of “Goals and Interests” where “many national security interests are accepted,” but “domestic political interests” shape the final perception of the problem.⁵⁰⁵ During the second term of the Clinton administration, actors in the Executive Group first perceived an economic information security problem in the form of protecting intellectual property from international thieves. Soon after that, the Clinton administration perceived a much larger domestic information security problem with hostile foreign countries and international organizations that could attack the nation’s vulnerable information infrastructure. This threat to the military and economic power of the United States drove the policies found in PDD/NSC-63. While

⁵⁰⁵ Allison and Zelikow, *Essence of Decision*, 298.

information security tools could protect the information infrastructure, these tools created international and domestic information access problems. Evidence of these problems was found in the Clinton administration's persistent information access position throughout the debate on the failed *SAFE Act* and the successful *E-SIGN Act*. President Clinton's 2000 National Security Strategy elevated the importance of information security requirements to a level higher than information access requirements, but still sought ways to rebalance information access and security requirements.

After the terrorist attack on September 11, 2001, the Bush administration did not use its NSS as a policy tool to advanced information security requirements. HSPD-7 on critical infrastructure protection did so, but was publicly silent on the information access problem. This part of the complex problem was subsumed by a continuing national intelligence debate within the administration and with Congress. I therefore assigned a Problem Perception valance of "2" to the Executive Group for perceiving a complex information control problem dominated by information security concerns and with international, domestic, and economic dimensions. Satisfying dominant information security concerns also satisfied actors concerned with protecting privacy, so long as the Global War on Terrorism did not dramatically elevate government information access requirements.

C. Favored Alternative Valance

Actors in the Executive Group favored new information control laws and regulations that promoted information security over information access requirements,

maintained United States technology leadership, and advanced domestic economic goals. In the area of satisfying treaty obligations on encryption control, actors in this group prodded Congress to retroactively legalize actions taken by executive orders. In the area of uniform information access laws and regulations, actors in this group agreed on the problem, but could not agree on a common solution. This disagreement can be traced to the blurring of the relationships between private sector information access and security requirements during the passage of the *Digital Millennium Copyright Act* in 1998.

The Clinton administration supported passage of the *DMCA* in order to ratify United States compliance with the World Intellectual Property Organization treaties. Assistant Secretary of Commerce Bruce A. Lehman conveyed the administration's information security position on economically valuable intellectual property during a House hearing on the *DMCA*:

We have to keep in mind that in other countries people will be looking to us for a signal. Many developing countries around the world—and we do not want to give them a loophole to be able to steal our intellectual property. So we had to draft this implementing legislation very, very carefully.

And I would just note, Mr. Chairman, that with regard to the anti-circumvention provision in Section 1201, that the test is that the [circumvention] device must be primarily designed or produced for the purpose of circumventing intellectual property protection; primarily designed or produced. That this is a very reasonable test, Mr. Chairman, and I think it goes to the reasonableness of the legislation.⁵⁰⁶

⁵⁰⁶ House Committee, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*, 35. Officials regularly misused the term “anti-circumvention device” when they should have used the term “circumvention device.”

The text shows that the Clinton administration was forced to use specific legislation to guarantee worldwide information security of digital intellectual property, because they believed that poorly crafted legislation would give “[m]any developing countries ... a loophole to be able to steal our intellectual property.” In addition, the text shows the specific piece of legislation that would eliminate this loophole was “the anti-circumvention provision in Section 1201.” This provision was an information security guarantee that gave legal protection to encryption systems used to control access to intellectual property.

The idea of using “chained protections” or protective laws compounded with technology solutions caused public concerns on restricting the fair use of intellectual property and on promoting the eventual extinction of public domain information. In a change of roles, the government saw fair use concerns as a public demand for information access. To alleviate these concerns, the administration believed in the “reasonableness of the legislation” to limit devices “primarily designed or produced for the purpose of circumventing intellectual property protection,” while allowing for the fair use of intellectual property and public access to information. In essence, the government would protect weak encryption as a way to regulate public information access requirements to copyrighted digital material and intellectual property.

The Clinton administration explained its preference to use information control legislation in its 1998 PDD/NSC-63 on protecting the critical infrastructure. PDD/NSC-63 set a policy that additional laws and regulations would be needed to take care of “a

material failure of the market to protect health, safety or well-being of the American people.”⁵⁰⁷ Within a year, the Department of Justice was of the opinion that the market control of encryption proposed in the 1999 *Security and Freedom through Encryption (SAFE) Act* would not work. In his testimony to the House committee hearing, Associate Deputy Attorney General Ronald D. Lee described the problem with this encryption-liberalizing bill:

The Department of Justice is, however, deeply concerned about the threat to public safety that is posed by the widespread availability and distribution of nonrecoverable encryption; that is, encryption where there is not a lawfully authorized means to obtain the plaintext of communications and data.

Law enforcement agencies, both Federal and State, have already begun to see cases where encryption has been used in an attempt to conceal criminal activity, and we anticipate the number and complexity of these cases will increase as encryption proliferates and as encryption increasingly becomes a component of mass market software items. We remain vitally concerned that agents will not be able to fully execute the search warrants, wiretap orders, and other legal processes authorized by Congress and ordered by the courts that are essential to effective law enforcements investigations today.⁵⁰⁸

The text shows the Department of Justice believed that even without a market failure, government maintenance of encryption controls was required to alleviate public safety concerns posed by the “widespread availability and distribution of nonrecoverable encryption.” In addition, the text implies that the unregulated market was part of the problem because encryption was becoming “a component of mass market software items.” The administration’ idea on preventing market failure by laws and regulatory

⁵⁰⁷ William J. Clinton, Presidential Decision Directive / NSC-63, “Critical Infrastructure Protection,” 22 May 1998: 4.

⁵⁰⁸ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 48.

controls persisted, even in a period when there were no market failures. The same idea was used during the hearings on digital signatures legislation.

The Clinton administration's balanced policy argued for new laws and regulations to satisfy both information access and information security requirements. During a 1999 House hearing on the *E-SIGN Act*, the General Counsel of the Department of Commerce, Mr. Andrew Pincus, suggested that laws and regulations were required to ensure information security of parties in digital transactions:

Mr. COBLE. Thank you both for appearing before our subcommittee. Mr. Pincus, in your statement you argue that if H.R. 1714 is enacted, it could force government to transact business and accept records by any means and according to any standards, which could pose a security threat to government system. I'm not quarrelling with that, but give us an example.

Mr. PINCUS. One of the concerns is that the bill has a technology neutrality requirement, which we agree with[,] with respect to government regulation of private transactions, because there are a lot of different ways to sign electronically, anything from just sending an e-mail with your named typed at the bottom to the most sophisticated and secure cryptography....

So the concern is that when government itself is a party to the transaction, just like any other party, it should be entitled to determine the level of security and trust that it needs for that transaction and to implement that. We are afraid the non-discrimination provision denies that to government at all levels.⁵⁰⁹

The text shows the Department of Commerce favored regulating digital signatures because they feared the private sector would resort to market alternatives that would "transact business and accept records by any means and according to any standards." Since the Department of Commerce's NIST had developed the Digital Signature

⁵⁰⁹ House Committee on the Judiciary, Subcommittee on Courts and Intellectual Property, *Electronic Signatures in Global and National Commerce (E-SIGN) Act*, 106th Congress, 1st sess., 30 September 1999, Serial No. 3, 16-17.

Standard (DSS) four years earlier, Mr. Pincus' statement that digital signatures ranged "from just sending an e-mail with your name typed at the bottom to the most sophisticated and secure cryptography" implied that the *E-SIGN Act* should focus on the use of public key encryption-based digital signatures. In addition, the text introduces the idea that all users should be "entitled to determine the level of security and trust" required for their electronic transactions. The administration's idea that the government and users should set their own security and trust requirements was inconsistent with the administration's objection to market control of information access and security requirements during the debate on the *SAFE Act*.

Instead of maintaining a consistent policy, actors in the Executive Group favored a persistent push for laws and regulations that balanced information security and access requirements. For example, President Clinton used his 2000 NSS to discuss his rationale for export controls on dual-use technology:

The Administration also seeks to prevent destabilizing buildups of conventional arms and to limit access to sensitive technical information, equipment, and technologies by strengthening international regimes, including the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ...⁵¹⁰

The text does not mention the requirement for a supportive domestic law to "limit access to sensitive technical information" or the details on how Congress would pass such a supportive law to authorize the "Wassenaar Arrangement on Export Controls." Both the

⁵¹⁰ The White House, *A National Security Strategy for a Global Age* (Washington, D.C.: GPO, December 2000), 15.

Clinton and Bush administrations escaped requirements for supportive legislations by issuing successive executive orders. This was the same solution tried during the Competitive Period, but with one important difference.

In November 2000, Congress passed PL 106-508 that retroactively extended the expired *Export Administration Act of 1979* until August 2001.⁵¹¹ This had the effect of adding legal weight to regulatory controls placed on encryption exports by the Clinton and Bush administrations. President Bush took advantage of Congress' retroactive legislation by issuing Executive Order 13206 on April 4, 2001 to terminate actions taken under emergency authority:

All rules and regulations issued or continued in effect under the authority of IEEPA and Executive Order 12924, including those codified at 15 C.F.R. 730–74 (2000), and all orders, regulations, licenses, and other forms of administrative action issued, taken, or continued in effect pursuant thereto, remain in full force and effect, as if issued, taken, or continued in effect pursuant to and as authorized by the Act or by other appropriate authority until amended or revoked by the proper authority. Nothing in this order shall affect the continued applicability of the provision for the administration of the Act and delegations of authority set forth in Executive Order 12002 of July 7, 1977, Executive Order 12214 of May 2, 1980, Executive Order 12938 of November 14, 1994, as amended, Executive Order 12981 of December 5, 1995, as amended, and Executive Order 13026 of November 15, 1996.⁵¹²

The text shows that President Bush's termination order under the *International Emergency Economic Powers Act* actually continued the regulatory details found in "15 C.F.R. 730–74 (2000), and all orders, regulations, licenses, and other forms of

⁵¹¹ *To provide for increased penalties for violations of the Export Administration Act of 1979, and for other purposes, U.S. Statutes at Large* 114 (2001): 2360.

⁵¹² President, Executive Order 13206, "Termination of Emergency Authority for Certain Export Controls," *Federal Register* 66, no. 68 (09 April 2001): 18397.

administrative action.” President Bush effectively continued President Clinton’s encryption export control policy directed by “Executive Order 13026 of November 15, 1996.” President Bush’s solution to continue previous encryption export policies and Congress’ approval of these policies by retroactive legislation effectively produced a form of legal information control policy.

This new form of export law appeared acceptable to the executive and legislative branches, despite Senator Michael B. Enzi’s (R-Wyoming) warning that the administration was making unilateral export laws:

As a result, our export control laws have been inadequately governed by either the EAA of 1979 or, more often than not, by emergency Presidential authority under the International Emergency Economic Powers Act. This situation has effectively allowed the administration, instead of Congress, to set the export control policies of the United States.⁵¹³

Senator Enzi warning was insufficient to secure passage of the *Export Administration Act of 2001*. Predictably, President Bush continued to set encryption export policy through Executive Order 13222, which covered the congressional lapse.⁵¹⁴ Once again, if Congress retroactively changes the date on old legislation to make it current, then the decisions found in Executive Order 13222 will effectively become export control law.

After September 11, 2001, actors in the executive branch did not take advantage of the *USA PATRIOT Act* to alter dramatically the balance between information access and

⁵¹³ *Congressional Record*, 107th Congress, 1st sess., 2001, 147, pt. 8: S461.

⁵¹⁴ President, Executive Order 13222, “Continuation of Export Control Regulations,” *Federal Register* 66, no. 163 (22 August 2001): 44026-27.

security requirements. President Bush, in a statement on this law, claimed that it necessarily increased surveillance powers to protect national security and public safety:

Surveillance of communications is another essential tool to pursue and stop terrorists. The existing law was written in the era of rotary telephones. This new law that I sign today will allow surveillance of all communications used by terrorists, including emails, the Internet, and cell phones. As of today, we'll be able to better meet the technological challenges posed by this proliferation of communications technology.⁵¹⁵

The text shows that President Bush believed the *USA PATRIOT Act* would "allow surveillance of all communications," but did not discuss how the "technological challenges" would be satisfied. One of these technology challenges was encryption use, which could both deny information access and increase information security.

President Bush preferred to use executive orders to satisfy both information access and security requirements, but eventually took advantage of the *Homeland Security Act of 2002* to protect the information infrastructure of the United States. At first, he used Executive Order 13228 to establish the Office of Homeland Security and its mission and functions:

Sec. 2. Mission. The mission of the Office shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. The Office shall perform the functions necessary to carry out this mission, including the functions specified in section 3 of this order.

⁵¹⁵ President, "Remarks on Signing the USA PATRIOT Act of 2001," 26 October 2001, *Weekly Compilation of Presidential Documents* 37, no. 43 (29 October 2001): 1550-1.

Sec. 3. Functions. The functions of the Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.⁵¹⁶

The text shows that the Office of Homeland Security had to implement a “comprehensive national strategy to secure the United States.” In addition, the text shows that two relevant functions of this office would be threat detection and protection of vulnerabilities “within the United States.” Eight days after Executive Order 13228, President Bush issued Executive Order 13231, which set his policy on the protection of the critical infrastructure of the United States to include the “critical information infrastructure.”⁵¹⁷ Congress passed the *Homeland Security Act of 2002*, which supported most of President Bush's objectives. In a statement on this law, President Bush appeared satisfied:

This bill includes the major components of my proposal—providing for intelligence analysis and infrastructure protection, strengthening our borders, improving the use of science and technology to counter weapons of mass destruction, and creating a comprehensive response and recovery division.⁵¹⁸

The text shows both the threat detection and vulnerability protection components of President Bush's strategy. However, the weak “intelligence analysis” term did not fully equate to threat detection or the intelligence capability of gaining information access to the plans and intentions of criminals, spies, and terrorists. This capability was delayed by the debate on a national intelligence bill, which was reaching a climax in December 2004.

⁵¹⁶ President, Executive Order 13228, “Establishing the Office of Homeland Security and the Homeland Security Council,” *Federal Register* 66, no. 196 (10 October 2001): 51812.

⁵¹⁷ President, Executive Order 13231, “Critical Infrastructure Protection in the Information Age,” *Federal Register* 66, no. 202 (18 October 2001): 53063-71.

⁵¹⁸ President, “Statement on Congressional Action on Legislation to Establish the Department of Homeland Security,” 19 November 2002, *Weekly Compilation of Presidential Documents* 38, no. 47 (25 November 2002): 2058.

The actions of the Executive Group matched Allison's GPM general proposition of "Action and Intention," where agreement on laws and regulations "reflect the momentary operational convergence of a mix of motives."⁵¹⁹ Actors in the executive branch reached agreement with the legislative branch to pass a series of laws to solve the international and economic issues surrounding information security. The Clinton administration, along with Congress, believed that the 1998 *Digital Millennium Copyright Act* would advance the economic interests of the United States by ensuring information security of selected industries. Legal measures, such as protecting encryption schemes used by intellectual property owners, would become a matter of contentious court actions. The Clinton administration agreed with Congress on the *E-SIGN Act*, which allowed the use of robust technology such as public key encryption-based digital signatures. The Clinton administration disagreed with Congress on the encryption liberalizing extent of the *SAFE Act*, because of the administration's support of the Wassenaar Arrangement. During the Status Quo Period, a convergence of actions happened when Congress was forced to retroactively renew export legislation. This had the effect of adding legal support and resources to encryption export controls directed solely by the executive branch.

While the Clinton administration overtly started the effort to protect the critical information infrastructure, the terrorist attack on September 11, 2001 gave the Bush administration the law they needed to support the required information security effort. The *Homeland Security Act of 2002* was strong enough to add resources and legal

⁵¹⁹ Allison and Zelikow, *Essence of Decision*, 306.

authority to the information security effort, but not to the information access effort required by the intelligence agencies. The *USA PATRIOT Act* did not satisfy information access requirements, especially for encrypted information, and further efforts would have to wait until the national intelligence debate was finished. I assigned a Favored Alternative valance of “2” to the Executive Group for favoring laws and executive orders reinforced by laws to achieve their information security goals, but at the delay of achieving their information access goals. Actors in the Executive Group could not integrate both sets of goals into a single information control law, so they went with using several laws.

D. Decision Timing Valance

During the Status Quo Period, actors in the Executive Group made incremental decisions on information control problems that were dependent on three interrelated information control tracts. The information access tract had a legacy from the first Clinton administration of using executive orders to control encryption exports, and this tract is shown by the upper “access” timeline in Figure 4-8. The viability of the evolving Export Administration Regulations (EAR) was threatened in the Status Quo Period by private lawsuits challenging encryption export laws. The loss and setback experienced by the United States government in the *Bernstein v. U.S. Department of Justice* and *Junger v. Daley* encryption control cases, respectively, limited the effectiveness of the EAR and required its incremental change. In May 1999, the United States Court of Appeals for the Ninth Circuit found that “insofar as the EAR regulations on encryption

software were intended to slow the spread of secure encryption methods to foreign nations, the government is intentionally retarding the progress of the flourishing science of cryptography.”⁵²⁰ In addition, this court found that on-going government information control efforts “appear to strike deep into the heartland of the First Amendment.”⁵²¹

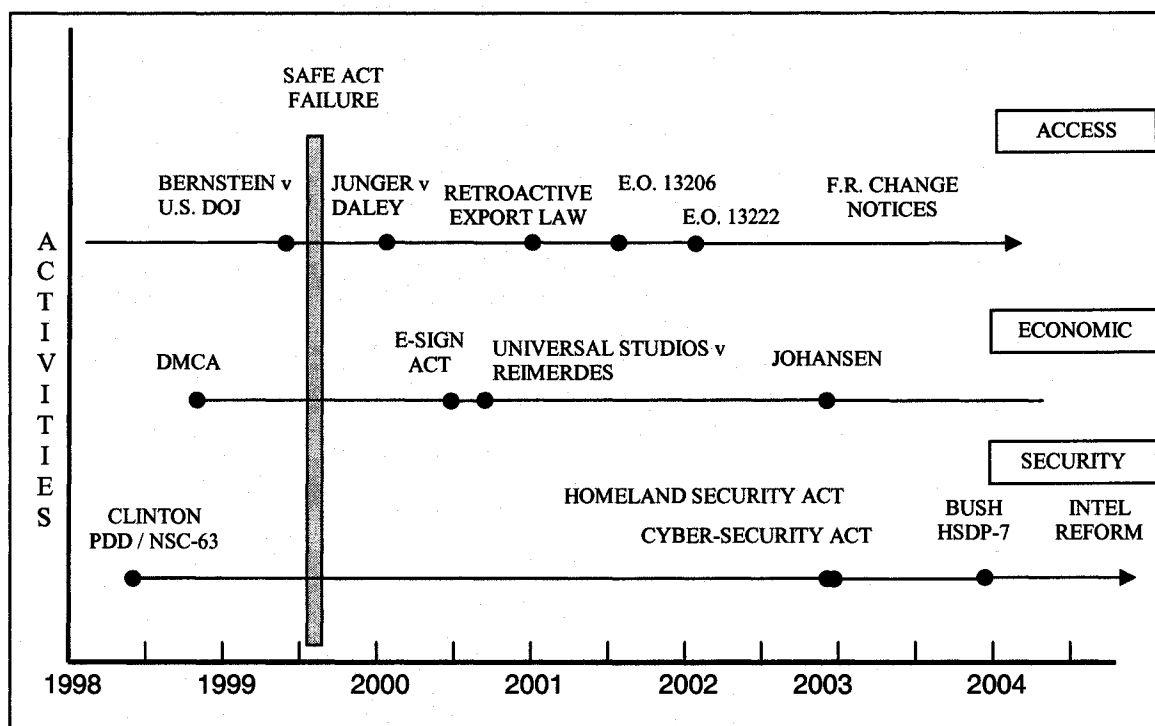


Figure 4-8 Timeline of executive branch activities on information and encryption control.

During the *Junger v. Daley* case, the executive branch used policy maneuvering to prevent a repeat of the Bernstein ruling. In April 2000, the United States Court of Appeals for the Sixth Circuit hearing the *Junger v. Daley* case found that “In light of the

⁵²⁰ *Bernstein v United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999). See the concluding comments on page 1145.

⁵²¹ *Ibid.*

recent amendments to the Export Administration Regulations, the district court should examine the new regulations to determine if Junger can bring a facial challenge.”⁵²² Challenges to the applicable EAR took years in court, as shown by Junger’s problems that started in 1997. By the time of his appeal, the executive branch had changed the relevant parts of the EAR, and the appeals court remanded the case back to the lower court. Thus, by incrementally modifying the EAR, actors in the Executive Group found a way to counter legal challenges to regulations controlling the export of encryption software. These two court rulings are shown in Figure 4-8 and bracket the failure of the 1999 *SAFE Act*.

The 1999 failure of the *Security and Freedom through Encryption Act* represented a success for the Clinton administration, because Congress was not able to liberalize in an abrupt fashion the encryption control policy found in the EAR. During the 1999 House hearing on the *SAFE Act*, NSA Deputy Director McNamara gave a rationale for supporting incremental changes to export regulations:

Passage of legislation that immediately decontrols the export of strong encryption will significantly harm NSA’s ability to carry out its mission and will ultimately result in the loss of essential intelligence being provide to this Government. Immediate decontrol of encryption exports will likely result in the global spread of strong encryption among our adversaries and the use of encryption at multiple levels within a communications network. This will greatly complicate our exploitation of foreign targets and the timely delivery of usable

⁵²² *Junger v Daley*, 209 F.3d 481 (6th Cir. 2000). See the paragraph before the remand decision on page 485.

intelligence because it will take too long to decrypt a message, if indeed we can decrypt it at all.⁵²³

The text shows that actors in the Executive Group believed that passage of the *SAFE Act* would “ultimately result in the loss of essential intelligence” and would “likely result in the global spread of strong encryption among [its] adversaries.” Thus, control of encryption exports was a method of ensuring information access to intelligence on potential enemies by limiting the global availability of encryption.

This legacy use of executive orders and incremental changes to the EAR continued with the George W. Bush administration as demonstrated by a recent change notice published in the December 2004 *Federal Register*:

Administrative Changes

This rule revises the e-mail address of the ENC Encryption Request Coordinator wherever it appears in § 740.9, § 740.13, and § 740.17 from *enc@ncsc.mil* to *enc@nsa.gov* to reflect the current e-mail address of that organization. In § 740.17(e)(5)(i), this rule revises the mailing address of the BIS office to which semi-annual License Exception ENC reports are sent, to reflect the current name of that office.

Although the Export Administration Act expired on August 20, 2001, Executive Order 13222 of August 17, 2001 (3 CFR, 2001 Comp., p. 783 (2002)), as extended by the Notice of August 6, 2004, 69 FR 48763 (August 10, 2004) continues the Regulations in effect under the International Emergency Economic Powers Act.⁵²⁴

The text shows the typical revisions to encryption export section of Title 15, Code of Federal Regulations and the continuing national security influence on information access

⁵²³ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 43.

⁵²⁴ U.S. Department of Commerce, Bureau of Industry and Security, "Encryption Export and Reexport Control Revisions," *Federal Register* 69, no. 236 (9 December 2004): 71356-71364.

requirements as demonstrated by the “ENC Encryption Request Coordinator” e-mail change from a “*enc@ncsc.mil*” military address to a “*enc@nsa.gov*” National Security Agency address. In addition, the text cites the continuing use of executive orders issued under the *IEEPA* and *Federal Register* notices to propagate changes to encryption export policy. The upper timeline in Figure 4-8 shows the executive branch’s decisions and Congress’ 2000 retroactive law to support these decisions. The net effect of this law was to legalize periodic changes to the EAR, which were used to control encryption technology exports and to defer continuing legal challenges.

The information security tract was divided along the lines of an economic area and a national security and public safety area. The 1998 *DMCA* and the 2000 *E-SIGN Act* were relatively successful legislations in protecting the economic value of information. These laws originally required little support from the executive branch, because private companies could now use legal actions to negate threats to their information security. The middle “economic” timeline in Figure 4-8 shows the 2000 *Universal Studios, Inc. v. Reimerides* case in which a private company used the *DMCA* to prevent an “Internet web-site owner from posting for downloading computer software that decrypted digitally encrypted movies.”⁵²⁵ While *DMCA* protection appeared to be working in the United States, actors in the Executive Group were told that the decision to allow broad legal protection of weak information security technology would eventually fail.

⁵²⁵ *Universal Studios, Inc. v Reimerides*, 111 F.Supp.2d 295 (S.D.N.Y. 2000).

Legal support for weak information security tools was a short-lived tacit decision. Simple reverse engineering techniques and fair-use doctrine, both made public by the Norwegian trial of Johansen for cracking the encryption system on his own DVD, threatened parts of *DMCA* specifically authored by the Clinton administration. In a 2002 statement on his proposed remedy to the *DMCA*, Congressman Rick Boucher (D-VA) highlighted the problems with enforcing legal protections from circumvention technology:

In response to these concerns, the Administration limited the prohibition to devices that are primarily designed or produced for the purpose of circumventing; have only a limited commercially significant purpose or use other than to circumvent; or are marketed for use in circumventing. Even with this modification, however, the provision still contained a fundamental defect: it prohibited circumvention of access controls for lawful purposes, and it prohibited the manufacture and distribution of technologies that enabled circumvention for lawful purposes.⁵²⁶

The text shows that Clinton administration wanted a law that “limited the prohibition to devices that [were] primarily designed or produced for the purpose of circumventing.” In addition, the text shows Congress believed that “the provision still contained a fundamental defect.” Once the tacit decision was made to sacrifice reverse engineering and fair use rights in *DMCA*, it was only a matter of time before less sympathetic WIPO signatories, such as Norway, would react unfavorably. The failure of a Norwegian court to convict Johansen signaled a limit to global information security laws.⁵²⁷ Figure 4-8

⁵²⁶ *Congressional Record*, 107th Congress, 2d sess., 2002, 148, pt. 129:E1760-1.

⁵²⁷ Morten Overbye, “Teenager Cleared in Landmark DVD Case,” *CNN.com/Technology*, 7 January 2003, < <http://www.cnn.com/2003/TECH/01/07/dvd.johansen/> >, accessed October 2004.

shows the evolution of laws favoring information security such as *DMCA* and the *E-SIGN Act*, Universal Studios' success in court, and the 2003 foreign rebuke of *DMCA*.

The lower timeline in Figure 4-8 shows the national security and public safety tract, which could be best satisfied by the use of strong encryption. The tract starts with the 1998 publication of President Clinton's PDD/NSC-63 on critical infrastructure protection. However, some actors in the Executive Group believed that the use of strong encryption should have been delayed to allow implementation of information access measures, which were also required to protect national security and public safety. In 1999, the Deputy Associate Attorney General, Mr. Ronald D. Lee, testified during the *SAFE Act* hearing on logic of delaying the use of strong encryption:

Mr. LEE. Excuse me sir, I think the key goes back to a statement that Secretary Reinsch made, which is there is a difference between availability and widespread use. What the Department of Justice and law enforcement ultimately will need is when strong encryption is available in a widespread way internationally, a way whether it is key recovery or another way, to present lawful authority and be able to recover pain text. So you have to look at the consequences of decontrol, which is what you are asking me about, versus the end stage—that law enforcement and I think our law enforcement allies would agree with this—the end stage which is we all want to have strong encryption in widespread international use. We want that done in a way, in a system, in an implementation with the proper doctrine and services that support law enforcement.

So I would draw a distinction between what will immediately happen if H.R. 850 is passed and versus the end stage, which we absolutely support, which is the widespread use of strong encryption both domestically and abroad that support law enforcement interests.⁵²⁸

⁵²⁸ House Committee, *Security and Freedom through Encryption (SAFE) Act*, Serial No. 34, 65.

The text shows that the Department of Justice ultimately supported the “widespread use of strong encryption both domestically and abroad,” but needed time to find an “implementation with the proper doctrine and services” to allow information access. The failure of the *SAFE Act* gave actors in the Executive Group several years to arrive at an encryption control solution, which is currently set to a 64-bit limit on secret key encryption tools exported to potentially hostile foreign actors.⁵²⁹ On the domestic side, actors in the Executive Group did not make progress on domestic encryption control to satisfy information access requirements.

The terrorist attack on September 11, 2001 elevated the priority of ongoing information security efforts and resulted in the presidential signing of the *Homeland Security Act of 2002* and the *Cyber Security Research and Development Act* within fourteen months of the attack. Figure 4-8 shows the incremental progression of information security efforts starting with the 1998 PDD/NSC-63 on infrastructure protection and including the dates for the two laws just mentioned. President Bush’s HSPD-7 was signed in December 2003 and superseded PDD/NSC-63. With information security covered by a series of presidential directives and laws, a tacit decision was made to separate the national intelligence reorganization issues from the homeland security problem. National intelligence issues, though organic to homeland and information security, surfaced just before the 2004 national elections. The controversial area on

⁵²⁹ U.S. Department of Commerce, Export Administration Regulations, *Code of Federal Regulations*, vol. 15, sec. 742.15 (Washington, D.C.: GPO, 2004), 305-308, <
http://www.access.gpo.gov/nara/cfr/waisidx_04/15cfr742_04.html >, accessed 15 December 2004.

encryption being used to defeat intelligence surveillance activities was not mentioned in the House report on the proposed *Intelligence Reform and Terrorism Prevention Act of 2004*.⁵³⁰ In effect, the encryption control problem was not coupled to this act. Prior legislations such as the *Economic Espionage Act of 1996* at least had reporting requirements to Congress on the number of times encryption was used to defeat government surveillance efforts. The acquiescence of the executive branch in supporting information access requirements in the intelligence bill may have been an organizational aversion to failed legislations that included debates on encryption control.

The actions of the Executive Group matched Allison's OBM general proposition of "Implementation Reflects Previously Established Routines," whereby the Clinton and Bush administrations continued older agreements and policies on balancing information access and security requirements in the hope of eventually gaining support through laws.⁵³¹ In the area of government information access, action was limited to the continued support of export regulations through executive orders and by pursuing violators in federal court. All the while, actors in the Executive Group never received guidance from Congress in the form of an export law, but did receive tacit approval in the form of retroactive date changes on expired export laws.

In the case of information security for economic reasons, Congress passed the *Digital Millennium Copyright Act*, but actors in the Executive Group knew that their

⁵³⁰ U.S. House, Conference Report, *Intelligence Reform and Terrorism Prevention Act of 2004*, 108th Congress, 2d sess., 07 December 2004, Report 108-796, 108.

⁵³¹ Allison and Zelikow, *Essence of Decision*, 178.

proposed anti-circumvention clauses were tacit decisions to help pass legislation and would eventually fail in the courts. When it came to satisfying information security requirements to protect the critical information infrastructure, actors in the Executive Group were successful with a series of presidential directives and in obtaining legislations such as the *Homeland Security Act of 2002* and the *Cyber Security Research and Development Act*. In the post September 11, 2001 legislative environment, the executive branch had to defer serious consideration of the intelligence consolidation bill until 2003 and did not discuss information access requirements to avoid upsetting the legislative process. I therefore assigned a Decision Timing valance of “1” to actors in the Executive Group for producing incremental directives, executive orders, and legislations in solving the information access and security problem.

Government Agencies Group

In the Status Quo Period, actors from the Government Agencies Group managed the development of secret key and public key encryption standards by asking the private sector to submit their best designs for consideration. While the Government Agencies Group did not develop a federal standard for a complete encryption system, they did develop standards for encryption subsystem components. In the area of public key encryption, they created a more flexible digital signature standard that allowed a choice among public key encryption algorithms. Unlike their Digital Signature Algorithm of the Competitive Period, the National Institute of Standards and Technology (NIST) developed a new Digital Signature Standard with the added choice of two commercial

algorithms. In the area of the secret key encryption, NIST developed the Advanced Encryption Standard (AES) to replace the obsolescent Data Encryption Standard. AES development was brought about through an open global competition, which the popular media highlighted. During the Status Quo Period, actors in the Government Agencies Group took actions that were dependent upon the availability of alternatives and did not openly take sides in the encryption control or encryption liberalization debate. Federal Information Processing Standards, official notices published in the *Federal Register*, presidential directives, and United States patents provided the data for analyzing the actions of the Government Agencies Group. I analyzed the actions of this group according to the four valances derived from Allison's decision models.

A. Lead Actor Valance

During the Status Quo Period, actors in the Government Agencies Group realized that government-directed standards were not viable in the global or domestic market and looked to the technology leadership of the private sector for help. In a 1997 *Federal Register* notice, NIST asked for public submissions that would make the revised Digital Signature Standard more useful and marketable:

The purpose of the revision will be to enable Federal departments and agencies greater flexibility, consistent with sound security practices, in the design, implementation, and use of public-key based signature systems.

Other algorithms approved for inclusion shall be either: (1) Freely available or (2) available under terms consistent with the American National Standards Institute (ANSI) patent policy.

The Administration policy is that cryptographic keys used by Federal agencies for encryption (i.e., to protect the confidentiality of information) shall be recoverable through an agency or third-party process and that keys used for digital

signature (i.e., for integrity and authentication of information) shall not be recoverable.⁵³²

The text shows that NIST sought digital signature solutions that would provide users with “greater flexibility, consistent with sound security practices.” Looking toward the private sector for help, NIST modified its previous restriction on using private sector algorithms from accepting only “[f]reely available” algorithms to accepting commercial standards sanctioned by the American National Standards Institute (ANSI). As ANSI normally registers government and commercial encryption standards used in the banking and finance industries, the text demonstrates that NIST was committed to using standards from the private sector. However, the text contained vestiges of encryption control as shown by the statement: “[C]ryptographic keys used by Federal agencies for encryption (i.e., to protect the confidentiality of information) shall be recoverable.” Liberalization pressure by encryption users tested the seriousness of this statement.

Actions by users in other federal agencies showed that the government sector was reliant upon the private sector for encryption solutions and that the encryption control statement found in the DSS notice was largely ceremonial. In 1998, user and compatibility requirements forced the Social Security Administration (SSA) to issue a waiver for the use of private sector encryption products:

⁵³² U.S. Department of Commerce, National Institute of Standards and Technology, "Announcing Plans to Revise Federal Information Processing Standard 186, Digital Signature Standard," *Federal Register* 62, no. 92 (13 May 1997): 26293.

SUMMARY: The Chief Information Officer of the Social Security Administration grants to SSA a waiver from the use of the following Federal Information Processing Standards (FIPS):

1. The Secure Hashing Standard (FIPS 180-1);
2. The Digital Signature Standard (FIPS 186); and
3. The Data Encryption Standard (FIPS 46-2).

This waiver is granted pursuant to authority granted to the Secretary of Commerce by 40 U.S.C. section 1441, and delegated to the Commissioner of Social Security in the above referenced FIPS Publications. This authority was redelegated by the Commissioner of Social Security to the Agency's Chief Information Officer. This waiver is granted to allow SSA to use commercial off-the-shelf cryptographic products such as those produced by RSA Data Security, Inc., in lieu of products conforming with the above-cited FIPS.⁵³³

The text shows that SSA selected to use “commercial off-the-shelf cryptographic products” instead of products based on government standards, such as the “Digital Signature Standard.” This decision represented an endorsement of private sector technology leadership over the once dominant government leadership. In addition, the text implies that SSA perceived higher utility in commercial products, such as “those produced by RSA Data Security” and lower utility in products based on the government’s original Digital Signature Standard. The Environmental Protection Agency joined SSA in granting waivers to use private sector software that did not incorporate government encryption standards.⁵³⁴ This internal erosion of support from large government agencies drove NIST’s efforts to improve their Digital Signature Standard by dropping burdensome government restrictions on the encryption capabilities of the candidate algorithms.

⁵³³ U.S. Social Security Administration, “The Chief Information Officer of the Social Security Administration Grants to the Social Security Administration a Waiver From the Use of Certain Federal Information Processing Standards,” *Federal Register* 63, no. 108 (5 June 1998): 30794.

⁵³⁴ U.S. Environmental Protection Agency, “Federal Information [Processing Standards] Publications (FIPs) [FIPS Pub] Waiver,” *Federal Register* 63, no. 190 (1 October 1998): 52693.

The 2000 publication of the final revised Digital Signature Standard, FIPS 186-2, showed that NIST accepted and incorporated commercial algorithms into a government standard:

Cross Index:

- a. FIPS PUB 46-3, Data Encryption Standard.
- b. FIPS PUB 73, Guidelines for Security of Computer Applications.
- c. FIPS PUB 140-1, Security Requirements for Cryptographic Modules.
- d. FIPS PUB 171, Key Management Using ANSI X9.17.
- e. FIPS PUB 180-1, Secure Hash Standard.
- f. ANSI X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).
- g. ANSI X9.62-1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).⁵³⁵

The text shows the incorporation of “Reversible Public Key Cryptography” and the “Elliptic Curve Digital Signature Algorithm” as acceptable digital signature algorithms. The term reversible public key cryptography referred to the commercial RSA public key encryption scheme that was dominant in the private sector and in major parts of the non-defense government sector. Following this success of using commercial standards, NIST was not about to lose United States dominance in the secret key encryption area when it replaced DES.

In a late start to replace DES, NIST solicited public submissions for candidate encryption algorithms that could become the Advanced Encryption Standard. A 1997 *Federal Register* notice displayed the rationale for a competition open to the public:

⁵³⁵ U.S. Department of Commerce, National Institute of Standards and Technology, Digital Signature Standard, Federal Information Processing Standards Publication 186-2 (Washington, D.C., 27 January 2000), 3-4.

It is intended that the AES will specify an unclassified, publicly disclosed encryption algorithm available royalty-free worldwide that is capable of protecting sensitive government information well into the next century.

The purpose of this notice is to solicit candidate algorithms from the public, academic/research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. Following the close of the submission period, NIST intends to make all submissions publicly available for review and comment.⁵³⁶

The text shows that NIST desired a “publicly disclosed encryption algorithm available royalty-free worldwide.” Although this notice solicited algorithms from all sources, the more probable sources of such submissions were thought to be from academia and the government sector, as presumably information technology companies would want compensation for their valuable products. However, the United States government did not submit an algorithm and the private sector produced all the candidate algorithms, as was shown in the Encryption Technology Group analysis.

Evidence that the lead actor was not from the government sector came from an examination of the submitted AES candidates. A 2000 report by NIST showed that no candidates came from government sources:

On August 20, 1998, NIST announced fifteen AES candidate algorithms at the First AES Candidate Conference (AES1) and solicited public comments on the candidates [33]. Industry and academia submitters from twelve countries proposed the fifteen algorithms. A Second AES Candidate Conference (AES2) was held in March 1999 to discuss the results of the analysis that was conducted by the international cryptographic community on the candidate algorithms. In August 1999, NIST announced its selection of five finalist algorithms from the

⁵³⁶ U.S. Department of Commerce, National Institute of Standards and Technology, "Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard," *Federal Register* 62, no. 177 (12 September 1997): 48051.

fifteen candidates. The selected algorithms were MARS, RC6™, Rijndael, Serpent and Twofish.⁵³⁷

The text indicates that the United States government did not have the technical leadership or motivation to submit its own design: “Industry and academia submitters from twelve countries proposed the fifteen algorithms.” The government could have submitted an improved version of its 80-bit SKIPJACK algorithm used in the Escrowed Encryption Standard but did not do so. NIST appeared satisfied in managing an effort to down-select private sector submissions in a rational manner until a final candidate remained.

On October 2, 2000, Mr. Norman Y. Mineta, the Secretary of Commerce, announced NIST’s selection of the Rijndael algorithm as the new AES. The press announcement described the roles of the government and private sectors in the development process:

Mineta named the Rijndael (pronounced Rhine-doll) data encryption formula as the winner of a three-year competition involving some of the world's leading cryptographers.

“Once final, this standard will serve as a critical computer security tool supporting the rapid growth of electronic commerce,” Mineta said. “This is a very significant step toward creating a more secure digital economy. It will allow e-commerce and e-government to flourish safely, creating new opportunities for all Americans,” he said.

Computer scientists at the National Institute of Standards and Technology, an agency of the Commerce Department's Technology Administration, organized the international competition in a drive to develop a strong information encryption

⁵³⁷ James Nechvatal, et al., *Report on the Development of the Advanced Encryption Standard* 2 October 2000 (Washington, D.C.: NIST, 2000), 7. Note that the reference numbers are in brackets and do not signify added material.

formula to protect sensitive information in federal computer systems. Many businesses are expected to use the AES as well.⁵³⁸

The text shows that NIST's development effort relied upon the efforts "of the world's leading cryptographers." In addition, the text shows that NIST's role in the actual development effort was not organic research and development, but involved organizing an "international competition in a drive to develop a strong information encryption formula to protect sensitive information in federal computer systems." Thus, the technology leadership behind AES did not rest with the federal government, but with academia, corporations, and private individuals from around the globe. The motivation behind the private sector's participation in the competition was indicated in the statement: "Many businesses are expected to use the AES as well." Actors in the Government Agencies Group anticipated that commercial gain from encryption services endorsed by the use of a new government encryption standard was a desired product of this competition. The network effects of using AES would benefit both the private and government sectors.

The actions of the Government Agencies Group matched Allison's RAM organizing concept of "Action as Rational Choice," whereby the "rational agent selects the alternative whose consequences rank highest."⁵³⁹ In the revised Digital Signature Standard and Advanced Encryption Standard cases, NIST allowed the private sector to use its technology leadership to develop solutions to the information security problem for

⁵³⁸ U.S. Department of Commerce, "Commerce Department Announces Winner of Global Information Security Competition," G 2000-176, (Washington D.C., 02 October 2000).

⁵³⁹ Allison and Zelikow, *Essence of Decision*, 24.

both the private and non-defense government sectors. In the DSS case, NIST acted as a facilitator and presented to the user one government and two private sector alternatives. In the AES case, NIST presented to the user the best alternative submitted from the private sector. Actors in the Government Agencies Group did not submit a government algorithm for the AES competition because of the technical limitations of available algorithms and NSA policy. I assigned a Lead Actor valance of "0" to the Government Agencies Group for effectively allowing the private sector to take the technology lead in providing encryption solutions and for not distorting the competitive process with regulations or government developed encryption control solutions.

B. Problem Perception Valance

Actors in the Government Agencies Group perceived a simple information security problem that primarily affected users in the private sector and the non-defense federal sector and did not use information access requirements as a driver. During the Status Quo Period, Federal Information Processing Standards cited regulations that limited the export of encryption products to certain countries. However, the citations of government regulations were in deference to the executive branch and practically meaningless, as all the encryption algorithms incorporated into FIPS were in the public domain or were of foreign origin. PDD/NSC-63 gave general directions that outlined and simplified the information infrastructure protection problem:

The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being

of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, providing information upon which choices can be made by the private sector.⁵⁴⁰

The text shows that actors in the Government Agencies Group were directed to use the “incentives that the market provides” first in order to solve the infrastructure protection problem. In addition, the text shows that government regulations would be used as a last resort and “only in the face of a material failure of the market to protect the health, safety or well-being of the American people.” Thus, NIST first focused on using market solutions to solve a domestic problem.

NIST believed that the information security problem was exacerbated by a loss of trust in government encryption standards, such as in the EES case, and that other government agencies would find commercial solutions to this problem. NIST attempted to restore government trust by selecting the best encryption algorithms from the private sector to become the next government standards. Such an approach did not consider the complexities presented by the political and international aspects of encryption control. However, actions by peer government agencies reinforced NIST’s perception that it had to solve a simple domestic problem or become irrelevant to the information infrastructure protection effort. During the update process for the Digital Signature Standard, FIPS 186, other federal agencies made NIST aware that the domestic information security problem was their paramount concern. The Social Security Administration (SSA), being

⁵⁴⁰ William J. Clinton, Presidential Decision Directive / NSC-63, “Critical Infrastructure Protection,” 22 May 1998: 4.

responsible for over two hundred million accounts, was concerned about using government encryption standards for Internet security:

SSA has found that an increasingly large number of its customers prefer to work with the Agency directly through Internet services. To effectively serve them, SSA must use commercially accepted and available off-the-shelf products. The above referenced FIPS [DSS and others] provide for the use of products which have not gained wide acceptance commercially, and these standards are not incorporated in commercial off-the-shelf products. Notably, the Internet Browsers published by MICROSOFT and NETSCAPE, together representing 93% of the publicly used browsers, do not use the algorithms published in the referenced FIPS.

The text shows that the Federal Information Processing Standard for the Digital Signature Algorithm had “not gained wide acceptance commercially.” In addition, the text suggests that information security solutions built into existing software products should have been the drivers for encryption standards. SSA sought to fix this problem by obtaining a waiver to use commercial products, and the EPA sought a similar waiver.⁵⁴¹

Waivers demonstrated the need for better information security tools and affected NIST’s decisions. The response by NIST was to complete the update of FIPS 186 by incorporating commercial public key encryption standards being sought by the SSA and EPA. The update, FIPS 186-2, used the government’s Digital Signature Algorithm, tried a new commercial Elliptic Curve algorithm, and added the popular commercial RSA public key encryption algorithm. As all three algorithms are encryption capable, FIPS

⁵⁴¹ U.S. Environmental Protection Agency, “Federal Information [Processing Standards] Publications (FIPs) [FIPS Pub] Waiver,” *Federal Register* 63, no. 190 (1 October 1998): 52693.

186-2 could have created a complex problem by interfering with information access requirements.

A section within FIPS 186-2 cites the applicable regulations on export control of encryption products and lends support to the idea that NIST perceived and solved a complex problem. However, NIST knew that export controls were political and procedural actions and did little to guarantee United States government access to encrypted information:

Export Control: Certain cryptographic devices and technical data regarding them are subject to Federal export controls. Applicable Federal government export controls are specified in Title 15, Code of Federal Regulations (CFR) Part 740.17; Title 15, CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.⁵⁴²

The text shows that three parts of Title 15, Code of Federal Regulations, controlled the export of public key encryption products from the United States. This appearance of regulatory control on products incorporating public key encryption algorithms was a political façade. The algorithms used in FIPS 186-2 were globally available and already incorporated into commercial and public domain software. The 2001 Advanced Encryption Standard, FIPS-197, continued this façade with more ambiguous language:

11. Export Control. Certain cryptographic devices and technical data regarding them are subject to Federal export controls. Exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the Bureau of Export Administration of the U.S. Department of Commerce. Applicable Federal government export

⁵⁴² U.S. Department of Commerce, National Institute of Standards and Technology, Digital Signature Standard, Federal Information Processing Standards Publication 186-2 (Washington, D.C., 27 January 2000), 3.

controls are specified in Title 15, Code of Federal Regulations (CFR) Part 740.17; Title 15, CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.⁵⁴³

The text claims, “Certain cryptographic devices and technical data regarding them are subject to Federal export controls.” As these “devices” and “technical data” included the Belgian Rijndael encryption algorithm, the application of export regulations to an algorithm developed overseas suggests a ceremonial attempt at encryption control. Export regulations and guaranteed information access requirements did not drive the decisions of NIST, because these considerations were not relevant to NIST’s management process that used encryption algorithms from academia, foreign countries, and the private sector. Thus, in the Status Quo Period, NIST had the same simple problem perception as did actors in the private sector. Actions by other actors in the Government Agencies Group reinforced this perception of a simple problem.

Up until to the Status Quo Period, the National Security Agency openly championed balanced information security and access requirements. In 1998, PDD/NSC-63 explicitly tasked the National Security Agency to concentrate its efforts on the protection of the critical information infrastructure within the federal government sector:

The NSA, in accordance with its National Manager responsibilities in NSD 42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability

⁵⁴³ U.S. Department of Commerce, National Institute of Standards and Technology, Announcing the Advanced Encryption Standard, Federal Information Processing Standards Publication 197 (Washington, D.C., 26 November 2001), *ii*.

information; establish standards; conduct research and development; and conduct [and] issue security product evaluations.⁵⁴⁴

The text indicates that PDD/NSC-63 directed NSA's attention toward protecting "U.S. Government systems" and presumably away from protecting systems in the private sector. This single sector focus permitted NSA to have its version of a simple problem, but with the potential of overlapping responsibilities with NIST. The PDD/NSC-63 phrase directing NSA to "establish standards" kept NSA in the development loop for Federal Information Processing Standards. This direction was inconsistent with the *Computer Security Act of 1987*, which specified that NSA was to provide technical assistance to NIST.

Actions by NSA showed that it learned to minimize the complicated aspects of the domestic encryption control problem by staying away from direct involvement with encryption standards used in the private and non-defense federal government sectors. In assisting NIST, NSA did not submit any of its national security encryption algorithms for use in the AES competition. In 1998, NSA took further action by declassifying the algorithms used in the controversial Escrowed Encryption Standard:

The National Security Agency today announced a decision to declassify both the Key Exchange Algorithm (KEA) and the SKIPJACK encryption algorithm. Both algorithms are used in the FORTEZZA PC card for key

⁵⁴⁴ William J. Clinton, Presidential Decision Directive / NSC-63, "Critical Infrastructure Protection," 22 May 1998: 18.

exchange and general purpose encryption, respectively, and the Escrowed Encryption Standard (FIPS 185) calls for the use of SKIPJACK.⁵⁴⁵

The text reveals that the secretive hardware internals of the Escrowed Encryption Standard were a public key encryption subsystem to exchange keys and the SKIPJACK secret key encryption subsystem that performed the data encryption. Once revealed, the key escrow features that satisfied national security and public safety requirements were made obsolete and the whole concept of government controlled encryption hardware was retired as well. Software engineers could now build "FORTEZZA" card equivalents that would not surrender their encryption keys to the federal government or any other escrow agent. With the government's key escrow concept dead, the information access problem in the private sector could only be solved by the market and by requirements from users.

The Department of Defense gave further direction to NSA on its new area of concentration, which was information assurance (IA) for the department using a public key infrastructure (PKI) system. PKI allows IA, as the Department of Defense certificate authority is NSA. NSA has access to the encryption keys required to perform counterintelligence and security countermeasure functions. This narrow focus simplified the information security and access problems for NSA, as market forces and privacy concerns were secondary to security considerations within the DOD. In an April 1999 directive, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Mr. Arthur L. Money, assigned "program management responsibility for

⁵⁴⁵ U.S. Department of Defense, National Security Agency, "Press Release: NSA Releases FORTEZZA Algorithms," (Washington D.C., 24 June 1998).

the DoD PKI to the National Security Agency.”⁵⁴⁶ Thus in the Status Quo Period, NIST and NSA were satisfied that PKI technology solutions could transform a complex multifaceted problem into a simple one. The use of strong encryption would ensure information security, and certificate authorities could now allow access to protected information.

The actions of the Government Agencies Group matched Allison’s RAM general proposition of a “Unified National Actor” that acts as a “unitary decision maker.”⁵⁴⁷ NIST and NSA took similar actions regarding the use of secret and public key encryption solutions for their PDD/NSC-63 directed responsibilities. The previous need to resolve the complex relationships among information security, export control, and information access requirements were politically driven perceptions accepted by NIST and NSA. However, private and government sector successes with the Public Key Infrastructure changed the problem perceptions of NIST and NSA. Both now perceived the value of market-based information security solutions, as made apparent by the growing demand for private sector solutions. I assigned a Problem Perception valance of “0” to the Government Agencies Group for perceiving a problem made simple by the availability of private sector information security solutions.

⁵⁴⁶ Arthur L. Money, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, “Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI),” Washington, D.C., 9 April 1999.

⁵⁴⁷ Allison and Zelikow, *Essence of Decision*, 25.

C. Favored Alternative Valance

Actors in the Government Agencies Group favored utility maximizing alternatives over laws, regulations, or standards. The security of electronic-commerce and electronic-government transactions depended upon cost effective and trustworthy encryption systems and not on government directed implementations, such as restricting algorithm flexibility or requiring tamper-resistant hardware. In order to offer utility maximizing systems, these actors had to overcome two legacies of the Competitive Period which were the government directed Digital Signature Standard and the Escrowed Encryption Standard. In both these standards, actors in the Government Agencies Group made restrictive development choices that set the level of information security to be commensurate with information access requirements. At the beginning of the Status Quo Period, other government agencies and the private sector demanded alternatives in which customers could select their desired level of information security and the extent of information access by other parties. In June 1998, the Social Security Administration became the largest group of users expressing its choice of encryption products by asking for a government standards waiver:

The Agency's Chief Information Officer has determined that compliance with the referenced FIPS would adversely affect the accomplishment of the mission of the SSA and accordingly has granted a waiver from the use of the referenced FIPS.

SSA has a customer base of over 260,000,000 people, including individuals, businesses, small employers, organizations, and other Federal, State, and local government agencies. To accomplish the mission of serving these customers cost

effectively, SSA is pursuing the use of electronic service delivery technologies, including the Internet.⁵⁴⁸

In the text, the SSA believed that Federal Information Processing Standards “adversely affected the accomplishment of [its] mission” and that a FIPS waiver was the better method for ensuring encryption product choice. The SSA strengthened their waiver rationale with claims that it had “a customer base of over 260,000,000 people” and that it had a “mission of serving these customers cost effectively.” The issuance of waivers and the perception of substandard or suboptimal FIPS forced NIST to change the definition of a FIPS and the timing of the update process.

The first NIST response to the demand for a variety of better choices was the interim Digital Signature Standard, FIPS 186-1. In a December 1998 *Federal Register Notice*, NIST demonstrated that it had anticipated the demand for encryption choices:

On May 13, 1997, NIST published a Federal Register notice soliciting comments on amending FIPS 186 to allow for the use of other techniques, specifically mentioning RSA and elliptic curve (but not with detailed specifications as now exist for RSA in the ANSI X9.31 standard). The public comments overwhelmingly supported revising FIPS 186 to include these additional algorithms. RSA, which has withstood widespread scrutiny by the cryptographic research community, is available in many commercial products. NIST believes it to be robust and sufficiently strong for use by federal agencies.⁵⁴⁹

⁵⁴⁸ U.S. Social Security Administration, “The Chief Information Officer of the Social Security Administration Grants to the Social Security Administration a Waiver From the Use of Certain Federal Information Processing Standards,” *Federal Register* 63, no. 108 (5 June 1998): 30794-5.

⁵⁴⁹ U.S. Department of Commerce, National Institute of Standards and Technology, “Announcing Approval of Federal Information Processing Standard 186-1, Digital Signature Standard,” *Federal Register* 63, no. 240 (15 December 1998): 69050.

The text uses the phrase “amending FIPS 186 to allow for the use of other techniques” to show that NIST had changed the definition of a Federal Information Processing Standard to now include “additional algorithms” or choices. The idea of standardized choices was a rational attempt by NIST to offer the more popular and flexible RSA public key encryption algorithm as a replacement for the government’s Digital Signature Algorithm. In addition, the text shows that NIST attempted to mitigate government capitulation to RSA Security and its proprietary algorithms by including less mature “elliptic curve” algorithms that did not have existing “detailed specifications.” Offering a new and uncertain encryption algorithm as a choice was not a trust building or a utility maximizing decision, but served to accentuate the idea of permitting customers to make decisions.

The 2000 final version of the Digital Signature Standard, FIPS 186-2, was unique in that NIST passed the encryption choices on to system developers and ultimately on to encryption users. The precedent of offering choices to encryption developers and users had issues as shown by the text:

Applications: A digital signature (ds) algorithm authenticates the integrity of the signed data and the identity of the signatory. A ds algorithm may also be used in proving to a third party that data was actually signed by the generator of the signature. A ds algorithm is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. The techniques specified in ANSI X9.31 and ANSI X9.62 may be used in addition to the Digital Signature Algorithm (DSA) specified herein. (NIST

editorial note: either DSA, RSA [ANSI X9.31], or ECDSA [ANSI X9.62] may be used; all three do not have to be implemented.)⁵⁵⁰

The text lists the uses of digital signatures and specifies, “ANSI X9.31 [RSA] and ANSI X9.62 [elliptic curve] may be used in addition to the Digital Signature Algorithm (DSA).” The issue with three possible standards becomes the cost effectiveness of having to implement all three in encryption software. The guidance phrase found in the text, “all three do not have to be implemented,” does not suggest the optimal choice.

From the waivers discussed earlier, NIST should have recommended the RSA algorithm. A possible explanation for the presentation of choices and not a single standard was the patent status of the RSA algorithm. As noted earlier, the United States Patent and Trademark Office awarded the inventors of the RSA algorithm patent 4,405,829 in September 1977. Seventeen years later, actors in the Encryption Technology Group web-blogged the expiration of the RSA patent in September 2000:

The end of the patent means that companies who want to use the RSA encryption algorithm in the United States no longer have to license it from the firm, RSA Security. The patent hasn't extended to products sold outside the United States, because the algorithm was published in 1977 before the Massachusetts Institute of Technology applied for its patent.⁵⁵¹

The text indicates that NIST could not make the RSA algorithm the sole standard for digital signatures because of its proprietary nature. The government's Digital Signature

⁵⁵⁰ U.S. Department of Commerce, National Institute of Standards and Technology, Digital Signature Standard, Federal Information Processing Standards Publication 186-2, (Washington, D.C., 27 January 2000), 2-3. Bracketed material is in the original.

⁵⁵¹ David Sims, “Public Domain RSA,” LinuxDevCenter.com, 08 September 2000, <<http://www.linuxdevcenter.com/pub/a/linux/2000/09/08/rsa.html>>, accessed on 16 October 2004.

Algorithm suffered a similar limitation as Public Key Partners used a patent infringement claim to force NIST into surrendering its rights to DSA. NIST learned from these experiences when it started the process to replaced the Data Encryption Standard.

The competitive development of the Advanced Encryption Standard as a replacement for DES relied on finding the utility maximizing solution among the fifteen submissions. Although the competition was open to all sectors, only academia and the private sector submitted candidate algorithms. In September 1997, NIST placed a notice in the *Federal Register* in order to “solicit candidate algorithms from the public, academic/research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations.”⁵⁵² NIST did not submit its 112-bit Triple DES algorithm and NSA did not submit its 80-bit SKIPJACK algorithm because newer and more efficient algorithms were available from the private sector. In contrast to the competitive advantages presented by newer algorithms, NSA’s SKIPJACK algorithm did not meet the minimum AES encryption strength, which meant that SKIPJACK required modifications.⁵⁵³ NSA released SKIPJACK into the public domain for potential modifications in June 1998, which was after the AES candidate submission deadline. Thus, the selection team did not consider encryption algorithms from the United States government.

⁵⁵² U.S. Department of Commerce, National Institute of Standards and Technology, “Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard,” *Federal Register* 62, no. 177 (12 September 1997): 48051.

⁵⁵³ *Ibid.*

NIST began the selection process to find the AES winner by using two selection rounds to find the utility maximizing solution. NIST used an open selection process, solicited public comments, and published the selection criteria in the *Federal Register*:

II. Comments Solicited on AES Candidate [Candidate]Algorithms

Written comments on the candidate algorithms are solicited by NIST in this “Round 1” technical evaluation in order to help NIST reduce the field of AES candidates to five or fewer for the “Round 2” technical analysis. It is envisioned that this narrowing will primarily be based on security, efficiency, and intellectual property considerations. Comments are specifically sought on: (1) specific security, efficiency, intellectual property, and other aspects of individual AES candidate algorithms; and, (2) cross-cutting analyses of all candidates.⁵⁵⁴

The text shows that NIST envisioned a two-stage selection process and the NIST was interested in “[w]ritten comments on the candidate algorithms.” This solicitation of public comments gave encryption system developers and users a significant voice in the selection of the AES. In addition, the text shows that the measures of encryption utility would be “based on security, efficiency, and intellectual property considerations.” Thus in selecting candidates, information security considerations had significant merit, while information access considerations for public safety and national security purposes were irrelevant or indicated that the algorithm had security weaknesses.

Actions taken by NIST to overcome impediments in the AES selection process demonstrated a commitment to selecting the best algorithm. In February 2001, NIST published a notice in the *Federal Register* soliciting comments on the proposed AES

⁵⁵⁴ U.S. Department of Commerce, National Institute of Standards and Technology, “Request for Comments on Candidate Algorithms for the Advanced Encryption Standard (AES),” *Federal Register* 63, no. 177 (12 September 1998): 49092.

Federal Information Processing Standard.⁵⁵⁵ In doing so, NIST received comments from “21 private sector organizations, individuals, and groups of individuals, and from one federal government organization.”⁵⁵⁶ NIST responded to these comments in December 2001. The proximity of the response date to the events of September 11, 2001 gave NIST the opportunity to cancel the AES development process for reasons of national security and public safety:

Comment: One comment recommended the selections [selection] of a different algorithm, one that had not been submitted during the AES development process.

Response: NIST conducted an open process to solicit and evaluate algorithms for consideration for the AES. All candidate algorithms have been thoroughly reviewed and analyzed by the international cryptographic community.⁵⁵⁷

The text shows that at least one actor did not want the Rijndael algorithm to become the AES. While the text does not contain the reason for this last-minute protest, the existence of such protests demonstrated that the national security establishment could have interjected demands for an encryption algorithm that would provide information access in a time of national peril. The response, “NIST conducted an open process to solicit and evaluate algorithms for consideration for the AES,” demonstrated NIST’s confidence in its selection process and its use of rational evaluation criteria. Any post-September 11,

⁵⁵⁵ U.S. Department of Commerce, National Institute of Standards and Technology, "Announcing Draft Federal Information Processing Standard (FIPS) for the Advanced Encryption Standard (AES) and Request for Comments," *Federal Register* 66, no. 40 (28 February 2001): 12762-3.

⁵⁵⁶ U.S. Department of Commerce, National Institute of Standards and Technology, "Announcing Approval of Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES)," *Federal Register* 66, no. 235 (06 December 2001): 63370.

⁵⁵⁷ *Ibid.*

2001 acquiescence by NIST to information control measures would have taken an inordinate amount of political effort. Analyses of the Congressional and Executive Groups showed that political consensus for information access requirements did not materialize.

The favoring of public key encryption choices for users and a utility maximizing secret key encryption solution by actors in the Government Agencies Group matched Allison's RAM general proposition that that increasing the utility value of a solution "increases the likelihood of that action being chosen."⁵⁵⁸ The main actor in this group was NIST, who attempted to restore trust and value in government encryption standards. During the Status Quo Period, both private and government sector encryption users perceived that encryption systems free of government constraints were utility maximizing solutions to the information security problem. Cost and benefit considerations on information access that satisfied public safety and national security requirements did not overtly enter the utility equation. Thus, commercial public key encryption subsystems and a competitively developed secret key encryption subsystem were the utility maximizing solutions offered by NIST. I assigned a Favored Alternative valance of "0" to the Government Agencies Group for offering utility maximizing solutions to solve the information security problem.

⁵⁵⁸ Allison and Zelikow, *Essence of Decision*, 25.

D. Decision Timing Valance

Actors in the Government Agencies Group perceived that the availability of encryption choices and the advancement of encryption technology were the main factors driving decisions. During this period, private sector alternatives replaced the government specified choices found in the Digital Signature Standard and the Escrowed Encryption Standard. Technical issues and procedures; such as documentation, public notification, and testing; may have delayed the revision of the DSS and the completion of the Advanced Encryption Standard. However, waiver activities by other federal agencies forced NIST into action. To prevent crisis action decisions, NIST relied on an interim Digital Signature Standard and suggested the use of Triple DES as an interim solution for the aging DES. NIST's first action was to expand its public key encryption choices.

Although NIST publicly advertised a revision for its restrictive Digital Signature Standard in 1997, the issuance of the revised DSS occurred after the Social Security Administration and the Environmental Protection Agency submitted waivers to use the commercial RSA public key encryption subsystem for digital signatures. The supposition that these waivers influenced NIST's decision timing was confirmed in a December 1998 *Federal Register* notice that announced the upgraded Digital Signature Standard, FIPS 186-1.

Recently, another technique, known as RSA, was approved as the X9.31 standard [*X9.31-1998 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*] by ANSI. A second standard, based upon a technique known as elliptic curve, is expected to be completed and

approved by ANSI in the near future. Agencies have expressed considerable interest to NIST in using these technologies.⁵⁵⁹

The text shows that other actors had “expressed considerable interest to NIST in using these technologies.” Although stated as an “interest,” the SSA and EPA already had waivers to use RSA as their digital signature algorithm. Figure 4-9 shows that the release of FIPS 186-1 followed the 1998 waivers by a few months, even though the 1997 update notice shows the NIST had time to change DSS on its own accord in order to prevent these waivers.

The decision to incorporate RSA as part of the revised Digital Signature Standard was based on user requirements and the availability of a suitable standard for this algorithm. The timing of such a decision should not be viewed as a tacit change in response to the information security problem, but as a decision contingent upon approval of an American National Standards Institute (ANSI) standard. The text shows that NIST waited for ANSI’s approval of RSA for digital signatures, and this approval happened in September 1998.⁵⁶⁰ NIST did not wait for ANSI’s January 1999 approval of an elliptic curve standard because there were no pressing waivers to use this standard.⁵⁶¹

⁵⁵⁹ U.S. Department of Commerce, National Institute of Standards and Technology, “Announcing Approval of Federal Information Processing Standard 186-1, Digital Signature Standard,” *Federal Register* 63, no. 240 (15 December 1998): 69050.

⁵⁶⁰ American National Standard Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998 (New York: American National Standards Institute Inc., 8 September 1998).

⁵⁶¹ American National Standard Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62-1999 (New York: American National Standards Institute Inc., 7 January 1999).

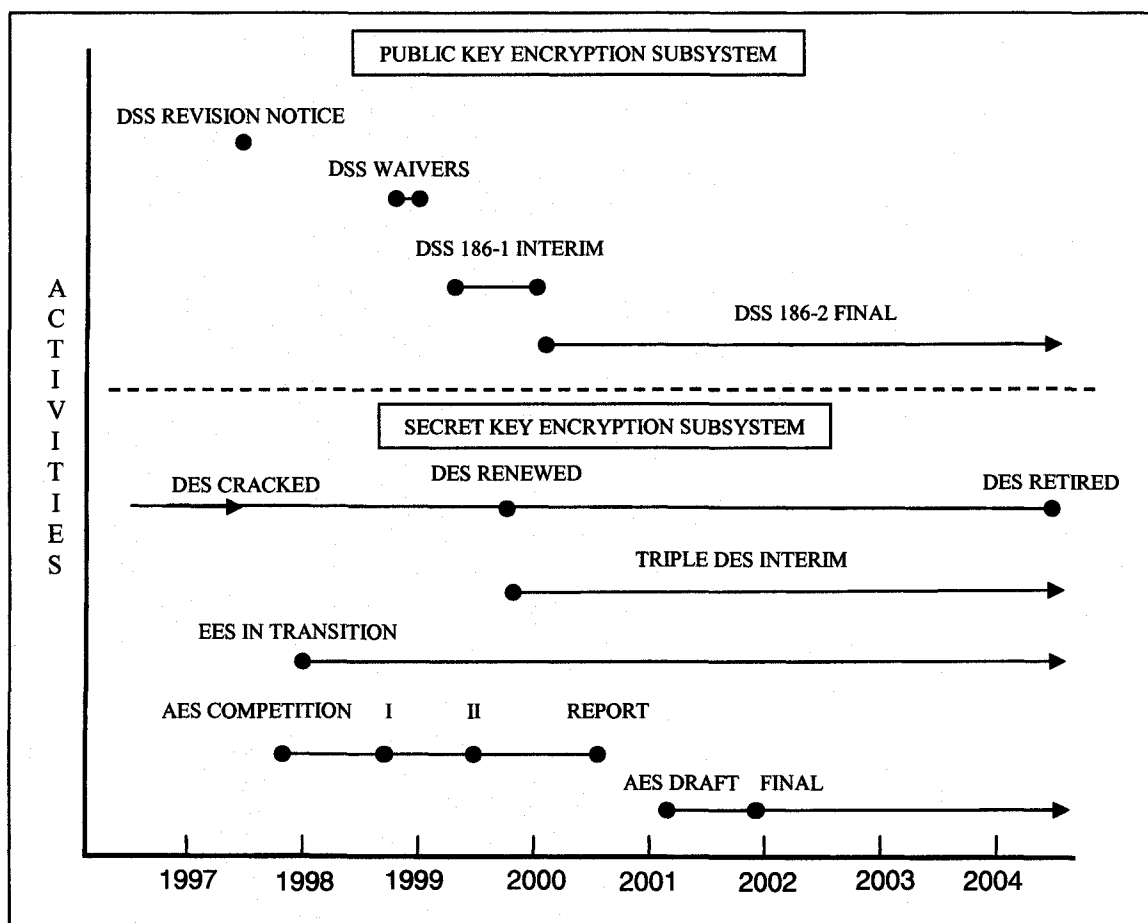


Figure 4-9 Timeline of key activities leading up to the publication of the DSS FIPS Pub 186-2 and AES FIPS Pub 197

Figure 4-9 shows that NIST published the final Digital Signature Standard, FIPS 186-2, in early 2000. This date allowed NIST ample time to incorporate another ANSI digital signature standard, which was the elliptic curve digital signature algorithm. The final Digital Signature Standard contained the sentence: “The techniques specified in ANSI X9.31 and ANSI X9.62 may be used in addition to the Digital Signature Algorithm

(DSA) specified herein.”⁵⁶² Thus, the final FIPS 186-2 was contingent on “ANSI X9.31 and ANSI X9.62,” which were ANSI’s RSA and elliptic curve digital signature standards, respectively.

NIST’s decision to replace the Data Encryption Standard with the Advanced Encryption Standard demonstrated that NIST had the time to make utility maximizing decisions and was not acting in a time crisis mode. RSA Security’s June 1997 DES cracking media event demonstrated the requirement for a new secret key encryption algorithm, but did not generate a panic among users of DES. While subsequent DES cracking efforts and successes supported the claim that the government “kept industry and the public mislead about DES’s security,” NIST’s counteraction to this negative publicity was to recommend Triple DES until the AES was completed.⁵⁶³ In a 1999 *Federal Register* notice, NIST announced that DES would be renewed in FIPS 46-3 for another five years:

Since 1998, there have been reports that the DES could be attacked through an exhaustion attack whereby possible keys are tested one at a time until the correct key is found. Because of this, NIST proposed to replace FIPS 46-2 with FIPS 46-3 to specify use of Triple DES. Triple DES was documented and specified as an American National Standard (ANSI X9.52) by Accredited Standards Committee X9 for Financial Services, which develops cryptography and public key infrastructure standards. Triple DES was developed by the private

⁵⁶² U.S. Department of Commerce, National Institute of Standards and Technology, Digital Signature Standard, Federal Information Processing Standards Publication 186-2, (Washington, D.C., 27 January 2000), 3.

⁵⁶³ Electronic Frontier Foundation, *Cracking DES*, page 1-5.

sector with NIST assistance and is used by many government and private sector organizations, particularly in the financial services industry.⁵⁶⁴

The text shows that NIST was cognizant of these DES cracking efforts and was confident in Triple DES by citing the “American National Standard (ANSI X9.52)” certification of this algorithm for use in the “the financial services industry.” The availability of a proven secret key choice allowed NIST time for its planned AES competition. Figure 4-9 shows the timing of the DES cracking event and NIST’s Triple DES response.

Both NSA’s decision to withdraw from the development of encryption standards and NIST’s decision timing behind the development of the Advanced Encryption Standard showed that the Government Agencies Group could develop and offer utility maximizing encryption choices to users. In 1998, NSA declassified the details behind its KEA and SKIPJACK algorithms, both of which made the Escrowed Encryption Standard a complete encryption system. NSA’s press release on this event indicated that NSA viewed AES as the future secret key encryption subsystem:

The declassification of these algorithms is not intended to make them candidates for the Advanced Encryption Standard (AES) competition. NSA plans to support and use the eventual winner of that competition in appropriate DoD applications when it becomes available. Software FORTEZZA is a transition vehicle in migrating to AES based commercial security solutions for the Defense Information Infrastructure.⁵⁶⁵

⁵⁶⁴ U.S. Department of Commerce, National Institute of Standards and Technology, “Announcing Approval of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard,” *Federal Register* 69, no. 214 (05 November 1999): 60425.

⁵⁶⁵ U.S. Department of Defense, National Security Agency, “Press Release: NSA Releases FORTEZZA Algorithms,” 24 June 1998.

The text shows that NSA was not going to participate in the AES competition and that NSA viewed their FORTEZZA instantiation of EES as a “transition vehicle in migrating to AES.” NSA’s FORTEZZA release provided the private sector with a proven, but interim, encryption alternative. However, the \$100 cost and the expected short lifetime of this alternative limited the commercial market for FORTEZZA encryption products. Figure 4-10 shows such a card being commercially available. Most users would wait for a better alternative.

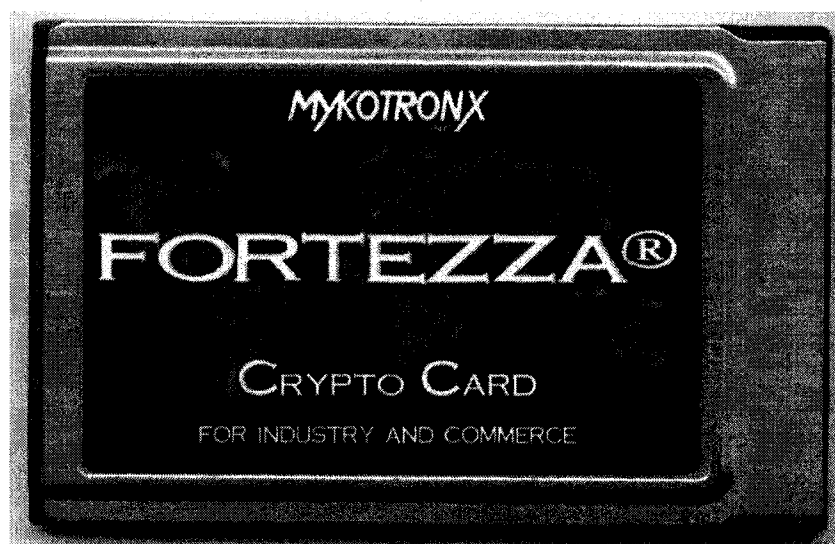


Figure 4-10 Author’s private FORTEZZA card purchased and used for software compatibility investigations

NIST took almost five years in the development of the Advanced Encryption Standard. NIST’s global AES competition required three years for the down-selection of candidate encryption algorithms and for the generation of the technical report. NIST’s

October 2000 report showed the timing and logic behind the selection of the Rijndael algorithm:

In 1997, the National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) Federal information in furtherance of NIST's statutory responsibilities. In 1998, NIST announced the acceptance of fifteen candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. This analysis included an initial examination of the security and efficiency characteristics for each algorithm. NIST reviewed the results of this preliminary research and selected MARS, RC6™, Rijndael, Serpent and Twofish as finalists. Having reviewed further public analysis of the finalists, NIST has decided to propose Rijndael as the Advanced Encryption Standard (AES). The research results and rationale for this selection are documented in this report.⁵⁶⁶

The text shows the down-selection pattern of accepting "fifteen candidate algorithms" in round one, selecting "MARS, RC6™, Rijndael, Serpent and Twofish" in round two, and Rijndael as the finalist. Figure 4-9 shows the timing for the AES competition and the issuance of NIST's report. This three-year period could have been shortened after round two if NIST had allowed multiple winners.

During the down selection process, a debate occurred on whether AES should specify a single utility maximizing choice or allow users to select what they perceived as the best algorithm. Offering users a choice, such as NIST did with the Digital Signature Standard, was rejected because NIST believed that it had considered all the decision variables:

⁵⁶⁶ James Nechvatal, et al., *Report on the Development of the Advanced Encryption Standard 2 October 2000* (Washington, D.C.: NIST, 2000), 1.

The team considered *all* of the comments and factors above before making the decision to propose only a single algorithm for the AES. The team felt that other FIPS-approved algorithms will provide a degree of systemic resiliency, and that a single AES algorithm will promote interoperability and address vendor concerns about intellectual property and implementation costs.⁵⁶⁷

The text shows that NIST had “other-FIPS approved algorithms,” namely Triple DES, to serve as a backup and that NIST believed “a single AES algorithm” would “promote interoperability and address vendor concerns about intellectual property and implementation costs.” NIST’s selection process and decision logic proved resilient enough to withstand the post-September 11, 2001 environment that called for increased government surveillance powers. In July 2004, NIST had enough confidence in AES to retire DES:

Future use of DES by Federal agencies is to be permitted only as a component function of the Triple Data Encryption Algorithm (TDEA). TDEA may be used for the protection of Federal information; however, NIST encourages agencies to implement the faster and stronger algorithm specified by FIPS 197, Advanced Encryption Standard (AES) instead.⁵⁶⁸

The text shows that DES could only be used as Triple DES and that agencies were encouraged to “implement the faster and stronger algorithm specified by FIPS 197, Advanced Encryption Standard (AES).” Thus in the Status Quo Period, NIST set encryption policy by creating a globally available secret key encryption algorithm to replace DES.

⁵⁶⁷ *Ibid.*, 15.

⁵⁶⁸ U.S. Department of Commerce, National Institute of Standards and Technology, “Announcing Proposed Withdrawal of Federal Information Processing Standard (FIPS) for the Data Encryption Standard (DES) and Request for Comments,” *Federal Register* 69, no. 142 (26 July 2004): 44509.

The actions of the Government Agencies Group matched Allison's RAM general proposition that increasing the utility value of a solution "increases the likelihood of that action being chosen."⁵⁶⁹ As the primary actor in the group during this period, NIST made decisions regarding public and secret key encryption solutions. NIST, feeling the pressure from federal agencies, modified the Digital Signature Standard to offer a choice of three algorithms. Users could then choose either the commercial RSA or elliptic curve algorithms over the DSA sponsored by the government. This choice increased the trust and perceived value of the solutions. In replacing DES as the secret key encryption standard, NIST used the availability of Triple DES to gain the time necessary for a competition among fifteen private sector algorithms. The selection of the Belgian Rijndael algorithm as the Advanced Encryption Standard produced a utility maximizing solution that was necessarily independent of export control restrictions. I assigned a Decision Timing valance of "0" to the Government Agencies Group for waiting on the availability of private sector choices and for competitively selecting the next secret key encryption subsystem.

Status Quo Period Summary

The four actor groups investigated during the Status Quo Period undertook actions that fit with the behaviors suggested by Allison's decision models. Table 4-3 summarizes these findings and shows that the actions of Congressional Group and the Executive Group followed patterns of behaviors that were in between those suggested by the

⁵⁶⁹ Allison and Zelikow, *Essence of Decision*, 25.

Organizational Behavior Model (OBM) and the Governmental Politics Model (GPM). Both groups had Lead Actor and Decision Timing valances that matched the OBM. One explanation for this match was that neither group had the technical ability to be the lead actor and hence could not force the development and use of encryption systems required to solve pressing information security requirements. The much delayed development of the Advanced Encryption Standard used to replace the 1973 vintage DES supports this explanation.

Both groups had Problem Perception and Favored Alternative valances that matched the GPM. One explanation for this match was that the Congressional and Executive Groups believed that solving complex problems with laws and regulations was a way to maintain a balance of political power between the branches of government, especially in the area of international relations. The technology specific *Digital Millennium Copyright Act* and the technology neutral *E-SIGN Act* were passed to solve international and domestic information security problems. By refraining from information security solution mandates, these actors allowed the other groups to have available market-based solutions in response to the attack on the United States.

The actions of Encryption Technology Group and the Government Agencies Group exhibited patterns of behavior suggested by the Rational Actor Model. Table 4-3 shows the behavior convergence of these two groups. Both believed that the private sector had the technical expertise and trust to solve the information security problem. Actors in the Government Agencies Group realized the value of private sector technology leadership

when encryption vendors, such as RSA Security, captured most of the information security market in the private and non-defense government sectors. Actors in both these groups perceived a simple information security problem, which could be solved by developing and using cost effective information security products. This perception represented a large behavioral change in the Government Agencies Group, which was signaled when the National Security Agency gave up on the mandated use of key recoverable encryption products. However, the abandonment of information access requirements for national security and public safety reasons did not occur because of the utility maximizing solutions demanded by users.

Table 4-3 Status Quo Period Summary

Analysis Unit	Lead Actor	Problem Perception	Favored Alternative	Decision Timing	Allison Model
Congressional Group	1 consortium	2 complex	2 laws/ regulations	1 incremental / tacit	OBM GPM
Encryption Technology Group	0 private sector	0 simple	0 utility maximizing	0 contingent on choices	RAM
Executive Group	1 consortium	2 complex	2 laws / regulations	1 incremental / tacit	OBM GPM
Government Agencies Group	0 private sector	0 simple	0 utility maximizing	0 contingent on choices	RAM

While the September 11, 2001 attack drove the development and use of information security products, users surprisingly wanted choices that allowed information access for

trusted administrators as a means to recover from the effects produced by lost or stolen passwords and incapacitated or malicious users. Since prior laws, such as the *Communications Assistance for Law Enforcement Act*, allow telecommunications service providers to assist with court-ordered information access activities, these users are effectively permitting e-mail and network administrators and their respective certificate authorities to work with government officials in policing information flowing through the Internet. Thus, private sector development of balanced information access and security choices during the Status Quo Period represents a de facto United States encryption policy. All the actor groups appear satisfied by this status quo, but its longevity is in question.

A differing interpretation of the Status Quo Period should be mentioned. If users come to believe that the government has been surreptitiously abusing information privacy through system administrators and encryption certificate providers, then such a shock to the technology policy system may instigate a Kingdon styled “policy window” for a comprehensive digital privacy law. Once the trust in information security is lost, national security and public safety requirements in the United States may lose to legislated digital information privacy and anonymity rights.

Chapter Five: Explanation and Discussion

The analysis section of this research used four actor groups and three periods to create twelve analytical segments; this section integrates these segments into research displays and explanations. It also presents the valances for each actor group arrayed over three periods in order to create visual explanations for long-term encryption policy actions and decisions. In addition, this section presents the results for all actor groups arrayed over the three periods in order to create a visual explanation of the long-term trends among groups. Following each visual explanation, there is a discussion of how the researched patterns and trends support Allison's decision models and the scholarly works of Seifert, Pednekar-Magal, and Morgan on information and encryption control policies. In particular, the discussion suggests that groups of actors are capable of being learning organizations that can successfully interact with other organizations and create satisfactory information and encryption control policies.

Congressional Group

Information control decisions and actions taken by the Congressional Group changed gradually over three periods from being fully associated with Allison's Governmental Politics Model to being partly associated with it and the Organizational Behavior Model. Figure 5-1 shows that in the First Mover Period from 1973 to 1986,

actors in the Congressional Group believed that the government was the lead actor and the information control problem was complex.

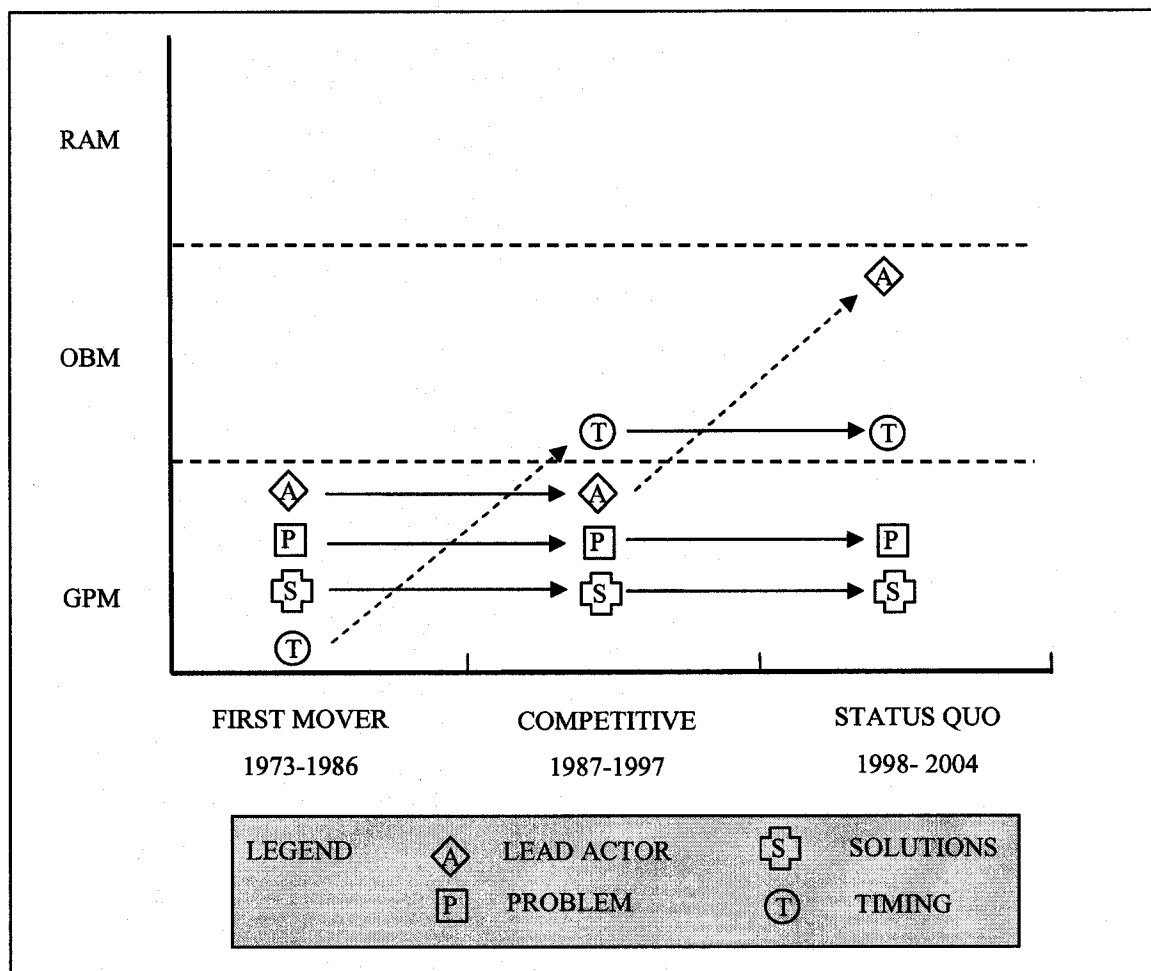


Figure 5-1 Congressional Group valances over three periods

In the next two periods, actors in this group consistently believed that the solution to this complex problem required a series of new laws. The motivation behind this consistency was a political competition with the executive branch. Actors in the Congressional

Group believed that the executive branch was a historical violator of information privacy and could not be trusted to balance information access and security requirements with directives, executive orders, and unilateral regulations.

The urgent passage of the *Privacy Act of 1974* was a critical event for information control legislation and came at a time that forced digital encryption control policy to the forefront of the information control debate. The valances exhibited during the First Mover Period were not static, as Allison wrote in *Essence of Decision*, “When a governmental or presidential decision is reached, the larger game is not over.”⁵⁷⁰ During the Competitive Period from 1987 to 1997, the political game continued with Congress passing the *Computer Security Act of 1987* and a set of less significant information control legislations. The “incremental / tacit” Decision Timing valance suggests that the political disagreement between the legislative and executive branches on controlling sensitive but unclassified information was not sufficiently polarizing to maintain a sense of urgency in Congress from the First Mover Period. When the Congressional Group had the opportunity to become the lead actor by mandating the use of escrowed-key encryption, there was little support for satisfying information access requirements that originated from the executive branch.

In the Status Quo Period, actors in the Congressional Group continued to make incremental and tacit decisions, but realized that they did not have the technical expertise required to be the lead actor. With the opportunity to push escrowed-key encryption

⁵⁷⁰ Allison and Zelikow, *Essence of Decision*, 303.

gone, the lead actor changed from the government sector to a consortium of actors. Figure 5-1 shows this change and resulting Lead Actor valance assignment. The Congressional Group reluctantly surrendered the lead actor role, as they learned from the passage of the *Digital Millennium Copy Right Act* that technical specificity hindered the development of information access and security solutions. Subsequent laws, such as the *E-SIGN Act* on electronic signatures, were technology neutral and controlled behaviors and not technologies. Thus, actors in the private sector were free to produce various technology solutions without government interference.

In the development of his models, Allison focused on delineating the attributes of each model and on anticipating future behaviors suggested by a particular model. He did not explicitly detail how decision behaviors could transition among models. However, in defining his OBM, Allison assimilated some attributes of organizational learning that could explain a transition mechanism. In *Essence of Decision*, Allison wrote the following: “In response to nonstandard problems, organizations search and routines evolve, assimilating new routines with considerable skill.”⁵⁷¹ Argyris provided a deeper understanding of organizational learning with a concept of double-loop learning, whereby an organization learns from correcting “mismatches” of problems and solutions and learns by changing “governing variables.”⁵⁷² In the case of the Congressional Group, a possible governing variable was the decision timing change during the Competitive Period. By sequentially solving the information control problem with laws, such as the

⁵⁷¹ Allison and Zelikow, *Essence of Decision*, 171.

⁵⁷² Argyris, *On Organizational Learning*, 68.

Computer Security Act of 1987 and the *Economic Espionage Act of 1996*, actors in the Congressional Group learned that they did not have to solve a complex problem in a single step. By using incremental solutions, this group changed their governing variable on the perceived timing requirement for the production of solutions.

Relaxed time constraints carried over to the Status Quo Period and may have affected the Lead Actor valance. As noted earlier, actors in the Congressional Group realized that laws should control behaviors and not technology. However, the legislative process controlling behaviors now had to be time-coupled with the technology activities of the private sector and in the government agencies. Actors in the Congressional Group used the hearings on the *DMCA* to equate the hazard of mandating specific legal protections for information security solutions with the hazard of mandating the use of escrowed-key encryption technology as an information access solution. A question challenging the ability of actors in the Congressional Group to use double-loop learning arises from this coupling. Congress should have learned from the escrowed-key encryption case that the better solution for *DMCA* was to forgo supporting a specific technology solution.

Argyris' double-loop learning theory counters this challenge by suggesting, "[L]earning occurs when the invented solution is actually produced."⁵⁷³ Congress did not learn from warnings on creating technology specific laws, because Congress did not produce a law on escrowed-key encryption. Only by enacting a partially flawed *DMCA*,

⁵⁷³ *Ibid.*, 68.

actors in this group learned about the consequences of specifying technology solutions. Congress refrained from specifying technology solutions in the subsequent *E-SIGN Act*, thereby allowing other actors in the consortium to create satisficing technical solutions.

The research of Seifert on encryption policymaking is consistent with my findings that actors in the Congressional Group did not have a sense of urgency and moved away from being the lead actor when confronted by encryption policy decisions. He examined the development of the Escrowed Encryption Standard and export control regulations during the Competitive and Status Quo Periods in order to determine the rules favored by private and government sector actors. He found that actors in the legislative branch were generally reluctant to create “normative rules,” rules to “standardize behavior,” or rules that had “strong enforcement mechanisms” when compared to actors in the executive branch and government agencies.⁵⁷⁴ Thus, actors in the legislative branch appeared to be more hesitant and less forceful in their decisions on escrowed-key encryption and export control regulations. Seifert’s findings agree with my work in that the actors in the Congressional Group did not pass legislation to mandate escrowed-key encryption and did not pass the *SAFE Act* to eliminate most forms of encryption control.

The research of Pednekar-Magal on encryption policymaking during the development of the Escrowed Encryption Standard is consistent with my finding that actors in the Congressional Group did not have a sense of urgency when confronted by

⁵⁷⁴ Jeffery W. Seifert, “Who(se) Rules (for) the Internet: Regime Formation and Global Public Policy for the Information Age” (Ph.D. diss., Syracuse University, 2000), 100-105.

encryption policy decisions. Her research used actor groups that did not include the legislative branch as active policymakers. She found that “the NSA continued attempts to dominate the encryption policy process,” despite the intent of Congress in the passage of the *Computer Security Act of 1987* to control the power of the executive branch and its agencies.⁵⁷⁵

During the Competitive Period, the apparent reluctance of Congress to act with legislation in settling the escrowed-key encryption policy debate led Pednekar-Magal to believe that actors in the Congressional Group became quiescent after 1990. This inference may be valid if one ignores other information control legislations, such as the *Communications Assistance to Law Enforcement Act* and the *Economic Espionage Act of 1996*. By choosing a specific encryption policy event, she discounted the explanatory power of her “Pluralist perspective,” whereby “state actors” minus Congress, “economic actors,” and “civil liberty groups” create encryption policy.⁵⁷⁶ Her attenuation of the contributions made by actors in the Congressional Group reinforced her “managerialist theory” finding, in which the executive branch and government agencies were the dominant government policymakers. While actors in the Congressional Group were transitioning from GPM to OBM behaviors during the period covered by Pednekar-Magal’s analysis, actors in this group continued to be active policymakers.

⁵⁷⁵ Vandana Pednekar-Magal, “State surveillance and the telecommunication policy process: The politics of United States encryption policy” (Ph.D. diss., Bowling Green State University, 2000), 138.

⁵⁷⁶ *Ibid.*, 131-2.

The research of Morgan used data on information and encryption control events to show that actors could form a technology enabled “virtual epistemic community” and that “interpreters” could act as leaders to influence specific policy decisions.⁵⁷⁷ Her research was consistent with my Competitive Period findings that actors in the Congressional Group were active policymakers, but took incremental steps and were not policy leaders. Her research covered three case studies, two of which were the negotiations on the 1996 WIPO treaties and the mid-1990s fight on encryption export controls. In the WIPO treaties case, she found that “the virtual epistemic community ... was able to play a significant role in expanding the participation in the debate beyond the narrow confines of the hearings, Congress and WIPO.”⁵⁷⁸ The subsequent expansion of participating actors made it difficult for Congress to write, debate, and pass comprehensive legislation on intellectual property.

The incremental and tacit nature of laws passed during the Competitive and Status Quo Periods reflected Congress’ attempts to satisfy the confluence of multiple policy actors. Specifically, the 1998 *Digital Millennium Copyright Act* arose from two House bills joined late in the legislative process in order to satisfy the multi-segmented WIPO treaties and to satisfy powerful domestic actors, such as the Recording Industry Association of America. Morgan’s encryption case added support for the ability of a virtual epistemic community to use “the technologies themselves to circumvent or

⁵⁷⁷ Glenda Nadine Morgan, “The message and the medium: Electronic communications technologies and global policy change in copyright, privacy and encryption” (Ph.D. diss., University of Minnesota, 2001), 201-2.

⁵⁷⁸ *Ibid.*, 204-5.

challenge controls on encryption.”⁵⁷⁹ My work found that actors in the Encryption Technology Group did release encryption software into the public domain to advance legislation on encryption liberalization, such as the *SAFE Act*, and to retard congressional attempts to pass restrictive export control laws. In addition, Morgan found that “in order to influence policymakers in Congress,” it took “conventional lobbying methods that the business community with their greater experience and larger budget were able to do with much larger effect.”⁵⁸⁰ This finding is consistent with my work, which suggested that actors in the Congressional Group were not the lead policy actors and were significantly influenced by conventional activities undertaken by actors in the Encryption Technology, Executive, and Government Agencies Groups. This form of lobbying was sufficient to prevent enactment of legislation on encryption export controls and on encryption liberalization.

In summary, the findings of Seifert, Pednekar-Magal, and Morgan are consistent with the idea that starting in the Competitive Period, Congress passed laws on the periphery of the information control problem and lost the status of being the lead information control policy actor. A sequence of important laws in the Status Quo Period, such as the *DMCA* and *E-SIGN Act*, were incremental steps toward a comprehensive information control policy, but were bounded by the failure to choose between the *SAFE Act* and substantive export control legislation. The evolution of decision behaviors from those suggested by the GPM to a mix suggested by the GPM and OBM may have

⁵⁷⁹ *Ibid.*, 205.

⁵⁸⁰ *Ibid.*, 323.

affected the other groups. As my work bracketed and covered the timeframe used by Seifert, Pednekar-Magal, and Morgan, it may yield further longitudinal conclusions on the Congressional Group when interactions are considered.

Encryption Technology Group

Actors in the Encryption Technology Group exhibited decision behaviors that remained constant over the three periods and were fully associated with Allison's Rational Actor Model. Figure 5-2 shows consistent information control decisions and actions from the First Mover, through the Competitive, and to the Status Quo Periods. In the First Mover Period, actors from the government sector believed that they were working as part of a consortium with the Encryption Technology Group to develop information security solutions. This belief was not reciprocal, as only the Encryption Technology Group possessed the technology leadership and the willingness to share proprietary encryption technology.

In the RAM, Allison introduced the idea that a nation or government could act as a "unitary decision maker" that was "anthropomorphized as if it were a single person with one set of preferences (a consistent utility function), one set of perceived choices, and a

single estimate of the consequences.”⁵⁸¹ Actors in the Encryption Technology Group behaved less like organizational actors and more like Allison’s unitary decision maker.

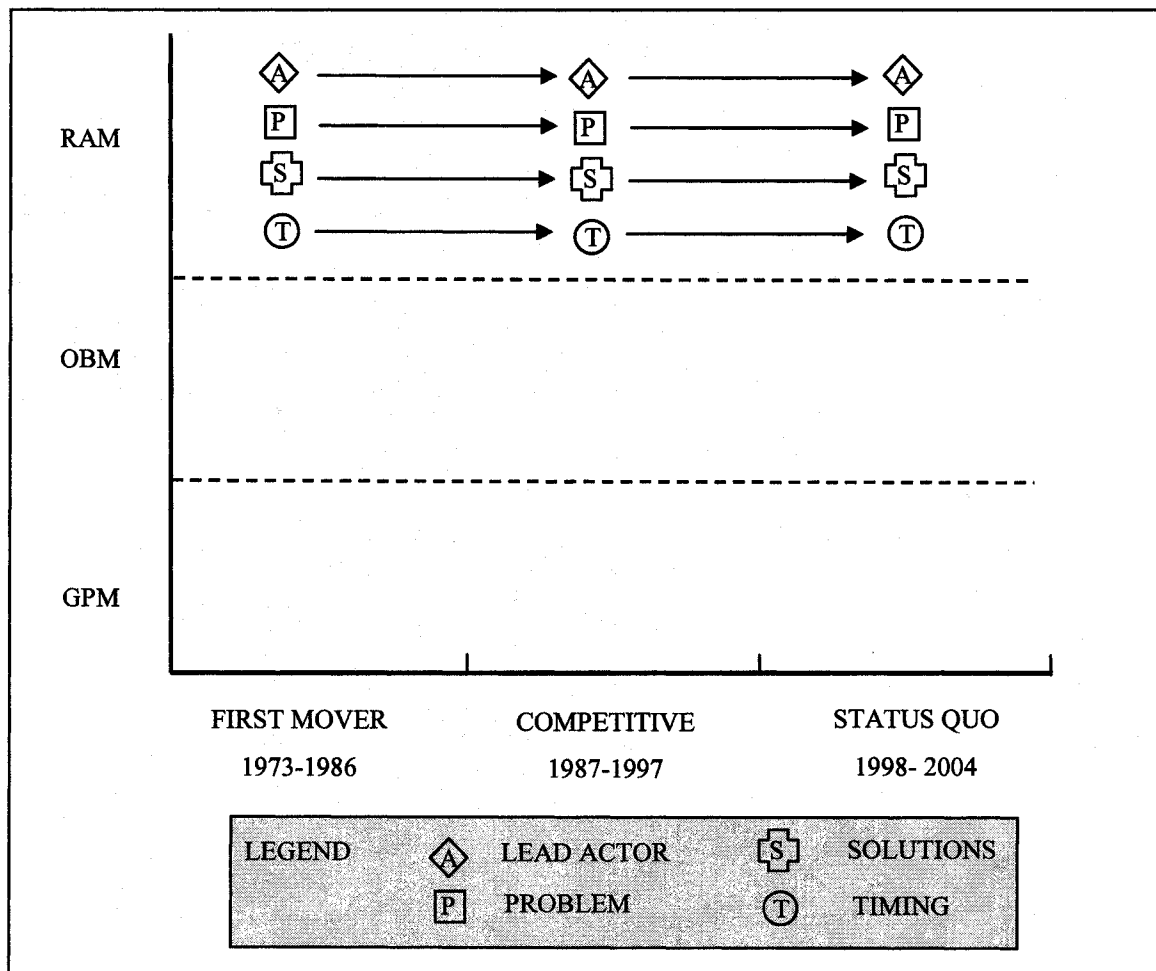


Figure 5-2 Encryption Technology Group valances over three periods

The unifying attribute of the Encryption Technology Group was its belief in the technology leadership of the private sector. Early in the First Mover Period, actors in this

⁵⁸¹ Allison and Zelikow, *Essence of Decision*, 24.

group realized that they possessed the encryption technology expertise required to solve the new digital information security problem. The development of an IBM encryption algorithm into the Data Encryption Standard (DES) represented a technology leadership awakening for actors in this group. During the DES competition, the reluctance of government actors to submit secretive national security encryption algorithms allowed the IBM algorithm to win by default. Following the information security movement created by the *Privacy Act of 1974*, actors in the Encryption Technology Group focused on encryption technology as the single best solution. As noted earlier, Allison's RAM required that the unitary decision maker use "one set of perceived choices."⁵⁸² In the case of encryption technology, actors in this group maintained a monopoly on technology alternatives by first beating government alternatives to market and then by defeating government attempts to manipulate the market through new laws and regulations. The 1976 discovery of public key encryption by Stanford University researchers was a technology innovation in the development of complete encryption systems. My work found that the government could have developed public key encryption first and capitalized on its funded research that led to the public key encryption patent. This would have denied actors in the Encryption Technology Group firm control over information security solutions. Again, the failure of the government to act bolstered the opportunity of actors in the Encryption Technology Group to develop utility maximizing solutions in the First Mover Period.

⁵⁸² *Ibid.*, 24.

The valances exhibited by actors in the Encryption Technology Group did not change in the Competitive Period, despite attempts by the government to force escrowed-key encryption and encryption-hindered digital signature technologies onto the market. My work indicated that both these attempts failed, in part, because actors in the Encryption Technology Group convinced Congress that technology specific laws would give the government an unfair competitive advantage and would stifle innovation by the private sector. More significantly and as suggested by Allison's RAM, my research found that the Encryption Technology Group used its technology leadership in the First Mover Period to produce utility maximizing solutions in the Competitive Period that were superior to the government's Escrowed Encryption Standard and Digital Signature Standard. Specifically, the RSA public key encryption algorithm coupled with DES allowed companies, such as RSA Security, to produce superior products.

Despite an initial setback caused by the technical specificity found in the *Digital Millennium Copyright Act*, actors in the Encryption Technology Group were able to develop and market information security solutions freely in the Status Quo Period. Users interested in better information security solutions avoided the government's offerings and waited for more powerful and trustworthy offerings from the private sector. Allison explained this behavior with his general proposition that "an increase in the value of the consequences that follow from an action ... increases the likelihood of that action being chosen."⁵⁸³ My research noted an exception to this proposition when some actors, such

⁵⁸³ *Ibid.*, 25.

as the Recording Industry Association of America, sought legal protection for their information security solutions. This reliance on laws instead of strong encryption technology resulted in the use of weak or obsolete technology, such as the DVD Content Scrambling System that was cracked by a teenager. Aside from this setback, actors in the Encryption Technology Group enjoyed continued market success in the Status Quo Period with the development of the Advanced Encryption Standard to replace DES and the organic development of information security solutions that also satisfied information access requirements. In contrast to rejecting government developed information control solutions, actors in this group readily accepted the emergence of market driven information control solutions. This suggested that the utility function on information control solutions placed a high value on the trustworthiness of actors developing these solutions.

Actors in the Encryption Technology Group did not experience major learning failures during the three analytical periods. Allison's RAM explanation of policymaking being a utility maximizing process is closely related to the notion of single-loop learning. Argyris defines single-loop learning as occurring when "an error is detected and corrected without questioning or altering the underlying values of the system."⁵⁸⁴ Actors choosing the best solution from an agreed upon set of alternatives qualifies as single-loop learning, because selecting a solution with lower utility would produce an error condition. My work found that by focusing on a simple information security problem and ignoring

⁵⁸⁴ Argyris, *On Organizational Learning*, 68.

the complexities caused by information access requirements, actors in the Encryption Technology Group never experienced a major decision failure. Even the failed section in the *DMCA*, which bolstered government protection of information security technology, counts as a successful decision because supporting the information access requirements of users would have produced an error condition with the economically powerful group of intellectual property originators.

Without the impetus to change governing variables, some actors in the Encryption Technology Group have yet to find an optimum balance between information security and information access requirements. A recent example of this is the continuing debate on how digital rights management will work with MPEG 4 encryption and compression technology. Dissention in the Encryption Technology Group has become more public, as seen by internal activism recently demonstrated by DVD cracker Jon Johansen, who is now in his twenties. According to a web-blog by an Electronic Frontier Foundation staff member, Johansen was able to crack the part of Apple's iTunes system that allegedly uses RSA public key and AES secret key encryption.⁵⁸⁵

The research of Seifert on the development of the Escrowed Encryption Standard and export control regulations is consistent with my finding that actors in the Encryption Technology Group acted as a unitary decision maker. In his research, he used a non-governmental actor group that included organizations, corporations, and lobbying groups.

⁵⁸⁵ Cory Doctorow, "Airport Express crypto broken by DVD Jon," BoingBoing blog, 12 August 2004 < http://www.boingboing.net/2004/08/12/airport_express_cryp.html >, accessed January 2005.

These actors were nearly identical to actors in my Encryption Technology Group.⁵⁸⁶ By grading the actions of his governmental and non-governmental groups, Seifert found that the non-governmental group favored “instruction sense rules,” while the governmental group favored “regulation sense rules.”⁵⁸⁷ He concluded that instruction sense rules dominated and that non-governmental actors “connected their goal to the broader interests of the various members of their coalition.”⁵⁸⁸ This conclusion matched Allison’s RAM idea of an actor having “one set of perceived choices.”⁵⁸⁹ This conclusion also matched my finding that actors in the Encryption Technology Group consistently chose to satisfy information security requirements over information access requirements. An example of this was found with the preferred strength of secret key encryption algorithms, which was set at 56-bits by DES and is now an incredible 128 bits and higher in AES. Actors in this group did not preserve the ability to use 64 or 80-bit encryption as a compromise choice to satisfy information access requirements of other groups. As noted earlier in the single-loop learning discussion, choosing a less than optimal solution is an error condition that will necessitate the search for a better choice and will not lead to a change in the governing variables of the information security problem.

Two research conclusions of Pednekar-Magal on encryption policymaking during the development of the Escrowed Encryption Standard (EES) are not consistent with my

⁵⁸⁶ Seifert, 36.

⁵⁸⁷ *Ibid.*, 119.

⁵⁸⁸ *Ibid.*, 120-21.

⁵⁸⁹ Allison and Zelikow, *Essence of Decision*, 24.

finding that the Encryption Technology Group was a unitary policymaker at least co-equal to the other actor groups. To test her thesis from a pluralist perspective, she divided policy actors into government agencies, “civil liberty,” and business actor groups.⁵⁹⁰ In her conclusion, she found that the pluralist perspective had “serious limitations” because “NSA clearly dominated the encryption policy process.”⁵⁹¹ My work found that the Encryption Technology Group, which encompassed her civil liberty and business actor groups, created policy through rational actions. The adaptation of an IBM algorithm into DES, the failure of NSA’s EES, and the ubiquitous use of RSA public key encryption were products of rational actions.

Her second conclusion used NSA’s co-option of ATT’s national security telephone business as evidence that a managerialist perspective better explained the encryption policy process.⁵⁹² While my work found some divisiveness in the Encryption Technology Group, such as the RIAA pushing for anti-circumvention laws, most actors in this group supported the unitary goal of a market-based encryption policy. To be consistent with her managerialist perspective, NSA would have needed to convince a majority of these actors, not just ATT, to side with the Government Agencies Group. If this were the case, then EES might have been successful and both Pednekar-Magal’s conclusions on state action theories may have gained greater merit. I showed that EES

⁵⁹⁰ Pednekar-Magal, 132-133.

⁵⁹¹ *Ibid.*, 136-139.

⁵⁹² *Ibid.*, 139-143.

failed badly and that NSA did not salvage part of the EES effort by entering the Advanced Encryption Standard competition.

The research of Morgan on the roles of a “virtual epistemic community” and “interpreters” in changing technology policy provides a deeper explanation of how a large Encryption Technology Group could act as a unitary actor.⁵⁹³ Unique properties of this group were their technology leadership and advanced use of electronic communications. Morgan found that their use of communication “technologies help bring together diverse sets of actors” and “had a large impact on the policy options that were developed within.”⁵⁹⁴ I also found that a diverse set of private sector actors, such as Citibank, EFF, Entrust, EPIC, IBM, RIAA, and RSA Security, were able to agree upon a general information security policy that promoted encryption liberalization.

Morgan’s second finding was that groups of actors relied on interpreters, “who were able to speak with authority and were acknowledged as leaders,” to provide policy coherency.⁵⁹⁵ This finding supported Allison’s RAM notion of a group being anthropomorphized into single actor by allowing group elites to champion a policy position for the entire group. My research reinforced the roles and identities of information security policy elites including Bernstein; Bidzos; Diffie and Hellman; Feistel; Kahn; Rivest, Shamir, and Adleman; Rotenberg; and Schneier. Following the logic of Morgan, the successful actions of these elites in challenging laws in court,

⁵⁹³ Morgan, 325-326.

⁵⁹⁴ *Ibid.*, 326-327.

⁵⁹⁵ *Ibid.*, 330.

inventing encryption technology, lobbying Congress, marketing encryption products, and resisting government pressure were the essence of RAM policymaking by a group.

In summary, the findings of Seifert and Morgan were consistent with my results and Allison's RAM. From the First Mover Period through to the Status Quo Period, the consistency of the decision behaviors exhibited by a diverse Encryption Technology Group is a significant finding. The apparent success of this group may have influenced the behaviors of other less successful groups. However, findings by Pednekar-Magal downplay the success of the Encryption Technology Group by highlighting the power of the Executive and Government Agencies Groups during the mid-1990s. My successful match of RAM behaviors and three decades of activities by the Encryption Technology Group may be a more significant finding because of the greater support provided by my longitudinal research.

Executive Group

Actors in the Executive Group exhibited the largest valance changes throughout the three analytical periods. Figure 5-3 shows that this group largely exhibited OBM decision behaviors in the First Mover Period, except for a Lead Actor valance more closely aligned with the GPM. The Soviet threat allowed actors in this group to maintain leadership of the national security piece of the information control problem.

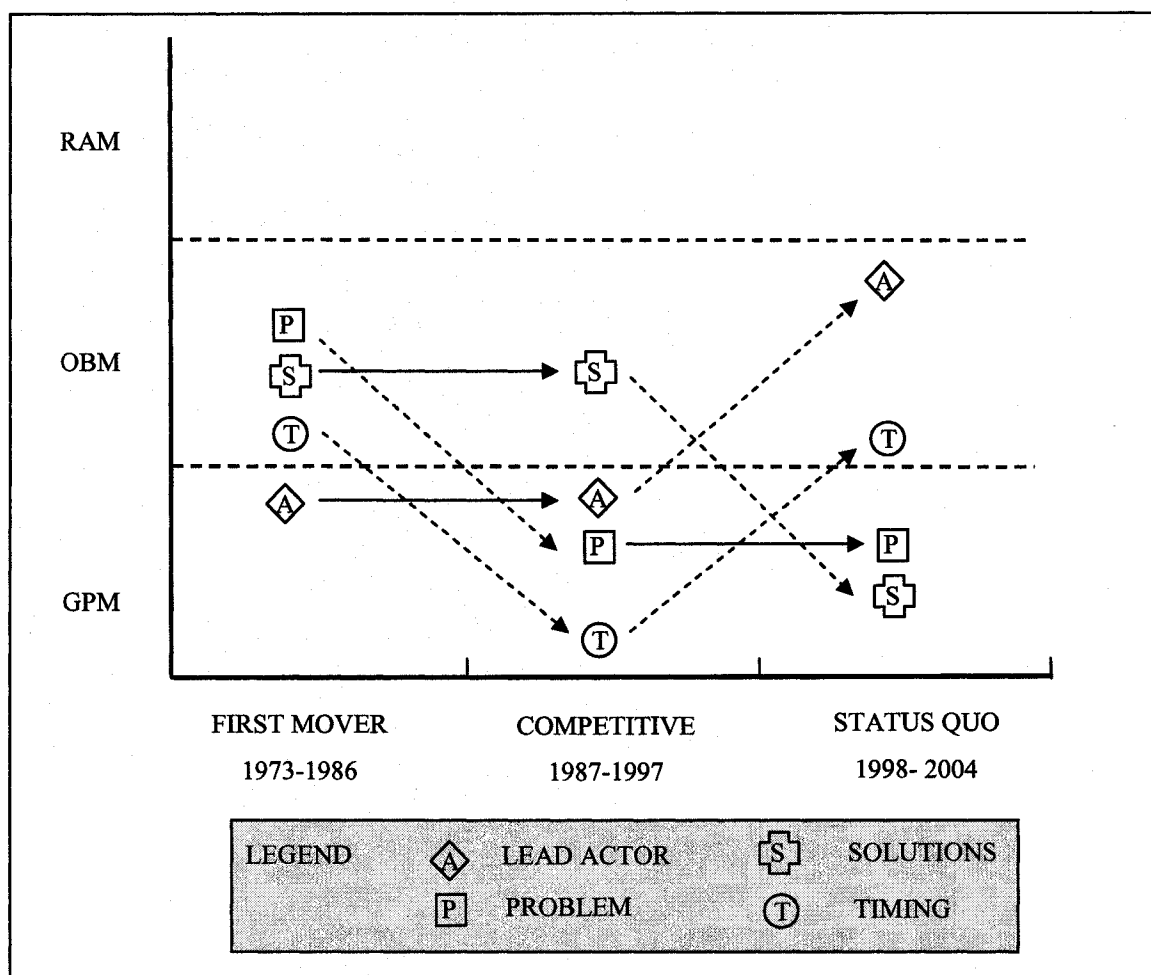


Figure 5-3 Executive Group valances over three periods

After the Watergate scandal, the power struggle between the executive and legislative branches on information control left actors in the Executive Group without specific information access laws to protect national security and public safety. The *Foreign Intelligence Surveillance Act of 1978* made it difficult to eavesdrop on Americans, and the *Electronic Communications Privacy Act of 1986* demonstrated that the use of encryption was a legal sign that such communications were protected from

interception. Their reactions to these legal limitations matched the behaviors suggested by Allison's OBM, whereby "behavior at one time, t , is marginally different from the behavior at $t-1$ "⁵⁹⁶ Thus, actors in the Executive Group used past precedents and routines to solve parts of the current information control problem.

Actors in the Executive Group followed past precedents, such as using existing regulations and issuing executive orders and presidential directives, to make both domestic and international information control policies. One such precedent was the awkward use of the State Department's Munitions List, which was part of the International Traffic in Arms Regulations, to control the export of encryption technology. On the domestic side, President Reagan's National Security Decision Directive 145 defined new categories of information, and the repercussions of these new information definitions were manifested in the next period.

Figure 5-3 shows that during the Competitive Period, actors in this group exhibited a Favored Alternative (solutions) valance consistent with the OBM and exhibited Lead Actor, Problem Perception, and Decision Timing valances more closely associated with the GPM. Actors in the Executive Group believed that information control was a complex problem with differing private and government sector dimensions and a compounding international dimension. NSDD-145 broadened the importance of information security beyond the traditional national security area to include all

⁵⁹⁶ Allison and Zelikow, *Essence of Decision*, 180.

unclassified information. By recognizing that information security was only as good as its weakest link, members in the National Security Council System created a new category of sensitive but unclassified information in order to protect selected information in the non-defense government and private sectors. Congress reacted with its own solution to the information security problem, which was the *Computer Security Act of 1987*. This law put Congress at odds with the executive branch in controlling private sector information. In addition, this law unleashed the development of competitive information security solutions from the private sector, which subsequently created a sense of urgency for the executive branch.

Information security solutions created information access problems for the government. President Clinton's Presidential Decision Directive / National Security Council 5 (PDD/NSC-5) pushed for the use of escrowed-key encryption to beat private sector solutions to market and to satisfy the government's information access requirements. Immediate Executive Group reactions to moves by Congress and the private sector matched the behaviors suggested by Allison's OBM, where he stated, "Deadlines and events raise issues and force busy players to take stands."⁵⁹⁷ Maintaining a prolonged sense of urgency on the information control problem was not possible, and their Decision Timing valance reverted to one of incremental change in the next period.

Figure 5-3 shows that during the Status Quo Period, actors in the Executive Group exhibited Lead Actor and Decision Timing valances indicative of the OBM. The

⁵⁹⁷ Allison and Zelikow, *Essence of Decision*, 299.

Executive Group could not be the lead actor because they did not have the technical knowledge to shape new information control solutions and did not have the political power to force the use of prior government solutions. Actors in this group had to abandon support for the Escrowed Encryption Standard in the Competitive Period, but supported the Advanced Encryption Standard competition along with a consortium of other actors in the Status Quo Period.

Without specific authorizing legislation, actors in the Executive Group supported the Wassenaar Arrangement on dual-use technology by issuing incremental executive orders and by periodically readjusting the Export Administration Regulations. Congress tacitly aided these incremental changes by its continual failure to renew the *Export Administration Act of 1979*. Before the September 11, 2001 attack, the Clinton administration realized the vulnerabilities of the critical information infrastructure in the United States and issued Presidential Decision Directive / NSC-63 in 1998 to attempt a solution. Yet, two years after the attack, actors in the Executive Group merely replaced President Clinton's PDD/NSC-63 with an updated Homeland Security Presidential Directive, HSPD-7. Allison suggested in his OBM that such a reaction is a "preeminent feature of organizational activity" and that "behavior in any particular case is an enactment of previously established routines."⁵⁹⁸ Less dynamic behaviors also marked the Status Quo Period.

⁵⁹⁸ *Ibid.*, 168.

The Problem Perception valance did not change during the Status Quo Period, as actors in the Executive Group perceived a further compounding of international and domestic information control problems from the Competitive Period. As noted earlier, maintenance of the Wassenaar Arrangement required controls on encryption exports that were not popular with domestic encryption vendors and electronic rights activists. My work also found that actors in this group preferred laws, such as the *Digital Millennium Copyright Act*, that satisfied politically powerful groups. In the *DMCA* case, the executive branch satisfied domestic intellectually property originators at the expense of research and development efforts on new information security tools.

After the September 11, 2001 attack, the Bush administration mistakenly believed that the *USA PATRIOT Act* allowed sufficient information access to accomplish the Global War on Terrorism. The Bush administration used the *Homeland Security Act of 2002* to address domestic information security requirements. However, congressional discontent on the recently passed *Intelligence Reform and Terrorism Prevention Act of 2004* suggests that satisfying information access requirements will have to wait for the vetting and maturation of a new national intelligence directorate and its leaders. The perception of a complex information access and security problem and the political capital expended to obtain favorable laws matched Allison's GPM concept in which a "player pulls and hauls with the power at his discretion for outcomes that will advance his or her conception of national, organizational, group, and personal interests."⁵⁹⁹ Problem

⁵⁹⁹ *Ibid.*, 302.

perceptions were moderated by the perceived political power available to the executive branch.

Actors in the Executive Group changed a governing variable of information control in the Competitive Period. The invention of unclassified but sensitive information allowed the NSCS to exert more control over information in the non-defense government and private sectors. This invention qualified as a governing variable in double-loop learning because the change was implemented and, to paraphrase Argyris, the change produced a state or environment in which actors could develop satisficing solutions.⁶⁰⁰ This state was an expansion of the classified information domain and subsequent control of sensitive information according to existing procedures developed for classified national security information.

Argyris further suggested that double-loop learning is often used to solve “complex, non-programmable issues.”⁶⁰¹ In the Competitive Period, my research found that actors in the Executive Group perceived a complex information control problem in accordance with GPM behaviors. However, by extending the domain of classified information, actors in this group attempted solutions suitable for classified information in accordance with OBM behaviors. Thus, past precedents and routines, such as following information assurance and communications security procedures, were applied as solutions outside of the national security area. The government’s Escrowed Encryption Standard was a

⁶⁰⁰ Argyris, *On Organizational Learning*, 68.

⁶⁰¹ *Ibid.*, 69.

poignant example of a solution that worked well in the national security area, but failed in the private sector. Partly because of this failure, Figure 5-3 suggests that actors in the Executive Group looked to laws and regulations as solutions during the Status Quo Period, which is a GPM behavior. Also during this period, actors in this group adapted an incremental timing approach to the problem, which is an OBM behavior. This split between OBM and GPM behaviors was identical to the decision behaviors exhibited by the Congressional Group.

The research of Seifert blended the contributions of all government actors into a single encryption policy group. One specific finding by Seifert was relevant to the actors in my analytical Executive Group. He found that the Clinton administration used a “complex web of regulations” to create an encryption export policy acceptable to the “competing demands of the various national security/law enforcement agencies, industry associations and civil liberties groups.”⁶⁰² By using these phrases, Seifert suggested that actors in the executive branch could be differentiated from actors in government agencies. Accordingly, I separated executive branch actors and government agency actors into different groups for my research.

Seifert’s “complex web” metaphor on the use of regulations suggested a Favored Alternative valance assignment of “new laws and regulations” that matched Allison’s GPM. However, I assigned a Favored Alternative valance of “past precedents and routines” that matched OBM behaviors. This difference can be explained by examining

⁶⁰² Seifert, 64.

Figure 5-3, which shows that actors in the Executive Group relied upon past precedents and routines during First Mover and Competitive Periods. The precedent set by the routine manipulation of export regulations was unchecked by Congress during these periods. Thus, instead of fighting for new laws and matching regulations that would mandate the use and export of escrowed-key encryption, actors in the Executive Group used older solutions that worked before. This changed during the Status Quo Period, because actors in the Congressional Group were more willing to oblige the executive branch with new information security laws to fight the Global War on Terrorism.

The research of Pednekar-Magal blended the contributions of the executive branch and government agencies in making encryption policy. However, one of her specific findings on the executive branch was applicable for comparison against my findings. In researching the motivation behind the development of the Escrowed Encryption Standard, she found that “the US administration was aware of a need for international acceptance of key escrow in order to give teeth to its policy.”⁶⁰³ I found that during the Competitive Period, actors in the Executive Group perceived a complex information control problem with international repercussions. International agreements on dual-use technology, such as the Wassenaar Arrangement, influenced actors in the Executive Group to seek domestic laws for support.

Without congressional support, actors in the Executive Group were forced to manipulate export regulations to support their policies. This manipulation gave favorable

⁶⁰³ Pednekar-Magal, 123.

export status to information security tools based on the Escrowed Encryption Standard. Pednekar-Magal stated that this approach was a “brute force” one, which supported her managerialist thesis.⁶⁰⁴ A law mandating the use and export of key-recoverable encryption would have qualified as a brute force approach, but Congress could not agree upon major encryption and export control legislations. Actors in the Executive Group perceived a sense of urgency in tailoring encryption export regulations, because Congress was leaning toward the *SAFE Act* that would have liberalized encryption use and exports.

The research of Morgan on the WIPO treaties and on encryption export controls supported a finding that actors in the Executive Group perceived a complex information control problem with tightly coupled domestic and international dimensions. With respect to the administration’s role in the WIPO treaties, she found that the “Administration was trying to get simultaneous agreement on the same set of proposals domestically and internationally.”⁶⁰⁵ My work covered the implementation of the WIPO treaties in the *DMCA* and found that the Clinton administration was vitally concerned about the lack of information security measures required to protect the digital intellectual property of the United States. The resulting information security law prohibiting circumvention technology that could defeat encryption stood in contrast to the Clinton administration’s desire of guaranteed access to domestic and international information. In her escrowed-key encryption case, Morgan found that “the US administration continued to pressure foreign governments and Wassenaar to adopt key recovery”

⁶⁰⁴ *Ibid.*, 123.

⁶⁰⁵ Morgan, 151.

encryption.⁶⁰⁶ This information access and security double standard was the result of organizational and political processes. An organizational process pushed for government information access as manifested by the Escrowed Encryption Standard and by export controls. A political process pushed for information security as manifested by the *DMCA* and by presidential directives on critical information infrastructure protection.

In summary, my analysis showed that actors in the Executive Group originally exhibited decision behaviors largely consistent with Allison's OBM in the First Mover Period, and then exhibited behaviors largely consistent the GPM in the Competitive Period. A finding by Seifert on the preferred use of regulations by actors in the Executive Group corresponded to a similar finding in my research, but Seifert attached a political significance to this use of regulations. During the Competitive Period, I found an organizational significance, because the executive branch could not get legal support from export laws stalled in Congress and only had extant regulations to manipulate. Allison's OBM better described this Favored Alternative valance of using "past precedents and routines" during this period. The findings of Pednekar-Magal and Morgan on the political interplay between international and domestic information control policies were consistent with a transition of behaviors during the Competitive Period. My research bracketed and covered the timeframe used by these three researchers, and my longitudinal conclusions on interactions of the Executive Group with the other groups will be presented in the Interactions section.

⁶⁰⁶ *Ibid.*, 316.

Government Agencies Group

Actors in the Government Agencies Group exhibited decision behaviors that were fully associated with Allison's Organizational Behavior Model in the First Mover Period. These behaviors changed dramatically during the Competitive Period to become largely associated with the Governmental Politics Model. In the Status Quo Period, these behaviors again changed to become fully associated with the Rational Actor Model. Figure 5-4 shows the evolution of these decision behaviors and the dramatic transition during the Competitive Period; a period of great interest among scholars of information and encryption control research. My research covered and bracketed the 1992-2000 period researched by Seifert, Pednekar-Magal, and Morgan. In addition, my research added longitudinal depth to the explanations in the existing literature.

In the First Mover Period, actors from the Government Agencies Group believed that they were working as part of a consortium to produce a first-ever data encryption standard. Actors in the Government Agencies Group exhibited a Lead Actor valance consistent with the OBM. In the OBM, Allison believed that organizational actors would behave as a constellation of actors and noted that this "constellation acts only when component organizations perform routines."⁶⁰⁷ Development of the Data Encryption Standard by the National Bureau of Standards was accomplished by using the normal and expected actions of all four analytical groups.

⁶⁰⁷ Allison and Zelikow, *Essence of Decision*, 166.

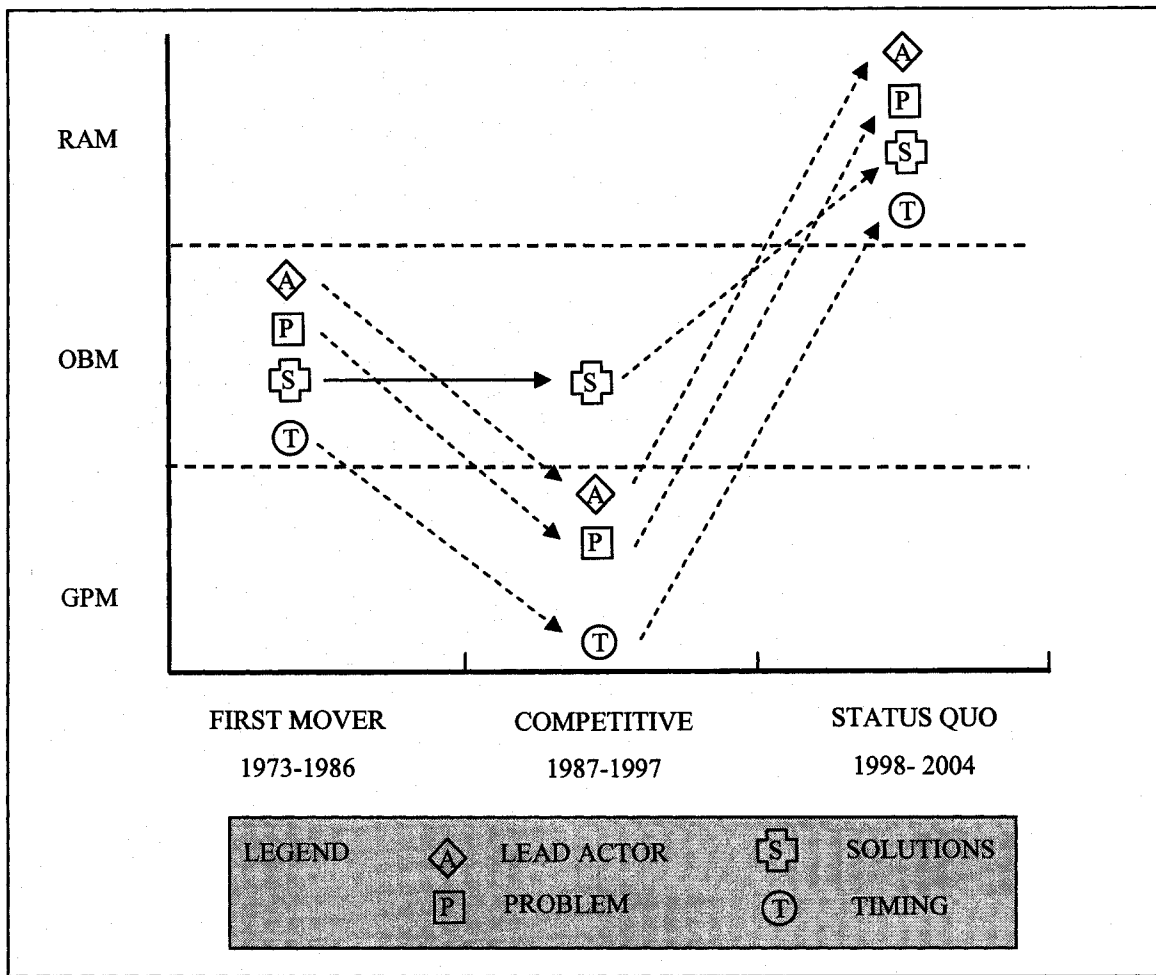


Figure 5-4 Government Agencies Group valances over three periods

The development of DES required a consortium of government and private sector actors and a confluence of routine actions and political processes for success. One action was Congress' heightened concern about privacy in the digital age and its forceful reemphasis of the 1965 *Brooks Act*, which directed NBS to develop automatic data processing equipment (ADPE) standards. Another action was the issuing of executive orders, which gave NBS, under the Department of Commerce, the responsibility for

ADPE standards. Perhaps the key enabling action was the participation of the private sector in the development of DES, as the National Security Agency did not volunteer national security solutions for this development. The perception of the lead actor changed during the Competitive Period.

Figure 5-4 displays the dramatic shifts in the valances exhibited by actors in the Government Agencies Group during the Competitive Period. The only static valance was the preference to use past precedents and routines as solutions to the information and encryption control problems. The National Institute of Standards and Technology and the National Security Agency agreed upon the development of the Escrowed Encryption Standard and the Digital Signature Standard as solutions to these problems. NIST and NSA now perceived a complex information access and security problem with international and domestic dimensions. I found that the requirement for government access to information was intended to address national security concerns on information assurance and counter-intelligence operations and to satisfy public safety concerns on wiretap and critical data recovery operations.

Actors in the Congressional and Encryption Technology Groups tried to influence the Government Agencies Group by claiming that escrowed-key encryption weakened national security through its vulnerable backdoors. Yet, actors in the Executive Group relied on the Government Agencies Group to persevere in satisfying information access requirements. Allison's GPM describes this reliance on the Government Agencies Group as an "action channel" which is a "regularized means of taking government action on a

specific kind of issue.”⁶⁰⁸ The Lead Actor and Decision Timing valances are consistent with this action channel notion. Actors in the Executive Group perceived that the government was the lead actor and urgently pushed actors in the Government Agencies Group to develop the EES and DSS. The goals of these standards were to beat private sector competitors to the market and to produce network effects with a critical mass of users.

In the Status Quo Period, actors in the Government Agencies Group exhibited behaviors consistent with the RAM, which is shown in Figure 5-4. The development of the Advanced Encryption Standard by NIST epitomized the decision behaviors of this group. In late 1990s, actors in this group recognized that a simple information security problem was behind the information infrastructure vulnerabilities of the United States. In addition, actors in this group realized that the private sector had the technology expertise, trust, and market skills required for leadership in this area. Two months after the September 11, 2001 attack, the approval of a virtually unbreakable 128-bit AES, as the encryption standard of the United States, represented a rational actor triumph of satisfying information security requirements. Satisfaction of government information access requirements remained uncertain.

An unanticipated finding of my research was that actions by the Government Agencies Group, such as not using a NSA developed algorithm, increased market trust in the AES. As noted earlier, actors in the Encryption Technology Group soon added to the

⁶⁰⁸ *Ibid.*, 300.

utility of United States information security products by allowing information access through key recovery from certificate authorities. Thus, the Government Agencies Group's unsuccessful escrowed-key encryption scheme of the previous period had now become acceptable to the private sector in the Status Quo Period. I used Allison's RAM to explain this dramatic change in the perceived value of a balanced information access and security solution as the simple rational creation of a "preference-maximizing choice."⁶⁰⁹ However, Allison cautioned that many decisions appear to be RAM-based and that "rules of evidence" must be applied before reaching such a conclusion.⁶¹⁰ To satisfy Allison's warning, I applied the valances to actions and events to find the best match before reaching a conclusion on the appropriate model. In *Essence of Decision*, Allison applied each of his models to a crisis event and then allowed the reader determine the better-fit decision model. My method may sometimes suffer from a "rhetorical closure," but saves the reader from perusing each encryption event from the perspectives of three decision models.

Actors in the Government Agencies Group experienced a major learning failure during the Competitive Period, which created an opportunity for double-loop learning. It may appear difficult for organizational actors within the Government Agencies Group to exhibit RAM behaviors. However, Argyris stated that if "individuals strive to 'satisfice' when they are acting," then these individuals "acting as agents for the organization" can

⁶⁰⁹ *Ibid.*, 25.

⁶¹⁰ *Ibid.*, 26.

accomplish double-loop learning.⁶¹¹ In doing so, these individuals could have set the governing variables of an organization to exhibit behaviors suggested by the RAM. A possible Allison style explanation would focus on finding the contributions of such individuals. An examination of NIST's centennial publication suggested that Miles Smid was one such individual who worked at both NSA and NIST. "Miles was the manager of the NIST Security Technology Group through most of the 1990s, a difficult period of contentious, highly charged policy as well as technical issues in cryptography."⁶¹² He was also given credit for the initial portion of AES development effort, which I found to be consistent with the behaviors suggested by the RAM. Contending with this governing variable explanation is a simpler explanation that the private sector was better at technology leadership.

I found that the private sector had a technology leadership advantage over NIST and NSA. Thus, actors in the Government Agencies Group realized that future technology solutions, such as AES, would come from the private sector. This utility maximizing behavior was single-loop learning. In addition, the national security government sector may adopt a modified AES to secure classified information. If this proves to be the case, then NSA's realization that secretive government encryption algorithms are no better than less expensive market-based solutions will be simple rational actor logic. The idea of the national security sector using commercial

⁶¹¹ Argyris, *On Organizational Learning*, 68.

⁶¹² Burr, "Data Encryption Standard," 250-253.

information security solutions may represent the future direction of the digital encryption paradigm.

Seifert's research on instruction-sense and regulation-sense rules offered a further explanation for the behavior of the Government Agencies Group in the Competitive Period. His research showed that NSA influenced Congress in a negative way, which caused Congress to introduce "pro-encryption bills."⁶¹³ Actors in the Government Agencies Group required legislations on both escrowed-key encryption and encryption-hindered digital signatures in order to compete against market-based alternatives. During this period, complete encryption systems based on DES-equivalent secret key and RSA public key encryption subsystems were available on the market. The market value of satisfying information access requirements was not yet established, as encryption use just started to increase along with computer ownership and Internet connectivity. However, the market values of EES and DSS-based solutions were significantly reduced by the lack of user trust in government solutions.

Only a government mandate could overcome the competitive advantages of market-based information security solutions. My work in examining congressional testimonies found that the Director of NIST and the Director of NSA attempted to be the action channels for the executive branch. Working against the executive branch were action channels in Congress, who were normally committee chairs. The resulting policy impasse left NSA and NIST without forceful legislation mandating the use of encryption

⁶¹³ Seifert, 100.

technology favorable to satisfying information access requirements. Allison, in his GPM, accepted the notion that action channels with conflicting political support could fail, and claimed, “[T]he context of shared power but separate judgments about important choices means that politics is the mechanism of choice.” With politicians choosing not to support encryption control with laws, the resulting actions by the Government Agencies Group followed past routines in the development of voluntary standards on escrowed-key encryption and digital signatures. Figure 5-4 shows that in the Competitive Period, actors in the Government Agencies Group exhibited a Favored Alternative (solutions) valance of “past precedents and routines,” which matched the behaviors suggested by the OBM and not the “new laws and regulations” valance suggested by the GPM.

My finding of GPM behaviors being exhibited by the Government Agencies Group during the Competitive Period is consistent with one of Pednekar-Magal’s findings. In her research supporting the managerialist perspective, she found that NSA was active in shaping legislation such as *Communications Assistance to Law Enforcement Act*, in satisfying the information access and security agendas of the Bush and Clinton administrations, and in technology leadership with the introduction of the Escrowed Encryption Standard.⁶¹⁴ Figure 5-4 shows that during the Competitive Period, the Lead Actor, Problem Perception, and Decision Timing valances were associated with the GPM. This association implies that that the decision behaviors of NSA dominated the decision behaviors of NIST during this period.

⁶¹⁴ Pednekar-Magal, 76-96.

My research adds to this implication with the finding that NIST developed Digital Signature Standard was handicapped in its encryption capability. Although NIST rationalized its DSS decisions in terms of avoiding the royalties of using the RSA algorithm, avoiding the export controls on encryption capable algorithms, and being faster than RSA in certain conditions, the participation of NSA in DSS decisions was strongly suggested. NSA's past behavior in suppressing public key encryption technology suggested that NSA would not support the use of encryption capable RSA. Pednekar-Magal's research does not explain why the Favored Alternative valance matched "past precedents and routines."

Morgan's research on encryption control and virtual epistemic communities found that the actions of the National Security Agency were in opposition to the desires of academicians, businesses owners, civil rights and privacy organizations, and congressional members.⁶¹⁵ Despite this opposition, actors in the Government Agencies Group were still able to develop highly secure, albeit restrictive, encryption standards. The developments of DSS and EES during the Competitive Period were the results of capable technology leadership within the government's national security community. While Morgan was able to consider the largely civilian virtual epistemic community, her research did not examine a physical community of NSA technologists, former NSA technology experts working for NIST, and quasi-government technology corporations such as MYKOTRONX. Figure 5-4 shows that the actions of this physical community

⁶¹⁵ Morgan, 285-321

matched a Lead Actor valance of the “government sector,” which suggested behaviors described by the GPM. In addition, a comparison of Lead Actor valances in Figure 5-3 and Figure 5-4 during the Competitive Period hints that the Executive Group supported the Government Agencies Group in its struggle against Morgan’s virtual epistemic community.

In summary, my research findings show that actors in the Government Agencies Group originally exhibited decision behaviors consistent with Allison’s OBM and then exhibited behaviors largely consistent the GPM in the Competitive Period. Seifert’s finding that NSA sought policy leadership from Congress supported my assignment of a “government sector” Lead Actor valance. The findings of Pednekar-Magal on NSA’s escrowed-key encryption development and lobbying activities were consistent with a transition of decision behaviors during the Competitive Period. Morgan’s research did not cover the actors that might have supported my notion that the Government Agencies Group was capable of technology leadership. Actors in this group required political support from the executive and legislative branches in the form of laws mandating the use of government developed encryption systems. My research shows that escrowed-key encryption came close to being successful during the Competitive Period, but ultimately failed because of competitive interactions among the groups.

Interactions

The patterns of the valances from four actor groups plotted against three analytical periods demonstrate the interactions among groups. Figure 5-5 shows three general decision patterns over time, which I have labeled as consistent, transient, and convergent decision behaviors. My analysis showed that the Encryption Technology Group exhibited RAM decision behaviors all through the First Mover, Competitive, and Status Quo Periods. This consistent string of behaviors was not exhibited by the other groups and suggests that repetitive successes in solving simple information security problems can perpetuate RAM behaviors. IBM's technology leadership and its successful submission of its proprietary encryption algorithm, which became the Data Encryption Standard, initiated a string of successes by other actors in the group. The next critical success was the private sector's discovery and development of public key encryption, thereby enabling the production of complete encryption systems.

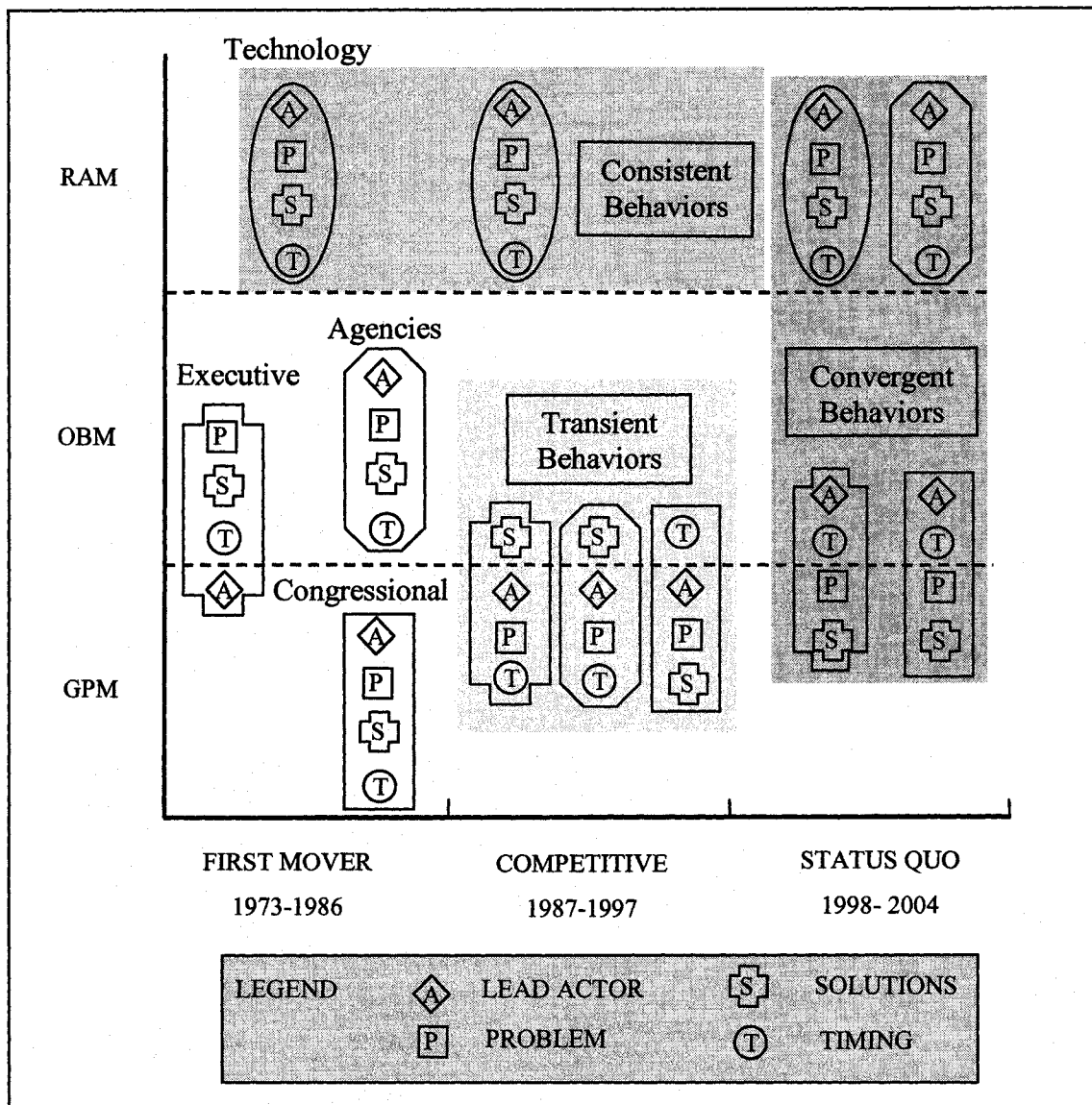


Figure 5-5 Actor group decision behaviors over three periods showing consistent, transient, and convergent groupings

During the Competitive Period, actors in the Encryption Technology Group were ready with several choices of secret key and public key encryption subsystems to compete in the market and against offerings by the government. I found that the

government's complete encryption solution in the form of the Escrowed Encryption Standard lacked trust and value when compared to private sector solutions, such as DES teamed with the RSA public key encryption algorithm. In the area of digital signatures, the government's Digital Signature Standard was less valuable than RSA in both the government and private sectors, because RSA was readily adaptable for digital signature use, and conversely, the Digital Signature Algorithm was not readily adaptable for encryption use. These market success shielded actors in the Encryption Technology Group from dramatic changes and from sophisticated organizational learning behaviors that may be required to overcome future failures.

In the changing national security and public safety context of the Status Quo Period, actors in the Encryption Technology Group continued to develop competitive technology solutions for the more dominant information security problem. Actors in the Congressional and Executive Groups realized that they did not have the technology leadership to solve the information security problem and had to rely on the activities of the Encryption Technology Group. Actors in this group primed the policy agenda by publicly proving that DES was obsolete and by participating in a competition to replace DES.

Although the Belgian Rijndael encryption algorithm eventually won the Advanced Encryption Standard competition, actors in the Encryption Technology Group readily accepted the outcome and incorporated AES into information security solutions. These RAM behaviors required the involvement of the Government Agencies Group to make

AES a reality, and in doing so, this group adopted RAM behaviors. An unexpected output of RAM behaviors was the incorporation of information access capabilities into information security solutions. The use of certificate authorities to maintain and archive encryption keys now appears to be an acceptable solution to the private sector because the government was not involved in the decision.

Other scholars have studied the transient behaviors of the Congressional, Executive, and Government Agencies Groups during the Competitive Period. However, they did not bracket their results with prior and post-period research. My research findings covered the periods before and after the Competitive Period. Figure 5-5 shows that during this period, these three actor groups exhibited valances largely corresponding to GPM behaviors and exhibited one valance apiece, corresponding to OBM behaviors. As these groups favored mostly GPM behaviors, researchers tend to consider all government actors as belonging to a single group that was in competition with actors from the private sector. Such a treatment does not account for the large decision behavior changes exhibited by the Government Agencies Group, which went from exhibiting OBM behaviors during the First Mover Period and ended by exhibiting RAM behaviors during the Status Quo Period. Transient decision behaviors may be explained by decision failures and by single and double-loop learning responses.

Actors in the Government Agencies Group experienced failures in the Competitive Period and were forced to change decision behaviors because they lacked supportive information and encryption control laws. By having to compete against the private

sector, its actors produced the Escrowed Encryption Standard and the Digital Signature Standard, which had lower perceived utilities than commercial products. Without a legislative mandate, restrictive government standards could not displace the widespread use of DES and RSA encryption subsystems. These failures caused actors in the Government Agencies Group to believe in private sector technology leadership, as it became apparent that private sector actors better understood user requirements, had higher user trust, and could produce utility maximizing products. In addition, private sector actions; such as free Pretty Good Privacy Software, court challenges to encryption export controls, and DES code breaking contests; targeted public opinion by showing that NSA and NIST no longer had a monopoly on encryption technology. Actors in the Government Agencies Group either had to join with the Encryption Technology Group or had to muster new laws from the Congressional and Executive Groups.

During the Competitive Period, actors in the Congressional Group believed that the government was the lead actor for a complex information control problem with international and domestic dimensions. In the First Mover Period, my work showed that actors in this group had a Decision Timing valance associated with the GPM, but subsequently experienced a transition in their Decision Timing valance to one associated with the OBM. Actors in the Congressional Group learned that they did not have to decide on information control problems in a timely fashion, as evidenced by their successive failures to pass export control laws. In addition, congressional indecision left open the balance between laws to liberalized encryption, such as the committee-bound *SAFE Act*, and proposed laws to control encryption, such as the unsuccessful attempt to

create a government-run key escrow. However, Congress did decide on pivotal information control legislations, such as the *Communications Assistance to Law Enforcement Act* and the *Economic Espionage Act of 1996*. These laws were incremental steps in balancing domestic information access and security requirements.

Tacit and incremental decisions by the Congressional Group affected the behaviors of other groups by enticing actors in the Executive Group to make their own export policies to control dual-use technology and by leaving actors in the Government Agencies Group without a mandate for encryption control standards. In the Competitive Period, the executive branch used a sequence of executive orders to manage export policy, while Congress tacitly approved this policy by failing to pass a comprehensive export control law dealing with information and encryption technologies. On the domestic side of information control, Congress avoided political risk by allowing NIST and NSA to implement an escrowed-key encryption scheme in the non-defense federal and private sectors without a supportive law. This lack of congressional support hurt actors in the Government Agencies Group and was a factor in their decision behavior change during the Status Quo Period. However, this lack of support had minimal repercussions for the Congressional Group because the predicted information access crisis did not occur. Therefore, actors in the Congressional Group changed their governing variable on decision timing from a crisis mode in the First Mover Period to a more incremental and tacit mode in the Competitive Period. By doing so, they avoided a political crisis with the executive branch on export policy and made steady progress in solving a complex information control problem with two laws. The *Communications*

Assistance to Law Enforcement Act and the *Economic Espionage Act of 1996* proved useful in the subsequent Status Quo Period and reinforced the actions of the Congressional Group.

Actors in the Executive Group experienced a transition from mostly OBM decision behaviors in the First Mover Period to mostly GPM decision behaviors in the Competitive Period, as shown in Figure 5-5. I found that these changes were the results of the elevated importance of information security requirements in the Information Age and of the perceived threat from the Soviet Union, which was desperate for technology. Executive orders and presidential directives allowed a national security state to take incremental actions without waiting for Congress to help with perceived national security problems. In the First Mover Period, actors in the Executive Group believed that the government was the lead actor for solving national security problems. An example of this was President Reagan's release of National Security Decision Directive 145. This 1984 directive created the sensitive but unclassified information category by claiming that pieces of unclassified data could be computer processed into classified information. The thefts of United States technology by the Soviet Union motivated actors in the Executive Group during the next period.

The effects of NSDD-145 were more pronounced in the Competitive Period when computers and digital data became prevalent. During this period, actors in the Executive Group tried to control sensitive but unclassified information in both the government and private sectors. Figure 5-5 shows that the Favored Alternative (solutions) valance was

one of using “past precedents and routines,” because the Bush and Clinton administrations were unable to convince Congress on the wisdom of legislating government information control beyond the national security area. By expanding an information dimension governing variable to now include all information critical to national security and the economy, actors in the Executive Group provided for better protection of the critical information infrastructure. However, these actors encroached upon proprietary and privacy information.

Figure 5-5 shows that all actor groups exhibited convergent decision behaviors during the Status Quo Period. The convergence of the Government Agencies Group and the Encryption Technology Group to the decision behaviors described by the Rational Actor Model demonstrates both the consistency and flexibility of the Lead Actor valance. Actors in the Encryption Technology Group consistently believed that the private sector was the better encryption technology leader when compared to the government sector. Actors in the Government Agencies Group did not share this belief until the Escrowed Encryption Standard failed during the Competitive Period. Part of this failure can be attributed to private sector actions, which found flaws with the security products produced by closed and secretive development processes favored by NSA. In time, actors in Government Agencies Group found that the use of open development processes could produce utility maximizing alternatives. Greater participation in open development processes produced greater trust in encryption technology solutions, while uncovering latent technical flaws.

Actors in the Government Agencies Group showed flexibility when reacting to failure. They accepted private sector technology leadership in solving a simple information security problem. This change was rewarded in the Status Quo Period by the success of NIST's Advanced Encryption Standard competition. In contrast to the early 1970s Data Encryption Standard competition where IBM had the only viable submission, I found that the AES competition received over a dozen submissions from the private sector and found that NSA elected not to participate with a submission. NIST did not require engineering expertise to develop the new standard, but did require an ability to manage the selection of the encryption algorithm with the best utility. NIST acted according to behaviors described by the RAM and was the dominant actor in the Government Agencies Group during the Status Quo Period.

The attack on September 11, 2001 reinforced requirements for protecting the critical information infrastructure with better information security solutions, many of which now use the Advanced Encryption Standard. AES use makes it improbable that information access requirements can be satisfied through encryption cracking. In addition, research efforts and resources applied to cracking schemes may be better expended on accessing certificate authorities. Instead of relying on encryption cracking or legal mandates to gain information access, actors in the Encryption Technology Group have followed RAM behaviors and have introduced information access capabilities into commercial information security products. NSA has always required information access to encrypted national security data for information assurance and COMSEC purposes, and now, NSA may be able to access encrypted information from all sectors by applying

legal and coercive pressures to encryption certificate authorities. It remains to be seen if NSA and the private sector can fulfill the information access requirements created by the *Intelligence Reform and Terrorism Prevention Act of 2004*. If not, the actors in the Government Agencies Group may see the government sector as being the better lead actor to balance information access and security requirements.

During the Status Quo Period, actors in the Congressional and the Executive Groups exhibited identical mixtures of OBM and GPM decision behaviors. This convergence was a result of changing governing variables and interactions among the groups. Figure 5-5 shows that actors in the Congressional Group displayed Lead Actor and Decision Timing valances described by the OBM. Also during the Status Quo Period, actors in this group learned that the government did not have the technical expertise or public trust to solve the information control problem and would have to work with the private sector. When Congress passed the complex *Digital Millennium Copyright Act* in 1998, actors in the Congressional Group soon found that protecting digital content originators against foreign circumvention measures hurt information security development in the private sector. This lesson from the imperfect *DMCA* served to reinforce the importance of combined private and government sector leadership. The subsequent 2000 *E-SIGN Act* exemplified this consortium approach because this law was technology neutral and did not favor specific industries or technologies. By passing the *E-SIGN Act*, actors in the Congressional Group also favored an “incremental / tacit” Decision Timing valance associated with OBM. The *E-SIGN Act* legalized electronic signatures using public key encryption and deferred decisions on the export and global

use of the underlying public key encryption subsystem. My work shows that actors in the Congressional Group continued this “incremental / tacit” behavior in the Status Quo Period and amplified their governing variable on making incremental decisions.

After the September 11, 2001 attack, actors in the Congressional Group continued to believe that a series of laws could eventually solve a complex information access and security problem with international and domestic dimensions. The *USA PATRIOT Act*, *Homeland Security Act of 2002*, *Cyber Security Research and Development Act*, and the *Intelligence Reform and Terrorism Prevention Act of 2004* demonstrated Congress’ preference for laws, albeit segmented laws. While this preference for laws matched the behavior suggested by the GPM, the incremental nature of these laws continued to reinforce the decision timing governing variable of this group and may have influenced the decision timing behavior of the Executive Group.

Before the terrorist attack on the United States, actors in the Executive Group exhibited Lead Actor and Decision Timing valances associated with the OBM. Figure 5-5 shows that the Executive Group lost the exclusive use of the technology leadership functions of the Government Agencies Group to RAM behaviors and to actors in the Encryption Technology Group. However, the 1998 PDD/NSC-63 on critical infrastructure protection required the development of information security tools to protect the information infrastructure. Thus, actors in the Executive Group had to work with the private sector, because this sector presented the greatest information infrastructure vulnerabilities and possessed the required technology leadership to reduce these

vulnerabilities. The net result was that the Executive Group exhibited the same “consortium” Lead Actor valance as the Congressional Group, with both groups being driven to work with the private sector for essentially the same reasons.

During the Competitive Period, the Government Agencies Group had the same Lead Actor valance as the Congressional and Executive Groups. This valance was transitory because the technology leadership potential of the Government Agencies Group dwindled during the Competitive Period. Figure 5-5 suggests the importance of the Lead Actor valance in predicting the convergent decisions behaviors of the four groups. By examining the patterns of the Lead Actor valances or “A” diamonds, the First Mover Period shows a 1:1:2 distribution among RAM, OBM, and GPM decision behaviors, respectively. The Competitive Period shows a 1:0:3 distribution, with the Lead Actor valance of the Government Agencies Group changing to GPM decision behaviors. After the collapse of the Escrowed Encryption Standard, the Lead Actor valance of the Government Agencies Group became associated with RAM decision behaviors in the Status Quo Period. The resulting 2:2:0 distribution of Lead Actor valances suggests that the Congressional and Executive Groups were forced to act as a consortium with the private sector because of the convergent behaviors of the Encryption Technology and Government Agencies Groups. As discussed earlier, the Congressional and Executive Groups did not have the technology leadership or trust to exhibit Lead Actor valances associated with GPM behaviors during the Status Quo Period. The terrorist attack on September 11, 2001 may have prevented both groups from abdicating policy leadership of the information security problem to the private sector.

The Executive and the Congressional Groups exhibited the same “incremental / tacit” Decision Timing valances in the Status Quo Period, because both groups were dependent on the legislative cycle for information control laws and the Executive Group was able to complement these segmented laws with executive orders and presidential directives. Figure 5-5 shows that actors in the Executive Group exhibited an “urgent / crisis” Decision Timing valance in the Competitive Period, but changed this behavior to “incremental / tacit” in the Status Quo Period. This change represented a tacit understanding between the executive and legislative branches to abandon making urgent decisions on information and encryption control, but not to surrender these decisions to the private sector and the market. A good example of complementation continues to occur with encryption export control, whereby the executive branch makes a string of export control decisions, and Congress retroactively supports these decisions with law. This complementary decision timing interaction appears to be agreeable and stable between the Executive and Congressional Groups, even to the extent of resisting crisis-action encryption control decisions called for by political leaders from both parties after the September 11, 2001 attack. The Executive Group experienced continued successes with incremental decisions and actors in the Congressional Group used incremental decision timing as a governing variable.

Figure 5-5 shows that during the Status Quo Period, actors in the Executive and Congressional Groups exhibited Problem Perception and Favored Alternative valances associated with the GPM. This alignment was not coincidental, as the terrorist attack reinforced the perception of a complex information control problem with international

and domestic dimensions. President Bush issued Executive Order 13231 on critical infrastructure protection a month after the attack and added policy details with his Homeland Security Presidential Directive / HSPD-7, which was issued in 2003 after passage of the *Homeland Security Act of 2002*. These directives emphasized protecting the critical information infrastructure, which now had a global expanse. In addition, these directives effectively expanded the information dimension governing variable of the Competitive Period to now cover this global expanse. Although logically correct in that the weakest link of a global information system limits overall security, the global control of sensitive but unclassified information was a governing variable that now added to the complex problem.

Although actors in the Executive Group believed that new laws were required to solve this complex information security problem, the Congressional Group limited the scope of these laws. Actors in the Executive Group experienced serious congressional opposition to such laws in the Competitive Period, but believed that the post-attack national security environment would justify expansion of information control measures internationally and into the non-defense government and private sectors. However, the fact of having a segmented *Homeland Security Act of 2002* and *Intelligence Reform and Terrorism Prevention Act of 2004* is sign of friction in the GPM behaviors of Executive and Congressional Groups.

If the expanding information dimension governing variable gives the government free access to privacy and proprietary information, then the status quo among these

groups may be broken. The result may be a return to the decision behaviors found in the First Mover Period where the Executive Group exhibited mainly OBM behaviors and the Congressional Actor Group exhibited GPM behaviors. In the mid-1970s, these behaviors resulted from Congress' distrust of the executive branch in protecting privacy rights and controlling private sector economic and technology information. Thirty years later, actors in the Executive Group may expand their governing variable and pursue encryption technology solutions that force information access. Congress may then have to decide on a counter-balancing information security law, as they did with the *Privacy Act of 1974*.

Chapter Six: Conclusion

The tumultuous events of September 11, 2001 did not produce Draconian information control policies in the United States because the major policy actor groups were in a status quo produced by three decades of making information and encryption control decisions. Although Kingdon's problem, policy, and political streams converged in an October 2001 policy window to produce the *USA PATRIOT Act*, no such window occurred for information or encryption control policy. Prognosticators of information control policies waited for actors in the executive branch and in the government agencies to champion guaranteed access to information, which would be critical for national security and public safety functions. What did occur was a reinforcement of information security requirements on the nation's critical information infrastructure. Actors in the private sector and the information technology market were ready for this event with reasonably priced and sophisticated information security tools.

In an unexpected move, the market also supported the development of balanced information security tools. Such tools, long sought by the government for mandatory use in the private sector, will allow trusted third parties access to encrypted information for information assurance and data recovery purposes. This state of affairs is the result of an organizational and political status quo between actors in the Executive and Congressional Groups.

Allison's Decision Models as an Analytical Tool

My work arranged popular data on encryption events and actions according to actor groups, used valances to fit this data into patterns, and subsequently matched these patterns to the behaviors suggested by existing decision models. Like most models that serve to simplify, explain, and predict, Allison's decision models have found applications beyond their original national security policy area and into such areas as business policy, economic policy, public policy, and technology policy.⁶¹⁶ In my work, I expanded the Rational Actor Model to account for multiple actors, the Organizational Behavior Model to account for learning behaviors, and the Governmental Politics Model to better account for all three branches of government. The results of using Allison's decision models to answer five research questions are measures of my success at these tasks.

Who are the major encryption control policy actors? I found that encryption policy actors are intrinsically related to information control policy actors and that these actors reside primarily in the United States. Currently, these actors are equally distributed in both the government and private sectors and have been so since the 1970s. From the time of electromechanical rotor machines of the early twentieth century to the 1977 Data Encryption Standard, United States information technology leadership has been contested within the government sector and between the government and private sectors. My research on the development of the Advanced Encryption Standard suggests that in the

⁶¹⁶ This model expansion is apparent when comparing Allison's 1971 version of *Essence of Decision* with his 1999 version.

twenty first century international actors may have a significant influence on United States information control policy. Evidence of this influence was seen in the AES development, in which a Belgian algorithm was selected. As the AES is now a globally available information security tool, global actors can strengthen the security of the Internet by strengthening their weakest links. Global actors will have to be considered in future information policy research.

What conceptual groups of actors emerge when major encryption events occur? I found that actors could be placed in one of four conceptual groups according to their branches of government or their functions in information control technology development and marketing. I used four actor groups for my longitudinal analysis that covered three decades of encryption related events. In my research, actors remained in the same Congressional Group, Encryption Technology Group, Executive Group, or Government Agencies Group for all three analytical periods, as the stability of these groups was based on the structure of the United States government and its free-market economic system. In addition, my four groups provided more analytical breadth than the normal government and private sector groups used by other scholars because using a large monolithic government actor group would have homogenized the different decision behaviors of the executive and legislative branches and the decision behaviors of the semi-autonomous government agencies responsible for information technology. Using four static groups helped my research to avoid the dynamic effects caused by emerging international actors and by virtual communities that can cross group boundaries.

In the course of research, I uncovered some evidence that suggested a differentiation of subgroups within the broad Encryption Technology Group. A specific example occurred when intellectual property originators pushed for anti-circumvention laws in the 1998 *Digital Millennium Copyright Act* instead of developing suitable information security measures. The recent introduction of information access features into commercial information security systems and the growing use of encryption-based digital rights management systems may cause disparate decision behaviors within this group. Disparate behaviors may require separate analytical groups for at least the electronic rights advocates and the intellectual property originators.

How strongly do the actions of these conceptual groups correspond with the patterns suggested by Allison's decision models? I found that by using Lead Actor, Problem Perception, Favored Alternative, and Decision Timing valances, three of four actors groups completely matched the behaviors suggested by Allison's decision models in at least one period. Only the Executive Group exhibited mixed behaviors during each analytical period. In *Essence of Decision*, Allison inferred the possibility of an actor group exhibiting mixed behaviors by applying each of his models to a critical scenario before permitting the reader determine the better-fit decision model. In my work, I elected to analyze many sub-critical actions and events using four valances and then determined the better-fit decision model. I believe my methodology satisfies Allison's advice that only by "putting on each of the alternative lenses in turn" can one reach a

conclusion on the appropriate Allison model.⁶¹⁷ I found that the Executive Group exhibited a majority of valances favoring the OBM during the First Mover Period and then favoring the GPM during the Competitive Period. One explanation for this change in decision behaviors was a shift in the Problem Perception and Decision Timing valances during the George H. W. Bush and Clinton administrations caused by the realization of a vulnerable critical information infrastructure in the United States. Similarly, the evenly mixed and symmetrical OBM and GPM behaviors exhibited by the Executive and Congressional Groups during the Status Quo Period suggest a stable interaction between the executive and legislative branches on information control policy.

Why do competitive and interactive groups show convergence toward common decision models? I found that actor groups do exhibit convergent decision behaviors given a sufficiently long interaction period. My encryption control case study analyzed events and actions over a three-decade period to arrive at this conclusion. The Encryption Technology Group exhibited consistent RAM behaviors because their technology leadership enabled development of utility maximizing solutions, which the market valued. The consistent valances of the Encryption Technology Group served not only as a RAM standard for analysis, but also as a reinforcement of the principles espoused by Allison for rational actor behavior.⁶¹⁸ The Government Agencies Group exhibited OBM behaviors at first, then transitioned through mixed GPM and OBM behaviors, and finally converged to RAM behaviors in the Status Quo Period. This

⁶¹⁷ Allison and Zelikow, *Essence of Decision*, 11.

⁶¹⁸ *Ibid.*, 23-26.

convergence was a reaction to an encryption control failure caused by actors in the Congressional and Executive Groups during the Competitive Period. The failure of the Escrowed Encryption Standard in the market and the success of commercial information security products from vendors, such as RSA Security, made it apparent to actors in the Government Agencies Group that the private sector was better at producing information security solutions. In adapting RAM behaviors, actors in the Government Agencies Group used at least single loop learning to select the private sector as the lead actor able to produce utility maximizing solutions. Actors in this group may have used double-loop learning by employing learning-leaders that worked in industry, NIST, and NSA. This claim is an area for future research.

The convergent decision behaviors of the Congressional and Executive Groups were the results of complementary organizational learning events and their realizations of the vulnerable information infrastructure in the United States. Well before the September 11, 2001 attack, the Executive Group changed a governing variable on the nature of information requiring protection and the Congressional Group changed a governing variable on incremental decision timing. Both changes had their origins in the Competitive Period when advances in computer technology and the Internet allowed mass use of complete, secret and public key, encryption systems. These two actor groups never settled the policy debate on the right balance between information access and security. Instead, a retreat from information access demands by the Executive Group and a steady supply of incremental laws from the Congressional Group produced an effective working relationship between these two groups during the Status Quo Period. Both actor

groups realized that they did not have the required technology expertise to be policy leaders and did not have the political consensus to drive the decision agenda and timing. However, the resulting OBM behaviors of these two groups allowed productive interactions with the private sector and the market. Limiting the OBM behaviors of both groups was the concurrent belief of a complex international problem that required laws and regulations to protect national security and public safety. The net effect of this status quo after September 11, 2001 was an executive branch interested in protecting critical information systems in the government and private sectors and a legislative branch interested in successive and measured laws that would not tip the balance of power in favor of the sitting administration.

How stable are these interactions among decision models when projecting future policy decisions? By using Allison's decision models, I found that a policy balance exists in the Status Quo Period with the Encryption Technology and Government Agencies Groups exhibiting RAM behaviors and the Congressional and Executive Groups exhibiting an even mix between OBM and GPM behaviors. Groups exhibiting RAM behaviors are likely to continue following such behaviors until there is a failure in technology leadership or the information security market. Failures could arise from finding a catastrophic flaw in the Advanced Encryption Standard or from finding a mathematical factoring technique that defeats RSA public key encryption. It is unlikely that single loop learning changes will overcome such failures, and the government may have to intervene first with crisis action measures and then by encouraging research and

development with laws. The 2002 passage of the *Cyber Security Research and Development Act* suggests that the government is preparing for such a scenario.

Actors in the Congressional and Executive Groups are unlikely to change decision behaviors that are the operational products of governing variables. Information security in both the government and private sectors is critical in the age of information warfare. Constant national security and public safety fears caused by the threat of information warfare have elevated the importance of the information dimension governing variable that drives the Executive Group. Working to balance the activities of the Executive Group, actors in the Congressional Group have passed a series of incremental, but successful, laws on pieces of the information control problem. Post attack laws, such as the *USA PATRIOT Act*, *Homeland Security Act of 2002*, *Cyber Security Research and Development Act*, and the *Intelligence Reform and Terrorism Prevention Act of 2004*, have reinforced the incremental decision timing governing variable that drives the Congressional Group. Having withstood the attack on September 11, 2001 without incurring dramatic changes in information control policies, future information warfare attacks may only serve to renew and reinforce the status quo of governmental actions in the United States.

The stable relationship between the Congressional and Executive Group may be susceptible to an over-reliance on private sector technology leadership and to possible market failures. A public loss of trust in information security tools may result from careless or criminal activity within the many certificate authorities required to operate a

global encryption system. If the United States had adopted government control of encryption technology, as envisioned with escrowed-key encryption, then damage assessment and control could be run like a crisis action event. The government would be fully accountable to the public in this case. With the ubiquitous use of commercial information security tools, the only accountability currently may be the refunding of the few dollars that users paid for information security services. An uncompensated loss of valuable information may require government action. Such action may cause a reevaluation of the governing variables used in the Status Quo Period and a significant following of the decision behaviors suggested by the GPM.

Implications for United States Technology Policymaking Field

I used an expansion of Allison's decision models to analyze three decades of United States encryption policy actions and events. By extending the use of his models beyond a single event, such as his seminal analysis of the Cuban Missile Crisis, I have found that the Rational Actor, Organizational Behavior, and Governmental Politics Models have descriptive and explanatory powers useful to policymakers. By using a qualitative analysis methodology suggested by Robert K. Yin and by using multiple groups of actors and analytical valances to pattern match group behaviors to those suggested by Allison's decision models, my work adds to the depth and breadth of knowledge in the technology policy field.

Relevant previous literature; as determined by scholars such as Seifert, Pednekar-Magal, and Morgan; suggests that the Escrowed Encryption Standard case was a definitive event in the history of United States information control policymaking. My research expands Seifert's finding of "Mixed Regimes" or the use of "instruction sense" and "regulation sense" policy rules into a longitudinal finding of policy competitions among government actors and between government and private sector actors. I found that the Escrowed Encryption Standard failed because it required the force of law to compete with market-based information security solutions.

My work amplifies Pednekar-Magal's "managerialist perspective" finding in that government actors did exhibit a mixture of OBM and GPM behaviors in the early 1990s. As a result of these mixed behaviors, government actors could not completely agree on an information control solution and when this solution would be needed. My research methodology is challenged by Morgan's finding that an interactive "Virtual Epistemic Community" may be responsible for information control policymaking. When actor groups are differentiated by their interaction mechanisms and not by their philosophical perspectives or common goals, then such groups may be too dynamic to be treated as units of analysis in a longitudinal study. The composition of actor groups remained relatively static for three decades, but the Encryption Technology Group may have to be separated into smaller groups for future research.

In the general field of technology policymaking, the sudden convergence of problem, policy, and political streams in Kingdon's "Policy Window" model may explain

the rapidity of legislation such as the *USA PATRIOT Act*, but does not provide the analytical framework required to examine the detailed interactions within each stream.⁶¹⁹ The transformation of a condition into a problem coupled with a solution is perhaps the most difficult phase of technology policymaking. When a solution has to be managed or developed, policymakers require a prerequisite level of technical expertise. For example, policymakers had to make an educated decision that modern encryption systems were unbreakable if these systems were to be used to guarantee information security. Yet, many of these same policymakers assumed that the government could break encryption schemes in order to access critical information when satisfying national security and public safety functions. By using Allison's decision models as an analytical framework, I found that this assumption was false and that public policy decisions on information access requirements were politically deferred, despite having an escrowed-key encryption solution available. Explanations of why groups of actors redefine difficult parts of a problem or take incremental steps toward a solution are not completely detailed in Allison's models.

I found that organizations and organizing processes can produce technology policies in a more efficient manner than portrayed by Allison's alternative Organizational Behavior and Government Politics Models or by an organizations, people, context, and

⁶¹⁹ Kingdon, *Agendas, Alternatives, and Public Policies*, 165-170.

change model as alluded to by James Q. Wilson in *Bureaucracy*.⁶²⁰ Argyris may be closer to elucidating how organizations change organizing behaviors when confronted by dramatic changes or failures. Consistent RAM behaviors exhibited by the Encryption Technology Group suggest that single-loop learning and its successive searches for the optimum solution is preferred when solving simple problems. When single-loop learning fails, Argyris suggests that double-loop learning can change the governing variables of an organization.⁶²¹ Learning organizations are better able to make technology policies because such organizations adapt to change faster than traditional organizations. I believe that if the information security market fails, then future policies will be set either by the Department of Homeland Security or by the new national intelligence organization. Future information technology policies may be determined by the more adaptable organization, and future researchers will have an expanded technology policymaking field to continue the investigation.

Future United States Technology Policymaking

The future of United States encryption control policymaking depends on a basic assumption regarding the technology market. Will government intervention be required if the market fails? Encryption liberalization proponents would generally say no to government intervention, but actors in the Encryption Technology Group have only

⁶²⁰ James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989). He does not layout a succinct model and one must peruse the entire book to arrive at one.

⁶²¹ Chris Argyris, *On Organizational Learning*, 67-69.

experienced a string of successes and have no experience in recovering from catastrophic information security failures. Encryption control proponents would note that one function of government policy is to mitigate market failures especially when the national security and public safety of the United States is threatened. A proactive public policy to prevent market failure is preferable to a reactive policy that would limit the damage caused by failure.

A proactive information control policy should make use of my finding that a status quo exists among actors following RAM behaviors and actors following mixed OBM and GPM behaviors. A proactive policy has already been set in motion by the information access capabilities of commercial information security solutions. The government can now gain access to information for national security and public safety purposes. However, certificate authorities will be the center of gravity for a global information system, and certificate authorities should be the target of public policy. A proactive policy design should include government regulation of encryption certificate authorities to ensure that they are trustworthy, accountable, and reliable. In a form similar to banking regulations, the government could limit the amount of risk that certificate authorities take by preventing the commingling of domestic and foreign certificates, by preventing hostile actors and criminal elements from obtaining encryption certificates, and by periodically inspecting and testing the system. There would be a loss of anonymity with Internet transactions and communications as public key encryption certificates and signatures become associated with specific users. In essence, a national digital communication and identification card would come into being by the use of

encryption certificates. However, Americans may be able to sacrifice some measure of their privacy rights to ensure the economic, national security, and public safety health of the nation, but only if solutions are not forced upon them by a powerful central government.

Bibliography

Bibliography

- Ackerman, Wytan M. "Encryption: A 21st Century National Security Dilemma." *International Review of Law, Computers & Technology* 12, no. 2 (July 1998): 371-394.
- Adleman, Leonard M. "Implementing an Electronic Notary public," *Crypto '82*. In *Advances in Cryptology 1981-1997: Electronic Proceedings of the Crypto and Eurocrypt Conferences 1981-1997*. Edited by David Chaum, Ronald L. Rivest, and Alan T. Sherman. New York: Springer-Verlag, 1998.
- Allison, Graham T. "Conceptual Models and the Cuban Missile Crisis." *American Political Science Review* 63, no. 3 (September 1969): 689-718.
- Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little, Brown and Company, 1971.
- Allison, Graham T. and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2d ed. New York: Longman, 1999.
- American National Standard Data Encryption Algorithm. ANSI x3.92-1981. New York: American National Standards Institute Inc., December 1980.
- American National Standard Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA). ANSI X9.31-1998. New York: American National Standards Institute Inc., 8 September 1998.
- American National Standard Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). ANSI X9.62-1999. New York: American National Standards Institute Inc., 7 January 1999.
- Argyris, Chris. *On Organizational Learning*. 2d ed. Malden, Massachusetts: Blackwell Publishers Inc., 1999.
- Argyris, Chris and Donald A. Schon. *Organizational Learning II: Theory, Method and Practice*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc., 1996.
- Arms Export Control Act. U.S. Code. Vol. 22, sec. 2778 (2001).*

- Arrow, Kenneth J. *The Limits of Organization*. New York: W.W. Norton & Company, 1974.
- Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency*. Boston: Houghton Mifflin Company, 1982.
- Begley, Sharon, Melinda Liu and Joshua Cooper Ramo. "The Code of the Future: Uncle Sam wants you to use ciphers it can crack." *Newsweek* 121, no. 23 (7 June 1993): 70.
- Blaze, Matt. "Protocol failure in the Escrowed Encryption Standard." in *Proceedings of the 2nd ACM Conference on Computer and Communications Security*. New York: ACM Press, 1994.
- Bork, Robert H. *The Tempting of America: The Political Seduction of the Law*. New York: The Free Press, 1990.
- Brooks Act*. *U.S. Statutes at Large* 79 (1965): 1127-1129.
- Burr, William E. "Data Encryption Standard." In *A Century of Excellence in Measurements, Standards, and Technology: A Chronicle of Selected NBS/NIST Publications 1901-2000*. NIST Special Publication 958. Edited by David R. Lide. Washington D.C.: GPO, January 2001.
- Burstyn, H. P. "Slow Growing Encryption market to spurt in '80's." *Electronic Business* (January 1979): 76-77.
- Bush, George H. W. National Security Directive 42. "National Policy for the Security of National Security Telecommunications and Information Systems." 5 July 1990.
- Bush, George H. W. National Security Directive 47. "Counter Intelligence and Security Countermeasures." 5 October 1990.
- Bush, George H. W. National Security Review 18. "Counter Intelligence and Security Countermeasures." 22 June 1989.
- Bush, George W. Homeland Security Presidential Directive / HSPD-7. "Critical Infrastructure Identification, Prioritization, and Protection." 17 December 2003.
- Carter, Jimmy. *Public Papers of the Presidents of the United States: Jimmy Carter, 1980-81*. Vol. 3. Washington, D.C.: GPO, 1982.
- Cate, Fred H. *Privacy in the Information Age*. Washington, D.C.: The Brookings Institution, 1997.

- Clark, Andrew J. "Key Recovery – Why, How, Who?" *Computers & Security* 16 (1997): 669-674.
- Clinger-Cohen Act of 1996. U.S. Code. Vol. 15, sec. 272 (2003).*
- Clinton, William J. Presidential Decision Directive / NSC 5. "Public Encryption Management." 15 April 1993.
- Clinton, William J. Presidential Decision Directive / NSC-63, "Critical Infrastructure Protection," 22 May 1998.
- Cohen, Michael D., James J. March, and Johan P. Olsen. "A Garbage Can Model of Organizational Choice." *Administrative Science Quarterly* 17 (March 1972): 1-25.
- Communications Assistance for Law Enforcement Act of 1994. U.S. Code. Vol. 18, sec. 2519 (2003).*
- Computer Security Act of 1987. U.S. Code. Vol. 15, secs. 271-278h and Vol. 40, sec. 759d. (2003).*
- Computer Security Act of 1987. U.S. Statutes at Large* 102 (1988): 1724-1730.
- Congressional Record. 93rd Congress, 2d sess., 1974. Vol. 120, pt. 27.*
- Congressional Record. 94th Congress, 2d sess., 1976. Vol. 122, pt. 12.*
- Congressional Record. 100th Congress, 1st sess., 1987. Vol. 133 pt. 26.*
- Congressional Record. 103rd Congress, 2d sess., 1994. Vol. 140, pt. 20.*
- Congressional Record. 104th Congress, 2d sess., 1996. Vol. 142, pt. 28.*
- Congressional Record. 104th Congress, 2d sess., 1996. Vol. 142, pt. 80.*
- Congressional Record. 104th Congress, 2d sess., 1996. Vol. 142, pt. 104.*
- Congressional Record. 104th Congress, 2d sess., 1996. Vol. 142, pt. 105.*
- Congressional Record. 104th Congress, 2d sess., 1996. Vol. 142, pt. 129.*
- Congressional Record. 104th Congress, 2d sess., 1996. Vol. 142, pt. 140.*
- Congressional Record. 105th Congress, 1st sess., 1997. Vol. 143, pt. 11.*

- Congressional Record*. 105th Congress, 1st sess., 1997. Vol. 143, pt. 156.
- Congressional Record*. 106th Congress, 1st sess., 1999. Vol. 145, pt. 30.
- Congressional Record*. 106th Congress, 1st sess., 1999. Vol. 145, pt. 31.
- Congressional Record*. 107th Congress, 1st sess., 2001. Vol. 147, pt. 8.
- Congressional Record*. 107th Congress, 1st sess., 2001. Vol. 147, pt. 118.
- Congressional Record*. 107th Congress, 1st sess., 2001. Vol. 147, pt. 119.
- Congressional Record*. 107th Congress, 1st sess., 2001. Vol. 147, pt. 122.
- Congressional Record*. 107th Congress, 1st sess., 2001. Vol. 147, pt. 161.
- Cugini, John. "FORTRAN test programs," in *A Century of Excellence in Measurements, Standards, and Technology: A Chronicle of Selected NBS/NIST Publications 1901-2000*. NIST Special Publication 958. Edited by David R. Lide. Washington D.C.: GPO, January 2001.
- Cyber Security Research and Development Act*. *U.S. Statutes at Large* 116 (2002): 2367-2382.
- Dam, Kenneth W. and Herbert S. Lin. "National Cryptography Policy for the Information Age." *Issues in Science and Technology* (Summer 1996): 33-38.
- Dam, Kenneth W. and Herbert S. Lin, eds. *Cryptography's Role in Securing the Information Society*. Washington, D.C.: National Academy Press, 1996.
- Denning, Dorothy E. "Encryption Policy and Market Trends." 17 May 1997. <<http://www.cs.georgetown.edu/~denning/crypto/Trends.html>>, accessed October 2004.
- Denzin, Norman K. and Yvonna S. Lincoln, eds. *Handbook of Qualitative Research* 2d ed. Thousand Oaks, California: Sage Publications, 2000.
- Diffie, Whitfield. "Cryptographic Technology: Fifteen Year Forecast," Crypto '81. In *Advances in Cryptology 1981-1997: Electronic Proceedings of the Crypto and Eurocrypt Conferences 1981-1997*. Edited by Allan Gersho. New York: Springer-Verlag, 1998.
- Diffie, Whitfield and Martin E. Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory* IT-22, no. 6 (November 1976): 644-654.

- Diffie, Whitfield and Martin E. Hellman. "Exhaustive Cryptanalysis of the NBS Data Encryption Standard." *Computer* 10, no. 6 (June 1977): 74-84.
- Dupree, Hunter A. *Science in the Federal Government: A History of Policies and Activities*. Baltimore: Johns Hopkins University Press, 1985.
- Economic Espionage Act of 1996. U.S. Code. Vol. 18, secs. 271-278h.*
- Economic Espionage Act of 1996. U.S. Statutes at Large* 110 (1997): 3487-3513.
- Edward Thompson Company and West Publishing Company staff editors. *United States Code Annotated: 2003 Popular Name Table*. St. Paul: West Group, 2003.
- Ehrsam, William Friedrich, et al. "Block cipher system for data security." U.S. Patent # 3,958,081, 18 May 1976.
- Electronic Communications Privacy Act of 1986, U.S. Code. Vol. 18, secs. 2510-2521. (2004).*
- Electronic Communications Privacy Act of 1986. U.S. Statutes at Large* 100 (1986): 1848-1873.
- Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. Sebastopol, California. O'Reilly & Associates, 1998.
- Electronic Privacy Information Center. *Cryptography & Liberty 2000 an International Survey of Encryption Policy*. Washington, D.C.: Electronic Privacy Information Center, 2000.
- Electronic Signatures in Global and National Commerce Act. U.S. Statutes at Large* 114 (2001): 464-476.
- Elteto, Laszlo, et al. "Method and system for secure distribution of protected data using elliptic curve systems." U.S. Patent # 5,737,424, 7 April 1988.
- Export Administration Act of 1969. U.S. Statutes at Large* 83 (1969): 841-847.
- Export Administration Act of 1979. U.S. Statutes at Large* 93 (1979): 503-536.
- Feistel, Horst. "Block Cipher Cryptographic System." U.S. Patent # 3,798,359, 19 March 1974.
- Ford, Gerald R. *Public Papers of the Presidents of the United States: Gerald R. Ford, 1974*. Washington, D.C.: GPO, 1975.

Foreign Intelligence and Surveillance Act of 1978. Public Law 95-11. 95th Congress, 2nd session, 25 October 1978.

Garfinkel, Simson L. "Cypher Wars: Pretty Good Privacy Gets Pretty legal." *Wired Magazine* 2, no. 11 (November 1994): 129 and 165-66.

Glendon, Mary Ann. *Rights Talk: The Impoverishment of Political Discourse*. New York: The Free Press, 1991.

Gross, Robin D. "Testimony of Electronic Frontier Foundation (EFF) before Copyright Office Public Hearings on Digital Millenium [Millennium] Copyright Act (DMCA)." 19 May 2000. <http://www.copyright.gov/1201/hearings/robin_gross.pdf>, accessed January 2005.

Hart, David M. *Forged Consensus: Science, Technology, and Economic Policy in the United States, 1921-1953*. Princeton: Princeton University Press, 1998.

Hellman, Martin E., et al. "Cryptographic apparatus and method." U.S. Patent # 4,200,770, 29 April 1980.

Industry Canada. *Cryptographic Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society*. February 1998. <[http://strategis.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/Cryptographypolicy_En.pdf/\\$FILE/Cryptographypolicy_En.pdf](http://strategis.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/Cryptographypolicy_En.pdf/$FILE/Cryptographypolicy_En.pdf)>, accessed October 2004

Inman, Bobby R. "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector." *Signal Magazine* (March 1979): 6-13.

Inman, Bobby R. "Classifying Science: A Government Proposal..." *Aviation Week and Space Technology* (8 February 1982): 10-12.

International Business Machines Corp. "License Under Patents." *Federal Register* 40, no. 52 (17 March 1975): 12138.

Kahn, David. *The Code Breakers: The Story of Secret Writing*. New York: Scribner, 1996.

Kammer, Raymond G. and Vice Admiral W.O. Studeman. "Memorandum of Understanding between the Director of the National Institute of Standards and Technology and the Director of the national Security Agency Concerning the Implementation of Public Law 100-235." 24 March 1989.

- Kingdon, John W. *Agendas, Alternatives, and Public Policies* 2d ed. New York: HarperCollins College Publishers, 1995.
- Kravitz, David W. "Digital signature algorithm." U.S. Patent # 5,231,668, 27 July 1993.
- Landau, Susan, et al. *Codes, Keys and Conflict: Issues in U.S. Crypto Policy: Report of a Special Panel of the ACM U.S. Public Policy Committee* New York: Association for Computing Machinery, June 1994.
- Levy, Steven. "Trying to Find the Key." *Newsweek* 128, no. 16 (14 October 1996): 91.
- Lipset, Seymour Martin. *Continental Divide: The Value and Institutions of the United States and Canada*. New York: Routledge, Chapman and Hall, Inc., 1990.
- Lipset, Seymour Martin. *American Exceptionalism A Double Edged Sword*. New York: W.W. Norton & Company, 1996.
- McCool, Daniel C., ed. *Public Policies Theories, Models and Concepts: An Anthology*. Engle wood Cliffs, New Jersey: Prentice Hall, 1995.
- McKeown, Timothy J. "The Cuban Missile Crises and Politics as Usual." *The Journal of Politics* 62, no. 1 (February 2000): 70-87.
- Micali, Silvio. "Fair cryptosystems and methods of use." U.S. Patent # 5,276,737, 4 January 1994.
- Micali, Silvio. "Fair cryptosystems and methods of use." U.S. Patent # 5,315,658, 24 May 1994.
- Miles, Mathew B. and A. Michael Huberman. *An Expanded Sourcebook: Qualitative Data Analysis*. Thousand Oaks, California: Sage Publications, 1994.
- Money, Arthur L. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. "Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI)." Washington, D.C., 9 April 1999.
- Morgan, Glenda Nadine. "The message and the medium: Electronic communications technologies and global policy change in copyright, privacy and encryption." Ph.D. diss., University of Minnesota, 2001.
- Murray, William H. "The Data Encryption Standard: 20 Years Later," Remarks of panelist, 20th National Information Systems Security Conference, Baltimore, Maryland, October 1997.

National Security Agency Central Security Service. United States Signals Intelligence Directive 18. 27 July 1993. Declassified copy.

National Technology Transfer and Advancement Act of 1995. U.S. Code. Vol. 15, sec. 272 (2003).

Nechvatal, James et al. *Report on the Development of the Advanced Encryption Standard 2 October 2000*. Washington, D.C.: NIST, 2000.

Nixon, Richard. *Public Papers of the Presidents of the United States: Richard Nixon, 1974*. Washington, D.C.: GPO, 1975.

Nunno, Richard M. *Encryption Technology: Congressional Issues*. CRS Issue Brief for Congress, IB96039. 14 July 2000.

Nye, J. Michael. "The Import/Export Dilemma." In *Advances in Cryptology 1981-1997: Electronic Proceedings of the Crypto and Eurocrypt Conferences 1981-1997*. Edited by Alan Gersho. New York: Springer-Verlag, 1998.

Office of Management and Budget. *Access with Trust*. Washington, D.C.: GITS, 1998.

Official Gazette of the United States Patent and Trademark Office 934 (13 May 1975): 452.

Official Gazette of the United States Patent and Trademark Office 949 (31 August 1976): 1717.

Oleszek, Walter J. *Congressional Procedures and the Policy Process* 4th ed. Washington, D.C.: CQ Press, 1996.

Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge, Mass.: Harvard University Press, 1971.

Overbye, Morten. "Teenager Cleared in Landmark DVD Case, CNN.com/Technology," 7 January 2003. < <http://www.cnn.com/2003/TECH/01/07/dvd.johansen/> >, accessed October 2004.

Pednekar-Magal, Vandana. "State surveillance and the telecommunication policy process: The politics of United States encryption policy." Ph.D. diss., Bowling Green State University, 2000.

President. Executive Order 11717. "Transferring certain functions from the Office of Management and Budget to the General Services Administration and the Department of Commerce." *Federal Register* 38, no. 91 (11 May 1973): 12315.

- President. Executive Order 10575. "Administration of Foreign-Aid Functions." 5 November 1954. *Federal Register* 19, no. 218 (9 November 1954): 7249-53.
- President. Executive Order 12923. "Continuation of Export Control Regulations." 30 June 1994. *Federal Register* 59, no. 127 (5 July 1994): 34551-2.
- President. Executive Order 12924. "Continuation of Export Control Regulations." 19 August 1994. *Federal Register* 59, no. 162 (23 August 1994): 51747-8.
- President. Executive Order 13026. "Administration of Export Controls on Encryption Products." 15 November 1994. *Federal Register* 61, no. 224 (19 November 1996): 58767-8.
- President. Executive Order 13206. "Termination of Emergency Authority for Certain Export Controls." *Federal Register* 66, no. 68 (09 April 2001): 18397.
- President. Executive Order 13222. "Continuation of Export Control Regulations." *Federal Register* 66, no. 163 (22 August 2001): 44026-7.
- President. Executive Order 13228. "Establishing the Office of Homeland Security and the Homeland Security Council." *Federal Register* 66, no. 196 (10 October 2001): 51812.
- President. Executive Order 13231. "Critical Infrastructure Protection in the Information Age." *Federal Register* 66, no. 202 (18 October 2001): 53063-71.
- President. "Remarks on Signing the USA PATRIOT Act of 2001." 26 October 2001. *Weekly Compilation of Presidential Documents* 37, no. 43 (29 October 2001): 1550-1.
- President. "Statement on Congressional Action on Legislation to Establish the Department of Homeland Security." 19 November 2002. *Weekly Compilation of Presidential Documents* 38, no. 47 (25 November 2002): 2058.
- Privacy Act of 1974. U.S. Code. Vol. 5, sec. 552a (2001).*
- Privacy Act of 1974. U.S. Statutes at Large 88 (1974): 1896-1910.*
- Ronald Reagan. National Security Decision Directive 145. "National Policy on Telecommunications and Automated Information Systems Security." 17 September 1984.
- Reagan, Ronald. *Public Papers of the Presidents of the United States: Ronald Reagan, 1984. Vol. 1. Washington, D.C.: GPO, 1986.*

- Reno, Janet. Office of the Attorney General. Letter to Congress. Washington, D.C., 18 July 1997.
- Ripley, Randall B. "Stages of the Policy Process." In *Public Policies Theories, Models and Concepts: An Anthology*, edited by Daniel C. McCool, 157-162. Englewood Cliffs, New Jersey: Prentice Hall, 1995.
- Rivest, Ronald L., et al. "Cryptographic communications system and method." U.S. Patent # 4,405,829, 20 September 1983.
- Rivest, Ronald L. "Block encryption algorithm with data-dependent rotations." U.S. Patent # 5,724,428, 3 March 1998.
- Schein, Edgar H. *Organizational Culture and Leadership*. 2d ed. San Francisco: Jossey-Bass Publishers, 1992.
- Schneider Anne Larason, and Helen Ingram. *Policy Design for Democracy*. Lawrence, Kansas: University Press of Kansas, 1997.
- Schneier, Bruce. *Applied Cryptography*. 2d ed. New York: John Wiley & Sons, Inc., 1996.
- Schnorr, Claus P. "Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system." U.S. Patent # 4,995,082, 19 February 1991.
- Seifert, Jeffery W. "Who(se) Rules (for) the Internet: Regime Formation and Global Public Policy for the Information Age." Ph.D. diss., Syracuse University, 2000.
- Shah, Agam. "Memory Experts releases biometric hard drive." *Computer Weekly*, 24 February 2004. < <http://www.computerweekly.com/Article128629.htm> >, accessed January 2005.
- Shapiro, Carl and Hal R. Varian. *Information Rules: A Strategic Guide to the Network Economy*. Boston: Harvard Business School Press, 1999.
- Simon, Herbert A. "Rational Decision Making in Business Organizations." *The American Economic Review* 69, no. 4 (September 1979): 493-513.
- Sims, David. "Public Domain RSA," *LinuxDevCenter.com*, 08 September 2000. < <http://www.linuxdevcenter.com/pub/a/linux/2000/09/08/rsa.html> >, accessed October 2004.

- Smith, Bruce L. R. *American Science Policy Since WWII*. Washington D.C.: The Brookings Institution, 1990.
- Smith, John Lynn. "Recirculation Block Cipher Cryptographic System." U.S. Patent # 3,796,830, 12 March 1974.
- Sorkin, Arthur. "Lucifer, a Cryptographic Algorithm." *Cryptologia* 8, no. 1 (January 1984): 22-41.
- Stanley, Jay and Barry Steinhardt. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society." ACLU Technology and Liberty Program, January 2003. < <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12126&c=207> >, accessed October 2004.
- Sturdevant, Cameron, "PKI Tells 'Who Goes There?'" eWeek, 11 December 2000. < <http://www.eweek.com/article2/0,1759,1282,00.asp> >, accessed January 2005.
- Sussman, Vic. "Lost in Kafka territory: The feds go after a man who hoped to protect privacy rights." *U.S. News & World Report* 118, no. 13 (3 April 1995): 32-33.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. U.S. Statutes at Large* 115 (2001): 272-402.
- U.S. Congress. Office of Technology Assessment. *Information Security and Privacy in Network Environments. OTA-TCT-606*. Washington, D.C.: GPO, September 1994.
- U.S. Department of Commerce. Bureau of Industry and Security. "Encryption Export and Reexport Control Revisions." *Federal Register* 69, no. 236 (9 December 2004): 71356-71364.
- U.S. Department of Commerce. Commerce Control List. *Code of Federal Regulations*. Vol. 15, sec. 738. Washington, D.C.: GPO, 1997. Microfiche.
- U.S. Department of Commerce. "Commerce Department Announces Winner of Global Information Security Competition," G 2000-176. Washington D.C., 02 October 2000.
- U.S. Department of Commerce. Export Administration Regulations. *Code of Federal Regulations*. Vol. 15, secs. 730-744. Washington, D.C.: GPO, 2001.
- U.S. Department of Commerce. Export Administration Regulations. *Code of Federal Regulations*. Vol. 15, sec. 742.15. Washington, D.C.: GPO, 2004, 305-8, <

http://www.access.gpo.gov/nara/cfr/waisidx_04/15cfr742_04.html >, accessed 15 December 2004.

- U.S. Department of Commerce. National Bureau of Standards. Computer Security Guidelines for Implementing the Privacy Act of 1974, Federal Information Processing Standards Publication 41. Washington, D.C.: GPO, 30 May 1975.
- U.S. Department of Commerce. National Bureau of Standards. "Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage; Solicitation of Proposals." *Federal Register* 38, no. 93 (15 May 1973): 12763.
- U.S. Department of Commerce. National Bureau of Standards. The Data Encryption Standard (DES), Federal Information Processing Standard Publication 46. Washington, D.C., July 1977.
- U.S. Department of Commerce. National Bureau of Standards. "Encryption Algorithm for Computer Data Protection: Request for Comments." *Federal Register* 40, no. 52 (17 March 1975): 12134.
- U.S. Department of Commerce. National Bureau of Standards. "Encryption Algorithms for Computer Data Protection; Reopening of Solicitation." *Federal Register* 39, no. 167 (27 August 1974): 30961.
- U.S. Department of Commerce. National Bureau of Standards. "Federal Information Processing Data Encryption: Proposed Standard." *Federal Register* 40, no. 149 (1 August 1975): 32395.
- U.S. Department of Commerce. National Bureau of Standards. Guidelines for Using and Implementing the NBS Data Encryption Standard. Federal Information Processing Standard 74. Washington, D.C., April, 1981.
- U.S. Department of Commerce. National Institute of Standards and Technology. Announcing the Advanced Encryption Standard, Federal Information Processing Standards Publication 197. Washington, D.C., 26 November 2001.
- U.S. Department of Commerce. National Institute of Standards and Technology. "Announcing Approval of Federal Information Processing Standard 186-1, Digital Signature Standard." *Federal Register* 63, no. 240 (15 December 1998): 69049-51.
- U.S. Department of Commerce. National Institute of Standards and Technology. "Announcing Approval of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard." *Federal Register* 69, no. 214 (05 November 1999): 60424-27.

- U.S. Department of Commerce. National Institute of Standards and Technology.
"Announcing Approval of Federal Information Processing Standard (FIPS) 197,
Advanced Encryption Standard (AES)." *Federal Register* 66, no. 235 (06
December 2001): 63369-71.
- U.S. Department of Commerce. National Institute of Standards and Technology.
"Announcing Draft Federal Information Processing Standard (FIPS) for the
Advanced Encryption Standard (AES) and Request for Comments." *Federal
Register* 66, no. 40 (28 February 2001): 12762-3.
- U.S. Department of Commerce. National Institute of Standards and Technology.
"Announcing Plans to Develop a Federal Information Processing Standard for
Public-Key Based Cryptographic Key Agreement and Exchange." *Federal Register*
62, no. 92 (13 May 1997): 26294.
- U.S. Department of Commerce. National Institute of Standards and Technology.
"Announcing Plans to Revise Federal Information Processing Standard 186, Digital
Signature Standard." *Federal Register* 62, no. 92 (13 May 1997): 26293-4.
- U.S. Department of Commerce. National Institute of Standards and Technology.
"Announcing Proposed Withdrawal of Federal Information Processing Standard
(FIPS) for the Data Encryption Standard (DES) and Request for Comments."
Federal Register 69, no. 142 (26 July 2004): 44509-10.
- U.S. Department of Commerce. National Institute of Standards and Technology.
"Announcing Request for Candidate Algorithm Nominations for the Advanced
Encryption Standard." *Federal Register* 62, no. 177 (12 September 1997): 48051-8.
- U.S. Department of Commerce. National Institute of Standards and Technology.
"Approval of Federal Information Processing Standards Publication 185, Escrowed
Encryption Standard (EES)." *Federal Register* 59, no. 27 (9 February 1994): 5997-
6005.
- U.S. Department of Commerce. National Institute of Standards and Technology.
"Approval of Federal Information Processing Standards Publication 186, Digital
Signature Standard (DSS)." *Federal Register* 59, no. 96 (19 May 1994): 26208-11.
- U.S. Department of Commerce. National Institute of Standards and Technology. *A
Century of Excellence in Measurements, Standards, and Technology: A Chronicle
of Selected NBS/NIST Publications 1901-2000*. NIST Special Publication 958.
David R. Lide, ed. Washington D.C.: GPO, January 2001.

- U.S. Department of Commerce. National Institute of Standards and Technology. Data Encryption Standard, Federal Information Processing Standards Publication, FIPS PUB 46-3. Washington, D.C., 1999.
- U.S. Department of Commerce. National Institute of Standards and Technology. Digital Signature Standard, Federal Information Processing Standards Publication 186. Washington, D.C., 19 May 1994.
- U.S. Department of Commerce. National Institute of Standards and Technology. Digital Signature Standard, Federal Information Processing Standards Publication 186-2. Washington, D.C., 27 January 2000.
- U.S. Department of Commerce. National Institute of Standards and Technology. Escrowed Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 185. Washington, D.C., 19 May 1994
- U.S. Department of Commerce. National Institute of Standards and Technology. "*NIST 94-28: Patent Agreement Removes Perceived Barrier to Telecommunications Security System.*" 11 July 1994.
- U.S. Department of Commerce. National Institute of Standards and Technology. "Notice of Proposal for Grant of Exclusive Patent License." *Federal Register* 58, no. 108 (8 June 1993): 32105-6.
- U.S. Department of Commerce. National Institute of Standards and Technology. "A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)." *Federal Register* 56, no. 169 (30 August 1991): 42980-2.
- U.S. Department of Commerce. National Institute of Standards and Technology. "A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES)." *Federal Register* 58, no. 145 (30 July 1993): 40791-4.
- U.S. Department of Commerce. National Institute of Standards and Technology. "Request for Comments on Candidate Algorithms for the Advanced Encryption Standard (AES)." *Federal Register* 63, no. 177 (12 September 1998): 49091-3.
- U.S. Department of Defense. National Security Agency. "*Press Release: NSA Releases FORTEZZA Algorithms.*" 24 June 1998.
- U.S. Department of Justice. Office of the Attorney General. Letter to Congress by Janet Reno. Washington, D.C., 18 July 1997.
- U.S. Department of State. Arms, Ammunition, and Implements of War. *Code of Federal Regulations*. Vol. 22, sec. 121.21. Washington, D.C.: GPO, 1958. Microfiche.

- U.S. Department of State. Arms, Ammunition, and Implements of War. *Code of Federal Regulations*. Vol. 22, secs. 121, 121.01 and 121.1. Washington, D.C.: GPO, 1969.
- U.S. Department of State. International Trade in Arms Regulations. *Code of Federal Regulations*. Vol. 22, sec. 121. Washington, D.C.: GPO, 2001.
- U.S. Department of State. "International Traffic in Arms." *Federal Register* 22, no. 250 (27 December 1957): 10787-10883.
- U.S. Department of State. "International Traffic in Arms." *Federal Register* 31, no. 233 (2 December 1966): 15173-15184.
- U.S. Department of State. "International Traffic in Arms." *Federal Register* 34, no. 134 (17 July 1969): 12029-12041.
- U.S. Department of State. "International Traffic in Arms." *Federal Register* 34, no. 156 (15 August 1969): 13274-13276.
- U.S. Department of State. "Revision of the International Traffic in Arms Regulations (ITAR)." *Federal Register* 45, no. 246 (19 December 1980): 83970-83995.
- U.S. Department of State. "Revision of the International Traffic in Arms Regulations (ITAR)." *Federal Register* 49, no. 236 (6 December 1984): 47682-47712.
- U.S. Department of State. United States Munitions List. *Code of Federal Regulations*. Vol. 22, sec. 121.1. Washington, D.C.: GPO, 1985. Microfiche, 1 March 1985 Edition.
- U.S. Department of Treasury. Federal Public Key Infrastructure Steering Committee. *The Evolving Federal Public Key Infrastructure*. Washington, D.C.: GPO, 2000.
- U.S. Environmental Protection Agency. "Federal Information [Processing Standard] Publications (FIPs) [FIPS Pub] Waiver." *Federal Register* 63, no. 190 (1 October 1998): 52693.
- U.S. House Committee on Commerce. Subcommittee on Finance and Hazardous Materials. *The Electronic Signatures in Global and National Commerce Act*. 106th Congress, 1st sess., 24 June 1999, Serial No. 106-33.
- U.S. House Committee on Commerce. Subcommittee on Telecommunications, Trade, and Consumer Protection. *The Electronic Signatures in Global and National Commerce Act*. 106th Congress, 1st sess., 9 June 1999. Serial No. 106-32.

- U.S. House Committee on Foreign Affairs. Subcommittee on Economic Policy, Trade and Environment. *Export Controls on Mass Market Software*. 103rd Congress, 1st sess., 12 October 1993.
- U.S. House Committee on Government Operations. Legislation and National Security Subcommittee. *Computer Security Act of 1987*. 100th Congress, 1st sess., 25-26 February and 17 March 1987.
- U.S. House Committee on the Judiciary. *Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001*. 107th Congress, 1st sess., 11 October 2001. Report 107-236, Part I.
- U.S. House Committee on the Judiciary. *Telecommunications Carrier Assistance to the Government*. 103rd Congress, 2d sess., 4 October 1994. Report 103-827, Part I.
- U.S. House Committee on the Judiciary. Subcommittee on Courts and Intellectual Property. *Electronic Signatures in Global and National Commerce (E-SIGN) Act*. 106th Congress, 1st sess., 30 September 1999. Serial No. 3.
- U.S. House Committee on the Judiciary. Subcommittee on Courts and Intellectual Property. *Security and Freedom through Encryption (SAFE) Act*. 106th Congress, 1st sess., 4 March 1999. Serial No. 34.
- U.S. House Committee on the Judiciary. Subcommittee on Courts and Intellectual Property. *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act*. 105th Congress, 1st sess., 16-17 September 1997. Serial No. 33.
- U.S. House Committee on Science. *Cyber Security Research and Development Act*. 107th Congress, 2nd sess., 4 February 2002. Report 107-355, Part I.
- U.S. House Committee on Science, Space, and Technology. Subcommittee on Technology, Environment and Aviation. *Communications and Computer Surveillance, Privacy and Security*. 103rd Congress, 2nd sess., 3 May 1994.
- U.S. House. *Computer Security Enhancement Act of 2001*. 107th Congress, 1st session, H.R. 1259. *Congressional Record*. (28 March 2001): H1294.
- U.S. House. *H.R. 850*. 106th Congress, 1st sess., 23 July 1999. Report No. 106-117, Parts I, II, IV, and V.
- U.S. Senate Committee on Banking, Housing and Urban Affairs. *Export Administration Act of 2001*. 107th Congress, 1st sess., 2 April 2001. Senate Report 107-10.

- U.S. Senate Committee on Banking, Housing, and Urban Affairs. Subcommittee on Financial Services and Technology. *The Digital Signature and Electronic Authentication Law [SEAL] of 1998—S. 1594*, 105th Congress, 2nd sess., 11 March 1998. Senate Hearing 105-896.
- U.S. Senate Committee on Commerce, Science, and Transportation. *The Promote Reliable On-line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999*. 106th Congress, 1st sess., 05 August 1999. Senate Report 106-142.
- U.S. Senate Committee on Commerce, Science, and Transportation. Subcommittee on Science, Technology and Space. *S. 1726, Promotion of Commerce Online in the Digital Era Act of 1996, or PRO-CODE” Act*. 104th Congress, 2d sess., 12 June 1996.
- U.S. Senate Committee on Commerce, Science, and Transportation. Subcommittee on Science, Technology and Space. *Security Risks in Electronic Commerce*, 107th Congress, 1st sess., 16 July 2001. Available from Federal Document Clearing House, Inc., published by Lexis Nexis. < <http://web.lexis-nexis.com/congcomp/document> >, accessed 24 December 2004.
- U.S. Senate Committee on the Judiciary. *The National Information Infrastructure Protection Act of 1995*. 104th Congress, 2nd sess., 27 August 1996.
- U.S. Senate. Report Card of the 106th Congress on Privacy. 106th Congress, 2nd session, *Congressional Record* (14 December 2000): S11777.
- U.S. Senate Select Committee on Intelligence. *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard*. 95th Congress, 2d sess., 1978. Committee Print.
- U.S. Social Security Administration. “The Chief Information Officer of the Social Security Administration Grants to the Social Security Administration a Waiver From the Use of Certain Federal Information Processing Standards.” *Federal Register* 63, no. 108 (5 June 1998): 30794-30795.
- Warren, Samuel D. and Louis D. Brandeis. “The Right to Privacy,” *Harvard Law Review* IV, no. 5 (15 December 1890): 193-220.
- Whitaker, Reg. *The End Of Privacy: How Total Surveillance Is Becoming a Reality*. New York: The New Press, 1999.
- The White House. *National Security Decision Directive 145, National Policy on Telecommunications and Automated Systems Information Security*. 17 September 1984.

The White House. *A National Security Strategy for a Global Age*. Washington, D.C.: GPO, 2000.

The White House. *A National Security Strategy for a New Century*. Washington, D.C.: GPO, 1997.

The White House. *The National Security Strategy of the United States of America*. Washington, D.C.: GPO, 2002.

Wilson, James Q. *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Basic Books, 1989.

World Trade Organization. Trade Policy Reviews: United States: July 1999. Press Release Press/TPRB/108, 1 July 1999.
<http://www.wto.org/english/tratop_e/tpr_e/tp108_e.htm>, accessed October 2004.

Yin, Robert K. *Case Study Research: Design and Methods*. 2d ed. Thousand Oaks, California: Sage Publications, 1994.

Zimmermann, Phil. "Interview with Author of PGP (Pretty Good Privacy)." *High Tech Today Hosted by Russell Hoffman*, 05 February 1996. <<http://www.animatedsoftware.com/hightech/philspgp.htm>>, accessed October 2004.

Curriculum Vitae

Mark L. DeVirgilio was born on 15 June 1956 in Honolulu, Hawaii. He graduated from Kailua High School in 1974. He earned a Bachelor of Science in Biology with High Honors in 1978 from the University of Hawaii at Manoa. Continuing on, he earned a Master of Science in Biochemistry in 1980 from the University of Hawaii School of Medicine. Mark worked in a forensics position for the Honolulu Police Department before joining the United States Air Force in January 1981. He earned a Bachelor of Science in Electrical Engineering, from the Air Force Institute of Technology in Dayton, Ohio.

He is currently the Course Director, Information Operations Specialized Studies, Air Command and Staff College, Maxwell AFB, Alabama. He has held previous positions as an electronic warfare analyst, classified system development manager, classified space system operations, classified information operations system development. Mark is a graduate of Squadron Officer School, Air Command and Staff College, and Air War College. He is a member of the Air Force Association, American Association for the Advancement of Science, Association of Computing Machinery, Eta Kappa Nu electrical engineering honor society, Institute for Electrical and Electronic Engineers, Phi Kappa Phi national honor society, Pi Alpha Alpha public administration honor society, and Tau Beta Pi engineering honor society. You may contact him using the following information:

Mark L. DeVirgilio
4104 Faunsdale Dr
Montgomery, Alabama 36019
devirgilio@devo-junkyard.us
(334) 272-8648