



THE UNIVERSITY *of* EDINBURGH

This thesis has been submitted in fulfilment of the requirements for a postgraduate degree (e.g. PhD, MPhil, DClInPsychol) at the University of Edinburgh. Please note the following terms and conditions of use:

- This work is protected by copyright and other intellectual property rights, which are retained by the thesis author, unless otherwise stated.
- A copy can be downloaded for personal non-commercial research or study, without prior permission or charge.
- This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the author.
- The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the author.
- When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given.

**Trusted Computing or trust in computing?
Legislating for trust networks**

Ioanna Danidou



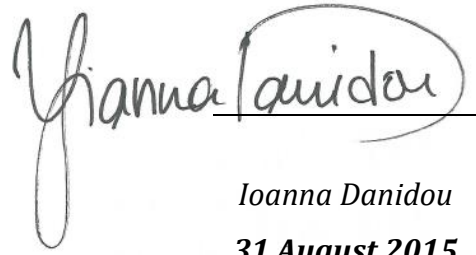
PhD

The University of Edinburgh

2015

Declaration

The candidate confirms that the work submitted is her own, except where work which has formed part of jointly-authored publications has been included. The contribution of the candidate and the other authors to this work has been explicitly indicated below. The candidate confirms that appropriate credit has been given within the thesis where reference has been made to the work of others. This work has not been submitted for any other degree or professional qualification.

A handwritten signature in black ink, reading "Ioanna Danidou", written over a horizontal line. The signature is cursive and includes a large loop at the end of the name.

Ioanna Danidou
31 August 2015

Acknowledgements

The completion of my dissertation and the Ph.D. has been a very long journey. Firstly, I would like to thank my primary supervisor, Professor Burkhard Schafer, who offered me the opportunity to undertake my PhD studies in his group; for his help, guidance, inspiration and support through the last years that I was pursuing this research as part-time. He has been supportive since the early days I began this PhD, and we have together published a number of journal papers, always under his academic eyesight. Further, I would like to thank my secondary supervisor Professor Claudio Michelon for his comments and fruitful thoughts on my research. The research work has benefited from discussions, feedback and input from them both. All mistakes and errors remain my own.

I continue, by thanking the most basic source of my life energy: my mother Roula, and sister Tina. I have an amazing yet perfect family, unique in some ways, who never gave up on me. Their encouragement and support has been unconditional all these years, both emotional, and financial. I feel they have sacrificed themselves a lot, to help me pursuit this degree. Without their encouragement and dedication, this dissertation would not be possible. Mom, especially, is a great role model of resilience, strength and character.

As time does not stand still, much has changed in the time I've been involved with this project; some of them being good, and some bad. Good news is that I have an excellent husband, Andreas, who stands by me and supports me through the years even on the writing up of this thesis. His love, support, affection and belief in me are a treasure. Bad news is that two persons who have made a statement in my life are no longer with me, and I refer to my two grandfathers: Yiannis and Demetrakis. I am confident that you are watching us from above and you are at least satisfied and pleased with what I have achieved so far. Finally, I would like to thank the rest of the family and friends, for their thoughts and prayers.

Abstract

This thesis aims to address several issues emerging in the new digital world. Using Trusted Computing as the paradigmatic example of regulation through code that tries to address the cyber security problem that occurs, where the freedom of the user to reconfigure her machine is restricted in exchange for greater, yet not perfect, security. Trusted Computing is a technology that while it aims to protect the user, and the integrity of her machine and her privacy against third party users, it discloses more of her information to trusted third parties, exposing her to security risks in case of compromising occurring to that third party. It also intends to create a decentralized, bottom up solution to security where security follows along the arcs of an emergent “network of trust”, and if that was viable, to achieve a form of code based regulation. Through the analysis attempted in this thesis, we laid the groundwork for a refined assessment, considering the problems that Trusted Computing Initiative (TCI) faces and that are based in the intentional, systematic but sometimes misunderstood and miscommunicated difference (which as we reveal results directly in certain design choices for TC) between the conception of trust in informatics (“techno-trust”) and the common sociological concept of it. To reap the benefits of TCI and create the dynamic “network of trust”, we need the sociological concept of trust sharing the fundamental characteristics of transitivity and holism which are absent from techno-trust.

This gives rise to our next visited problems which are: if TC shifts the power from the customer to the TC provider, who takes on roles previously reserved for the nation state, then how in a democratic state can users trust those that make the rules? The answer lies partly in constitutional and human rights law and we drill into those functions of TC that makes the TCI provider comparable to state-like and ask what minimal legal guarantees need to be in place to accept, trustingly, this shift of power. Secondly, traditional liberal contract law reduces complex social relations to binary exchange relations, which are not transitive and disrupt rather than create networks. Contract law, as we argue, plays a central role for the way in which the TC provider interacts with his customers and this thesis contributes in speculating of a contract law that does not result in atomism, rather “brings in” potentially affected third parties and results in holistic networks. In the same vein, this thesis looks mainly at specific ways in which law can correct or redefine the implicit and democratically not validated shift of power from customer to TC providers while enhancing the social environment and its social trust within which TC must operate.

Table of Contents

ACKNOWLEDGEMENTS	I
ABSTRACT	II
TABLE OF CONTENTS	III
LIST OF PUBLICATIONS	VI
LIST OF ABBREVIATIONS	VII
LIST OF FIGURES	IX
CHAPTER 1 : INTRODUCTION	1
1.1 INTERNET AS A COMPLEX DYNAMIC SYSTEM	1
1.2 THE IMPORTANCE OF SECURITY	3
1.3 RESEARCH QUESTIONS	7
1.4 METHODOLOGY	8
1.5 TC BENEFITS	9
1.6 DEBATES AND CONCERNS	12
1.7 OBJECTIVES	17
CHAPTER 2 : INTRODUCTION TO TRUSTED COMPUTING	19
2.1 INTRODUCTION IN TRUSTED COMPUTING	19
2.2 TRUSTED COMPUTING FUNDAMENTALS	33
2.3 TRUSTED COMPUTING GROUP – THE HISTORY	36
2.4 TRUSTED COMPUTING GROUP – STRUCTURE	37
2.5 TRUSTED COMPUTING GROUP AND THE CREATION OF TRUST	38
2.6 TECHNICAL ANALYSIS OF TRUSTED COMPUTING TECHNOLOGY	54
2.6.1 <i>How the Trusted Platform works</i>	54
2.6.2 <i>Direct Anonymous Attestation Protocol</i>	67
2.6.3 <i>Technology / Protocols On Trusted Computing</i>	75
2.7 RECAP AND SUMMARY	83
CHAPTER 3 : TRUSTED COMPUTING AND THE DIGITAL CRIME SCENE (FORENSICS COMPUTING AND CRIME PREVENTION)	91
3.1 WHOM TO TRUST WITH CRIME PREVENTION AND DETECTION	91
3.2 CRIME INVESTIGATION IN A TC WORLD	109

3.2.1	Scenario 1.....	110
3.2.2	Scenario 2.....	110
3.2.3	Scenario 3.....	110
3.2.4	Scenario 4.....	110
3.2.5	Scenarios close up	111
3.3	WHAT IS THE RELEVANCE OF ALL THESE FOR DIGITAL EVIDENCE?.....	112
3.4	CONSEQUENCES FOR THE REGULATORY ENVIRONMENT.....	117
3.5	LEGAL RESPONSIBILITY IN AN AGE OF TC	121
3.6	A CASE STUDY: RETENTION AND PRESERVATION OF DATA	134
3.6.1	<i>Chain of custody and Audit trails.....</i>	152
3.6.2	<i>Collecting online evidence.....</i>	160
3.7	CONCLUSIONS.....	163
CHAPTER 4 : RELIANCE LIABILITY ISSUE IN ANALOGY TO TMS.....		167
4.1	INTRODUCTION	167
4.2	SETTING THE SCENE.....	175
4.2.1	<i>Contractual relation between buyer and seller.....</i>	184
4.2.2	<i>An alternative view: Security as service and the relational contract theory.</i>	202
4.2.3	<i>Third party liability – no contractual relations – the reliance liability case</i>	219
4.2.4	<i>Reliance liability</i>	225
4.2.5	<i>Relying on the TCG.....</i>	226
4.3	TMS - PROMOTING THE FEELING OF SECURITY AND TRUST	228
4.4	THE ANALOGY BETWEEN TMS AND TC.....	231
4.5	LEGAL ENVIRONMENTS FOR DIGITAL TRUST	235
4.6	WRAP-UP	243
4.7	REGULATING RELIANCE.....	244
4.7.1	<i>“What persons are under such duty?”.....</i>	254
4.7.2	<i>“To whom do these professional people owe this duty?”.....</i>	255
4.7.3	<i>“To what transactions does the duty of care extend?”.....</i>	256
4.8	FROM EXAMPLES TO DOCTRINE: CONTRACTUAL LIABILITY ON RELIANCE	257
CHAPTER 5 : CONCLUSIONS.....		259
5.1	CONCLUSIONS.....	259
5.1.1	<i>TCG as an Internet Security provider.....</i>	261
5.1.2	<i>TC and regulation.....</i>	263
5.1.3	<i>TC and digital forensics.....</i>	268
5.2	RESEARCH SIGNIFICANCE.....	270
5.3	FUTURE RESEARCH.....	273

BIBLIOGRAPHY	277
---------------------------	------------

List of Publications

- Danidou, Yianna (2007). *Legal Implications of Trusted Computing*. Paper presented at the Proceedings of the 22nd British and Irish Law, Education and Technology Association (BILETA), Hertfordshire, UK.
- Danidou, Yianna, & Schafer, Burkhard. (2009). In Law We Trust? Trusted Computing and Legal Responsibility for Internet Security. In D. Gritzalis & J. Lopez (Eds.), *Emerging Challenges for Security, Privacy and Trust* (Vol. 297, pp. 399-409): Springer Boston.
- Danidou, Yianna, & Schafer, Burkhard. (2011). "Trust me, I'm a computer" – Trusted Computing and the law between liability and responsibility. *Information & Communications Technology Law*, 20(3), pp. 185-199. doi: 10.1080/13600834.2011.603962
- Danidou, Yianna, & Schafer, Burkhard. (2011). *Legal Environments for Digital Trust: Trustmark, Trusted Computing and the Issue of Legal Liability*. Paper presented at the LSPI, Nicosia, September 19 – 22, Nicosia.
- Danidou, Yianna, & Schafer, Burkhard. (2011). Trusted Computing and the Digital Crime Scene. *Digital Evidence & Elec. Signature L. Rev.*, 8 pp. 111 - 123.
- Danidou, Yianna, & Schafer, Burkhard. (2011). Legal environments for Digital trust: Trustmark, Trusted Computing and the issue of Legal liability. *Journal of Milton campos School of law*, 23, pp. 197-220.
- Danidou, Yianna, & Schafer, Burkhard. (2012). Legal Environments for Digital Trust: Trustmarks, Trusted Computing and the Issue of Legal Liability. *Journal of International Commercial Law and Technology*, 7(3).

List of Abbreviations

AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
AIK	Attestation Identity Key
AMD	Advanced Micro Devices
CA	Certifying Authority
CCTV	Closed-circuit television
CD	Compact Disc
CICA	Canadian Institute of Chartered Accountants
CPU	Central Processing Unit
CRTM	Core Root Of Trust For Measurement
CSPs	Certification Service Providers
DAA	Direct Anonymous Attestation
DDoS	Distributed Denial of Service
DMCA	Digital Millennium Copyright Act
DoS	Denial Of Service
DRM	Digital Rights Management
DVD	Digital Versatile Disc
EK	Endorsement Key
EULA	End-User Licence Agreement
GPL	GNU Public Licence
GPL	GNU Public Licence
ICT	Information Communication Technology
ISP	Internet Service Provider
ISSP	Information Society Service Providers
IT	Information Technology
NGSCB	Next Generation Secure Computing Base
NSL	National Security Letters
OS	Operating System
OSS	Open Source Software
P2P	Peer To Peer Networks
PC	Personal Computer
PCA	Privacy Certification Authority
PGP	Pretty Good Privacy
PIPA	Protect IP Act
RAND	Reciprocal Reasonable And Non-Discriminatory

RFC	Requests for Comments
RSA	Ron Rivest, Adi Shamir and Len Adleman Algorithm
RTM	Root Of Trust For Measurement
RTR	Root Of Trust Reporting
RTS	Root Of Trust Storage
SCA	Stored Communications Act
SECaaS	Security as a service
SGA	Sale of Goods Act
SOA	Service Oriented Architecture
SOPA	Stop Online Piracy Act
STP	Security Trust Privacy
TBB	Trusted Building Blocks
TC	Trusted Computing
TCG	Trusted Computing Group
TCI	Trusted Computing Initiative
TCPA	Trusted Computing Platform Alliance
TM	Trust Marks
TMOs	Trustmark Organisations
TP	Trusted Platform
TPM	Trusted Platform Module
TSS	TCG Software Stack
TTPs	Trusted Third Parties
USB	Universal Serial Bus

List of Figures

Figure 1: Reputation representation	41
Figure 2: Direct (blue arrows) and Indirect (red arrows) trust.....	42
Figure 3: Square of regulation proposed by Larry Lessig.....	53
Figure 4: Runtime/Loadtime Measurements and Reference Measurement Processes	159
Figure 5: Analogy between TMOs (left) and TC (right)	233

*“With great power comes great responsibility”
(Spiderman)*

CHAPTER 1 :

INTRODUCTION

1.1 Internet as a complex dynamic system

The Internet is the largest global network system that currently exists, called also “the network of networks” because it is comprised out of smaller interconnected networks.¹ Through the Internet extensive information and services are routed every day, to facilitate the communications and services we are requesting from it by any connected digital device. Guadamuz characterized the Internet as a complex dynamic system which is self-organising.² While Internet’s architecture has been proven robust enough through years, it has also proven itself highly vulnerable concerning cyber attacks and cyber crime; including computer viruses, worms, botnets, Denial of Service (DoS) attacks and others. It is an open system that allows anyone to be connected, upload and download information to it, yet giving space for cyber attacks to take place.

As the Internet became a common place for online users globally and since the Internet was not designed for this type of commercial activity, huge problems have been caused both economically but mainly concerning online safety and reduction of the cyber crime.³ Zittrain, in his book with title “The future of the Internet and how to stop it” states that:

¹ RFC 1122. (1989). Requirements for Internet Hosts -- Communication Layers. 1.1.2 *Architectural Assumptions*.

² Guadamuz, A. (2013). *Networks, complexity and internet regulation scale-free law*: The University of Edinburgh. p. 254

³ Gordon, L., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), pp. 438-457.

“If the Internet had been designed with security as its centerpiece, it would never have achieved the kind of success it was enjoying, even as early as 1988. The basic assumption of Internet protocol design and implementation was that people would be reasonable; to assume otherwise runs the risk of hobbling it in just the way the proprietary networks were hobbled. The cybersecurity problem defies easy solution, because any of the most obvious solutions to it will cauterize the essence of the Internet and the generative PC”.⁴

Attempts to deal with the growing number of reported cybercrime incidents include legislation, user training, public awareness, and other technical security measures.⁵ The UK government recognizes the detrimental impact that a cyberattack can have on the economy and the social well being of the country⁶ and the effect of how nations deal with internet freedom and security. While the legal system struggles to keep up with technology developments and their enforcement and prosecution, the regulation through technology took

doi: 10.1145/581271.581274, Gordon, L., & Loeb, M. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, 8(5), pp. 335-337. doi: 10.1007/s10796-006-9010-7

- ⁴ Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven [Conn.]: New Haven Conn. : Yale University Press.p. 60
- ⁵ EU fights against cybercrime and has implemented a strategy European Commission. (2013a). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. In T. C. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS (Ed.): European Commission. EU elaborates more in its recent digital agenda European Commission. (2015, 2/3/2015). Cybersecurity. Retrieved 26/6/2015, 2015, from <https://ec.europa.eu/digital-agenda/en/cybersecurity#Article>. See also UK's strategy report Cm7642. (2009). *Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space*. London: The Stationery Office Limited.
- ⁶ Cm7234. (2007). The Government reply to the fifth report from the House of Lords Science and Technology committee. London: The Stationery Office Limited, Cm7948. (2010). *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. London: The Stationery Office Limited. The Home Office minister Baroness Neville-Jones presented an estimation that cybercrime costs UK £27bn each year in UK Cabinet Office and National security and intelligence. (2011). *The Cost of Cyber Crime - full report*. UK: Detica Limited.

increasingly center stage.⁷ Rather than prosecuting crime, the focus shifted on communicating architectures that make it impossible to commit crimes in the first place.

1.2 The importance of Security

Transactions over the Internet such as e-commerce are perceived as high risk; and trust is mostly needed in such cases of high risk.⁸ In the absence of interaction with people who are validated as trustworthy, risk is higher. With technology improving and upgrading online and offline, and as digital crimes increase, consumers seem more and more concerned regarding privacy and security, while researches identify that the primary goal to balance these is by winning public trust. Both consumers and merchants are negatively influenced by lack of trust which leads to failure in the desirably wide deployment of the technology.⁹

These concerns have been addressed by the research community in a number of studies, using different indices that may affect individuals' perception

-
- ⁷ See also Lessig, L. (1996). The Zones of Cyberspace. *Stanford Law Review*, 48(5), pp. 1403-1411. , Pagallo, U. (2015). Good onlife governance: On law, spontaneous orders, and design *The Onlife Manifesto* (pp. 161-177): Springer, Yeung, K. (2008). Towards an Understanding of Regulation by Design. In K. Yeung (Ed.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 79-108). Oxford: Hart, Yeung, K., & Dixon-Woods, M. (2010). Design-based regulation and patient safety: a regulatory studies perspective. *Social Science & Medicine*, 71(3), pp. 502-509.
- ⁸ Mutz, D. C. (2005). Social Trust and E-Commerce: Experimental Evidence for the Effects of Social Trust on Individuals' Economic Behavior. *Public Opinion Quarterly*, 69(3), pp. 393-416. doi: 10.1093/poq/nfi029
- ⁹ Katsikas, S., Lopez, J., & Pernul, G. (2005). Trust, Privacy and Security in E-Business: Requirements and Solutions. In P. Bozanis & E. Houstis (Eds.), *Advances in Informatics* (Vol. 3746, pp. 548-558): Springer Berlin Heidelberg.

on trustworthiness.¹⁰ Inside the digital world we are currently experiencing every day, there are two evident conclusions:

- that the digital companies will need to find the measures to increase the trust and security that they provide towards their customers;
- technology solutions should be implemented to ensure based on their carrying features protection over consumer's trust, privacy and security while transacting over the internet.

In the same vein, prior research review suggests that new technologies and frameworks should be developed to address the issue of security, trust and privacy assuring that data are safe while used over the internet, considering the large number of vulnerabilities existing.¹¹ While security solutions and technologies have been developed in an effort to deal with security, trust and privacy issues, a unified solution has not been achieved leading Service Providers, Collaborators and Trusted Third Parties to create an unstable and imbalance environment for users.¹²

Achieving the ideal unified and balanced framework is supposed to include STP policies, technologies, processes and legal aspects all blended together to present the optimal trusted environment. As a step towards the success of a

¹⁰ The ability of an online seller to handle business transactions with benevolence and integrity are the three main dimensions of trustworthiness as research has validated Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *Academy of Management Review*, 32(2), pp. 344-354. doi: 10.5465/amr.2007.24348410. Therefore consumers would ultimately expect online sellers to be proficient and reliable, while being honest and benevolent Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, 11(3-4), pp. 245-270. .

¹¹ Ab Manan, J.-L., Mubarak, M. F., Isa, M. A. M., & Khattak, Z. A. (2011). Security, Trust and Privacy—A New Direction for Pervasive Computing. *Information Security*, pp. 56-60.

¹² *ibid.*, p.2

holistic system that promotes and assures security, trust and privacy in all levels, computer scientists, architects, engineers, designers and developers from large market players have reached to the decision that Trusted Computing is the ideal environment that can meet all the issues.

Internet security is a big problem. In the past, it was left with little success to individual users or companies to keep their own systems safe, leading to a fragmented approach. Guadamuz's book¹³ shows why such an approach is doomed to failure: if you are part of a complex dynamic network, trying to keep yourself protected while not caring for what happens outside your small sphere of influence is doomed to failure. It tries to deal with individual threats, one at a time, while ignoring that the main security threats match the structure of the network, so that taking out one node at a time won't be successful.

TC emerged as a possible solution to this dilemma. It not only promises to take the weakest link in the security chain - the individual PC user - out of the equation. It also promises to "build up" secure networks in the same way the Internet itself operates - that is, as a complex dynamic system of mutually assured trustworthiness. What seems like an excellent candidate for a technological fix of a major threat to our critical infrastructures is based on a massive shift of power away from individual users to a monopoly of major industry players. There has been, to date, little in terms of systematic reflection or analysis of what this power shift means for our society, the winner and losers, and also, importantly, the role of law to manage this paradigm change in the way internet security is provided.

Legal discussion, to the extent that it took place at all, focused on narrow issues of privacy or copyright law. These are important issues, but we argue that they are only symptoms of a more far reaching shift in the technology landscape. At the same time, uptake and market success of TC was disappointingly low.

¹³ Guadamuz, A. (2013). Networks, complexity and internet regulation scale-free law: The University of Edinburgh.

Regarding the legislative aspect that should apply for this type of system as well as the implications that appear, an exhaustive discussion follows in the next chapters. There, we will argue that systemic features of the TC philosophy are inevitably creating legal issues for which the current legal system is insufficient. Under the technical issues that we identify in the next chapters, underlying we find fundamental legal and jurisprudential issues that make “scale-free law”¹⁴ difficult to achieve.

TC’s aim is to allow the computer user to trust his own computer and for third parties to trust that specific computer.¹⁵ TC tries to build complex dynamic trust networks “bottom up”,¹⁶ without central, let alone state, oversight or control. If social trust relations in complex modern societies also organize themselves in dynamic complex networks, and if security “travels along” the trust edges in this network - because we only trust those whom we can securely trust, those who are “trustworthy” - the result would be an environment with ubiquitous security, which is the ultimate aim of the TCI. We will show that the TC network will only work when in addition to security and techno-trust, also legally enabled social trust “runs along” the edges that connect the nodes of the network. That is, if for any two connected nodes in the TC network, the parties can trust each other in the computer science sense, and have as a fallback a shared trust in institutions that can apply legal sanctions; we will get dynamic complex networks that are isomorphic to the communication network of the Internet.

¹⁴ “It is called scale-free because the same distribution of relationships exists at any scale” *ibid.*, p.27

¹⁵ Lipson, H. F. (2002). Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. In C. M. University (Ed.), *CERT Coordination Center, Special Report CMU/SEI-2002-SR-009*.

¹⁶ Using base elements to build up a larger system.

1.3 Research questions

With this background in mind, this thesis asks a number of interrelated research questions:

- How can the law make conceptual sense of the technological change that TC heralds?
- Is the disappointing uptake of TC in parts caused by an adverse legal environment?
- How, if at all, can the law reassure consumers and mitigate the increasing power imbalance, while at the same time not disincentivising industry investment in security?
- Which parts of the law, and what type of concepts, are best suited to provide a legal environment for TC that meets the above criteria?

This in turn leads to some tentative research hypothesis:

- The disappointing uptake of TC can in parts be attributed to a divergence of legal, technological and societal understandings of trust.
- Law and technological expertise are both important ways to create trust - but neither can on its own create the type of trust societal acceptance of technology requires. They need to be coordinated so that they can make up for each other's shortcomings.
- TC is a particularly problematic type of technology for legal regulation as it straddles the private-public law divide. In some ways the TC consortium takes on powers and responsibilities previously more closely associated with the policing function of the state, a public law issue. It remains however a private law entity, and relates to the people affected by the technology mainly through contract law.
- Contract law in modern, liberal market societies plays an important role to foster trust - but is badly suited, for deep conceptual reasons, to promote trusts in networks.

- However, some traditional legal concepts, and some emerging conceptions of (private) law itself, might be much better suited to engender trust, especially if they are backed up or complemented by public law regulation. In particular, we can use the law of evidence and procedure to promote trust in the “public law face” of TC; reliance liability and a relational conception of contract law to promote trust in the “private law face” of TC.

1.4 Methodology

To substantiate this thesis’ arguments, the thesis uses mainly an interdisciplinary, conceptual analysis. This analysis looks at legal, technological and societal conceptions of trust, and tries to distill for each some rather abstract, structural descriptions. It then tries to match the respective concepts across the disciplinary boundaries. For the analysis of TC, the thesis relies in addition to academic analysis on the software and hardware specifications as released by the TCG, and discusses them from the understanding of a computer scientist. It then tries to match them with concepts from social and political science, in particular theories of trust in modern society. This is gained mainly through an analysis of classical texts in sociology and the “grand theory” tradition of Weber, Durkheim or Luhmann: What does, according to these thinkers, trust mean in modern society, and how is it generated? Their analysis points to the role of law, and here we take a mix of academic and jurisprudential legal analysis, together with examples from statutory and case law, to gain an understanding of the role of law to build trust. This means in particular that this thesis is not primarily a doctrinal analysis of the legal issue caused by TC in a given jurisdiction. Rather, we take ideas and examples from a variety of jurisdictions as our inspiration or illustration, to gain a more abstract, conceptual understanding of how “the law” thinks about private and public law relations, issues of liability and responsibility.

We then try to match them to the more substantive concept of trust in modern society on the one hand, the techno-conception of trust on the other. We support some of these claims by a limited empirical analysis that tries to understand how the “concept matching” works in practice. For this, we look at the way in which computer scientists actively involved in the development of TC think about and understand the legal environment of their product.

We then argue, following Guadamuz, that if we want to understand the Internet as a regulatory problem, we need to take its nature as a complex dynamic network seriously. To defeat security threats that are parasitic on the Internet structure, and with other words themselves (complex dynamic networks) are typical for a DoS attack for instance, we need “networks of security” rather than isolated security solutions and “gated communities”. In the case of TC in particular, this requires networks of trust relations that are isomorphic to the structure of the internet. If law is needed to support this network, legal trust needs to mirror technological trust in the sense that the network of legal relations, duties and rights has to be isomorphic to the network of technology driven communication relations. In more accessible terms: If my computer trusts your computer because of its technological signature, then I can trust you because of the liability relation between us. We will argue however that classical private law, with its focus on litigation and individual contract relations, can disrupt rather than enhance this network of trust - unless we rethink in more systematic ways the interaction of law and technology.

1.5 TC benefits

The proponents of TC suggest that Trusted Computing promises to provide four crucial advantages: reliability, security, privacy and business integrity. Thus, these guarantee a system that will be available when in need, that will resist any attack once protecting the system itself and the data, that will give the demanded privacy to the user and finally that provides to businesses the ability to interact

effectively with their customers. Also, TC will provide protection from viruses due to the fact that a check will be applied to all files trying to “enter” the system. This is to be done through structuring new applications that give new possibilities to the owners of computer systems and/or end users. One of them is that a TC system can detect files that are unauthorized, such as pirated music or software, or viruses and, delete them remotely. This means that TC could be used to restrict access to everything from music files to pornography to writings that criticize political leaders. This approach is not uncontroversial. Content-owning businesses may wish to prevent end-users doing particular things with files e.g. ripping copyright music files; and employers may wish to control employees' ability to access and/or distribute information across corporate networks, and so support this functionality. However, individuals are likely to have significant concerns about the effect of such technical solutions on their rights for privacy and freedom of speech. This may well lead possible buyers to refuse to purchase TC systems.

There is clearly corporate support for the TC concept, but it is important that such support should be viewed critically. In an executive e-mail sent to Microsoft employees, Bill Gates suggested that the firm needed to build “a Trustworthy Computing environment for customers, that is as reliable as the electricity that powers our homes and businesses today”.¹⁷ He went on to suggest that possible goals for TC might include: authentication of users; the inhibition of spam and junk emails that could probably reach to the user as they appear to come from trusted senders; production of software that satisfies the needs of the users either individuals or businesses; and lastly trustworthiness provided to computing experiences. He pointed out that now “making security improvements is an even higher priority than adding features”. This statement would appear to be

¹⁷ Gates, B. (2002, 18 July 2002). Executive E-mail: Trustworthy Computing. Retrieved 26 April 2006, 2006, from <http://www.microsoft.com/mscorp/execmail/2002/07-18twc.asp>

somewhat at odds with Microsoft's previous processes, which appear to have concentrated on adding features to applications rather than building in security features. Given the dominance of its current O/S, Microsoft's stated strategy with regard to TC may need to be treated with some caution.

Siani Pearson of HP Laboratories in Bristol notes that "the most important aspect for users is that Trusted Platforms provide a low-cost way to trust a software environment for some particular purpose".¹⁸ This may be true in principle, and there are certainly other potential advantages for users that she indicates, including hardware-based security, feedback about trust to the user, technological foundation for privacy and trustworthy digital signature; all of which seek to create better user confidence. However, in the light of the literature review, it is arguable that a key element in determining probable cost has not been fully examined: the lack of a discussion of liability issues suggests that there may yet be important "hidden" costs.

Finally, Gehring argues that TCG offers the advantage that it standardises components while building trusted systems.¹⁹ Standard setting is likely to be a key element of TC; however Gehring's point also raises questions, not least about the effect of such standardization upon the dynamics of the computing market. There is a significant risk in such a scenario of the promotion of anti-competitive behavior. The personal computing market already faces competitive failures caused by the domination of "Wintel";²⁰ adding TC, where 'non-trusted'

¹⁸ Pearson, S. (2005, 23-26 May 2006). *Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy*. Paper presented at the Proceedings of the Trust Management: Third International Conference, iTrust 2005, Paris, France (pp. 305-320), Springer-Verlag GmbH.

¹⁹ Gehring, A. R. (2006, 2006). Trusted computing for digital rights management. http://www.indicare.org/tiki-read_article.php?articleId=179. from http://www.indicare.org/tiki-read_article.php?articleId=179

²⁰ Windows is still the most dominant OS that exists at the moment: NetMarketShare. (2016). Desktop Operating System Market Share. from <https://www.netmarketshare.com/operating-system-market->

computers and applications can be frozen out, and unauthorized files can be barred or deleted, without significant safeguards, may only make things worse.²¹

1.6 Debates and Concerns

Given the foregoing, it is unsurprising that Trusted Computing has given rise to number of controversies between its proponents and opponents. This is due to the fact that the aim of TCG will provide more trustworthiness from the point of view of software vendors and the content industry, but will be less trustworthy from the point of view of their owners. Consequently opponents say that cryptographic systems don't offer enough security for the computer and thus for the user, but instead provide vendors and technology companies with the freedom to make "decisions about data and application that typically have been left to users".²² Proponents state that the implementation and application of technologies that provide trusted computing will increase users' trust in their

share.aspx?qprid=10&qpcustomd=0. Yet, if we consider the CPU AMD vs Intel market share, INTEL possesses by far a highest portion of the pie. Some people may argue that the dominant market role of "Wintel" has been eroded recently, and that this alone indicates the possibility that market mechanisms can come to bear. It is true that new players have entered the market. However, in sheer numbers, "Wintel" still dominates significantly. It is also correct that competition authorities especially in Europe have challenged the supremacy of the big providers, and may do so more in the future. These developments have the potential to alleviate some of the concerns raised in the thesis. However, it is important to realise that the infrastructure and standard decisions made now, will have a lasting effect and force certain design and business model choices even if the originators should eventually lose their dominating position.

- ²¹ Felten, E. W. (2003). Understanding Trusted Computing: Will Its Benefits Outweigh Its Drawbacks? *IEEE Security & Privacy*, 1, 60-62, Schoen, S. (2005). Compatibility, competition, and control in trusted computing environments. *Inf. Secur. Tech. Rep.*, 10(2), pp. 105-119. doi: <http://dx.doi.org/10.1016/j.istr.2005.05.005>
- ²² Vaughan-Nichols J. S. (2003). How Trustworthy is Trusted Computing? *IEEE Computer Society Press*, 36 (3), pp. 18-20.

ability to protect their systems from malicious code and guard their data from theft.

There are numerous criticisms of TC. As mentioned by Vaughan-Nichols some critics say that TC companies are merchandising the technology because it helps online-content owners enforce intellectual-property policies at the expense of the end user.²³ On the other hand TC proponents argue that users have the choice of not installing and running the TC technology if they don't want to use it. Yet, not running the TC technology might mean that such users lose the ability to use applications or download content that will work only with trusted technologies.

Some harsh critics have emerged who will not be easily won over. Richard Stallman, founder of the Free Software Foundation and creator of the well-known GPL open source license is an opponent to TC. He declares that trusted computing or as he brands it "treacherous computing", will allow content providers; together with computer companies to make the computers obey them, instead of the users. The aim of these companies and TC is to make sure that the computers will disobey the users. In other words, the "computer will stop functioning as a general-purpose computer" and "every operation may require explicit permission".²⁴

Arbaugh notes TC's incapability to be used in conjunction with "free" operating systems. This is because, firstly the owner will not be able to load alternate trusted storage root and, secondly, TC does not have the ability to "disable the "extended" capability",²⁵ as a result, the owner will not have the

²³ *ibid.*, p.18

²⁴ Stallman, R. (2002). Can you trust your computer? *NewsForge-The Online Newspaper for Linux and OpenSource*. <http://www.zelig.org/business/02/10/21/1449250.shtml%3Ftid=19.html>

²⁵ Arbaugh, W. (2002). The TCPA; what's wrong; what's right and what to do about it. <http://www.cs.umd.edu/~waa/TCPA/TCPA-goodnbad.pdf>

choice of using any operating system he likes. Consequently, this awaits the danger of circumvention of the GNU Public Licence (GPL). Although GPL requires the TC's result to be Open Source, to compile and to be able to be verified, the source code will not stand-alone, as a TPM-specific certificate will be necessary.²⁶ The latter though, is not an uncontroversial issue. Safford in his attempt to clarify any misunderstandings on the TCPA, states that this is a pure invention and that the TCPA chip can have full functionality without the need for a TPM-specific certificate.²⁷

Microsoft and HP have stated that both Palladium and TCPA will have an open specification, and Linux can be written for it, yet there are no formal guarantees, and thus Microsoft and/or HP retain the capability at some future point to go back on those statements.²⁸

A number of problems will arise from the adoption of TC technology. The foremost problems as stated by the opponents of TC are that sharing will be impossible due to the fact that TC will be used for what they term "Digital Restrictions Management", so that videos, music and other multimedia can be played only on a specified computer. Secondly, Digital Rights Management (DRM) will be used for email and documents, leading to documents and emails that will disappear, or will not be readable on certain computers. Restrictions in downloading and installing all types of software unless permitted by the TC technology may also cause problems. Critics suggest that TC might threaten Open

²⁶ Green, L. (2002). Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers. *Presented in DEFCON 10.* from <http://www.cypherpunks.to/TCPADEFCON10.pdf>

²⁷ Safford, D. (2002a). Clarifying Misinformation on TCPA. *White paper.* from http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

²⁸ Green, L. (2002). Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers. *Presented in DEFCON 10.* from <http://www.cypherpunks.to/TCPADEFCON10.pdf>, Safford, D. (2002a). Clarifying Misinformation on TCPA. *White paper.* from http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

Source Software (OSS) development, as both OSS operating systems and applications may fail to be recognized as trustworthy by TC systems, which will then refuse to run them. In addition, programs that use TC when installed will be able to continually download new authorization rules through the Internet and impose those rules automatically. In such circumstances it is claimed, the computers may apply the new instructions downloaded, without notification, to such a degree that a user will no longer be able to fully interact with their computer.²⁹

It is almost inevitable that TC will cause problems of incompatibility with legacy systems, both hardware and software. As a result, users may find themselves at risk of "forced upgrades" and lost data from old applications e.g. applications whose serial numbers have been removed from support schedules or blacklisted.

Remote Censorship is another "feature" that TC can provide. Applications that delete pirated music or other non-authenticated files via remote-control are possible. It seems likely that, applications that report files that are not authenticated in order to report the user and then remotely delete the files are about to be applied in business models. Anderson refers to this model as "traitor tracing".³⁰

An additional point is that especially for businesses it will be very hard to swap from TC products to any competitors' products. Further, after switching into competitors' products, these products may not work properly on the TC system, or may cause other compatibility problems. For businesses the impact will also be on the economical area. The cost of any swapping between products plus the cost of training the employees for proper use of the new products will be

²⁹ Anderson, R. (2003a). Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA – Version 1.1. (2003). <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

³⁰ *ibid.* p.2 Question 2

extravagant.³¹ Although this paper does not focus on this aspect of TC, this clearly has the potential to raise competition law issues - particularly where existing near-monopoly players such as Microsoft and Intel are involved.³²

Opponents of TC have not been unaware of these implications, and some have claimed that the reason for Intel investing to TC was a “defensive play”.³³ By increasing market size, enlargement of the company will be achieved. Anderson points out that “They were determined that the pc will be the hub of the future home network”. Microsoft, they say, was motivated by the aspiration of embedding entertainment into their empire, the perspective of being able to cut down dramatically software copying, and economic enlargement by the cost created by switching software to any similar competitive products.³⁴

Interoperation with other products is another issue that needs discussion. Interoperation will be achieved only where the vendor wants to be applied. Vendors have a very good reason why they would want the latter to happen: because then all buyers will purchase the same product from the same company – so that they can interoperate with each other – and therefore there will be a network effect. In such a market, the leading company may choose not to interoperate with other companies and thus locking all other companies outside this network and all the users inside it.³⁵

³¹ *ibid.* p.4 Question 6

³² Schoen, S. (2005). Compatibility, competition, and control in trusted computing environments. *Inf. Secur. Tech. Rep.*, 10(2), pp. 105-119. doi: <http://dx.doi.org/10.1016/j.istr.2005.05.005>

³³ Anderson, R. (2003a). Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA – Version 1.1. (2003). <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html> at p.4

³⁴ *ibid.*, p.4 Question 6

³⁵ Felten, E. W. (2003). Understanding Trusted Computing: Will Its Benefits Outweigh Its Drawbacks? *IEEE Security & Privacy*, 1, 60-62.

1.7 Objectives

This thesis grew out of an interest with the technical aspects of Trusted computing as the “last best hope” for a secure internet. As a pure computer scientist, I was fascinated by the technological potential, but instinctively worried by the social implications that seem to be neglected. Looking at law as a way to balance out what I still think as a major power grab by an international consortium, I tried to learn enough about the law to make sense of this development. It soon became transparent that law alone also did not provide an answer, making it necessary to learn about social and economic theories of trust as well. This thesis is the result of an attempt by a computer scientist to make, in her own conceptual framework, enough sense of both law and sociology and to understand how it might apply to TC.

This meant in particular that the thesis is interested in legal concepts, which is abstract structures: abstract forms that “match”, in a parallel reading, what computer technology does, rather than a concept analysis of the doctrinal solution of any specific country. For the legal reader, this cavalier attitude to issues such as jurisdiction, or even the more detailed issue of most of the laws mentioned here might be disconcerting. In this case I ask for indulgence and an openness to the type of question that the thesis tries to answer. Not: what does UK law say about the liability of TC providers, but: can law as a system, at least in principle, come to grips with the technological development hate face? In this it takes much in inspiration from Guadamuz’ book on Networks, Complexity and Internet Regulation. It showed how sociological, computer scientific and legal analysis can work in coronation to give account of a phenomenon in general, without getting bogged down in the particulars of a national legal order. For computer scientists, the often parochial nature of law is a cognitive problem: computer programs compile or don’t compile regardless of what country they are in, Law, as I learned, is very different in this respect, and a major challenge was

to develop an account that remained sufficiently abstract and general and yet sufficiently “legal”.

CHAPTER 2 :

INTRODUCTION TO TRUSTED COMPUTING

2.1 Introduction in Trusted Computing

This section contains an introduction to the technical basis of trusted computing, using as a case study the Trusted Computing Group as arguably the most influential promoter of this technology.¹ A few comments are necessary to put our argument into perspective: Even though this thesis uses the Trusted Computing Group as an example throughout the discussion, this is not intended to be just, or indeed mainly, an analysis of the TCG. Rather, we consider their solution as paradigmatic for a specific philosophy of Internet security. As commentators have noted, even though trusted computing “seemed” to be a highly plausible answer to various threats of cybercrime, the implementation promoted by the TCG failed to achieve the crucial economy of scale and network effect that would have made it from an incremental technological improvement for specialist applications into a game changer.² But this does not mean that we can or should ignore trusted computing as a subject of legal and socio-legal academic inquiry. First, interest in the trusted computing approach has recently gained new momentum, driven on the one hand by cloud computing and virtualization,³ on the other by the Internet of Things and the specific demands

¹ see Proudler, G., Chen, Liqun, Dalton, Chris. (2014). *Trusted Computing Platforms: TPM2.0 in Context* (1 ed.): Springer International Publishing. Chapter 1; see also Huanguo, Z., Jie, L., Gang, J., Zhiqiang, Z., Fajiang, Y., & Fei, Y. (2006). Development of trusted computing research. *Wuhan University Journal of Natural Sciences*, 11(6), pp. 1407-1413. doi: 10.1007/BF02831786

² Sadeghi, A.-R. (2012). *The rise, fall and reincarnation of trusted computing*. Paper presented at the Proceedings of the seventh ACM workshop on Scalable trusted computing, Raleigh, North Carolina, USA (pp. 1-2),ACM.

³ See e.g. Neisse, R., Holling, D., & Pretschner, A. (2011). *Implementing Trust in Cloud Infrastructures*. Paper presented at the Proceedings of the 2011 11th IEEE/ACM

that autonomous, flexible and decomposable systems pose.⁴ The legal issues that we identify in this thesis are likely to reemerge in these new applications of TC. Even more importantly though, the limited success of TC can also be attributed to the divergence of technical, social and legal understandings of “trust”. TC from its inception caused public controversy. Some of this was ill deserved, though partly caused by major mistakes on the side of the TCG to introduce and promote the concept. Others, as we will see, were more serious. TC, if taken serious, would have changed not just some technical details of the way in which computing works. Rather, it would have meant a significant change in the way we relate to our machines, and through them to other citizens of the digital world. By treating

International Symposium on Cluster, Cloud and Grid Computing. , Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). *Towards trusted cloud computing*. Paper presented at the Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California. , Schiffman, J., Moyer, T., Vijayakumar, H., Jaeger, T., & McDaniel, P. (2010). *Seeding clouds with trust anchors*. Paper presented at the Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA. , Zhidong, S., Li, L., Fei, Y., & Xiaoping, W. (2010, 11-12 May 2010). *Cloud Computing System Based on Trusted Computing Platform*. Paper presented at the Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on (pp. 942-945), for the specific problems caused by multi-cloud environments see AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). *Cloud Computing Security: From Single to Multi-clouds*. Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on (pp. 5490-5499), IEEE.

- ⁴ See e.g. Gessner, D., Olivereau, A., Segura, A. S., & Serbanati, A. (2012, 25-27 June 2012). *Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things*. Paper presented at the Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 998-1003), IEEE, Ukil, A., Sen, J., & Koilakonda, S. (2011, 4-5 March 2011). *Embedded security for Internet of Things*. Paper presented at the Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on (pp. 1-6), IEEE. Skeptical on the usefulness of TC for the IoT is Hoepman, J.-H. (2012). In Things We Trust? Towards Trustability in the Internet of Things. In R. Wichert, K. Van Laerhoven & J. Gelissen (Eds.), *Constructing Ambient Intelligence* (Vol. 277, pp. 287-295): Springer Berlin Heidelberg.

TC as a mere technical fix, the wider societal implications of TC were ignored, and as a result the “suitability” of the social and socio-legal environment for the approach was insufficiently understood.

Law plays in this picture a dual role. It can hinder the development of TC by exposing TC providers with new and difficult to quantify litigation risks, or it can fail to protect the reasonable expectation of consumers of TC to have remedies in case TC causes them harm. Conversely, it could promote TC by matching or underwriting the technological concept of trust with a legal or socio-legal concept of trust – if as a user, I was entitled to “trust” a computer system as the term is understood in the technology community, and the legal system rewards this trust by protecting the reliance I put into the system through appropriate remedies, then I’ll be much more likely to accept the shortcomings associated with TC. As we will see in more detail, this “matching” or “isomorphism” between technical and legal understandings of trust was never really developed or made fully explicit; something which we claim contributed to the lack of uptake of TC. Crucially though, these problems were not (just) the result of the specific approach the TCG took, though the history, corporative structure and communication strategy of the TCG did not help to instill public trust in their product. Rather, we will argue that systemic features of the TC philosophy itself are inevitably creating legal issues for which the legal system is badly prepared. Some of them are of a more technical doctrinal nature, but underlying them all are fundamental legal and jurisprudential issues which generally make “scale-free law” (in the terminology of Guadamuz) difficult to achieve. To the extent that *any* approach to cybersecurity is based on “scale free” trust and self-organizing trust networks in the way TC is, law is in danger of being left behind. But as law is left behind, so is one of the major instruments for governments to instill social acceptance and *public* trust in institutions, as opposed to *personal* trust between individuals. While in theory, TC as a computing paradigm could work as a purely self-organising, complex network that is based on nothing but individual trust

relations, in reality and in its implementation it is crucially dependent on public trust in the TCG as an institution. It is at this nexus between personal and public trust, Trusted Computing and the Trusted Computing Group as a paradigmatic institution; that the most pressing conceptual issues emerge.

As indicated above, this analysis is less concerned with the TCG as a specific historical and contingent group that tries to make the Internet more secure. Rather, the TCG is seen as but an example, or even an “ideal type”, for the type of institution that may find itself charged with providing Internet security. As an ideal type, we can contrast it to approaches that try to ensure Internet security directly through the state – that approach sees the Internet as equivalent of public roads or “the king’s highway” whose maintenance and security is a core provision of the nation state, and backed where necessary by non-negotiable sanctions. Equally, we can contrast it with approaches that leave Internet security solely or primarily an issue to be addressed by individual users – the approach that gave us firewalls or anti-virus software that individuals have to install, sometimes for payment, on their own machines and can configure to their liking. Similarly, we treat TC as the security paradigm promoted by the TCG as a paradigmatic case for an entire family of programming and development approaches to Internet security. As any approach to Internet security, it has to balance often conflicting demands, including privacy, costs, security, user autonomy and transparency. TC proposes, as we will see, a very specific mix of these characteristics, with different degrees of emphasis on each of them. Some of these choices result in core commitments that can be used to characterize a class of approaches to Internet security. To the degree that these design choices raise interesting legal issues, all approaches that share these features will raise similar challenges. To illustrate this point, a short example that will be discussed in more detail later may suffice. While trusted computing tries to make using the Internet more secure, it is not

what is technically known as “secure computing”.⁵ Proudler draws the distinction like this:

- “Secure” is a classification, the result of an assessment to determine that an item does exactly what it is supposed to do, nothing more and nothing less.
- Something can be trusted if it behaves as expected.
- Something is trustworthy if its behaviour is predictable.

We can draw here an analogy from the epistemology and history of science that may help some readers to understand the difference. “Secure computing”, as defined above, corresponds to the Cartesian ideal of security - we can prove, using only undisputable (“clare et distincte”, in Descartes’ words) axioms and equally certain rules of inference, that a given machine will never do anything else but what is expected of it. Trusted computing by contrast is Humean, or maybe Popperian in its approach. It is based on observations and inductive inferences: “Right now this machine seems to be performing as intended, and it also did so in the past, so we probably can trust it for time being.” Once new information comes in, we may have to revisit (falsify) this conclusion, which is tentative like all knowledge. Finally, “trustworthy”, in Proudler’s somewhat idiosyncratic definition, is something that is predictable. Staying with the analogy, “trustworthy” is a judgment that raises Hume’s problem of induction – an extrapolation from past and present observed behavior to the future.⁶ He continues this discussion by accepting that trusted computing is less secure than secure computing, but that secure computing is prohibitively expensive, whereas

⁵ Proudler, G., Chen, Liqun, Dalton, Chris. (2014). *Trusted Computing Platforms: TPM2.0 in Context* (1 ed.): Springer International Publishing. p. 9ff.

⁶ We assume Proudler means that behavior is trustworthy if it is predictably benevolent. A known fraudster’s behavior might be highly predictable, but only in the sense that we can trust him to be up to no good. In the same vein, we can “trust” Microsoft products to predictably not work as intended but have bugs etc.

trusted computing, while far from being cost-neutral, could benefit from the economies of scale to deliver a higher degree of protection at viable costs. Or in his own word:

“The overwhelming majority of commercial users won’t consider owning secure computers because they are too expensive. Trusted platforms are less secure than secure platforms, but cheaper to buy because they are manufactured in huge quantities, and cheaper to maintain because they can provide variable levels of protection, even when the platform’s software changes. This compromise should promote an increased level of protection in commercial computers.”⁷

The dilemma that he describes here is one that every technological solution to computer vulnerabilities faces – make it too secure, and nobody but the military can afford it, and even they only for the most security critical tasks, or make it affordable, but trade in a bit of security. Every system that opts like the TCG for affordable yet imperfect security faces however two issues – one purely legal, the other a technico-legal problem. The first is a simple question of liability. Because TC is a less-than-perfect solution to the security challenge, things can – and given enough time – will go wrong.⁸ At the same time, TC increases

⁷ Ibid., p.9

⁸ as the ongoing studies in vulnerabilities of TC, and how they can be rectified, shows. The approach is, as we argued above, Popperian, and continues to evolve through a system of trials and errors. See e.g. Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013). *Trusted Computing vs. Advanced Persistent Threats: Can a Defender Win This Game?* Paper presented at the Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC) (pp. 396-403),IEEE.; see also e.g. Zhu, L., Zhang, Z., Liao, L., & Guo, C. (2012). A Secure Robust Integrity Reporting Protocol of Trusted Computing for Remote Attestation under Fully Adaptive Party Corruptions. In Y. Zhang (Ed.), *Future Wireless Networks and Information Systems* (Vol. 143, pp. 211-217): Springer Berlin Heidelberg. for a study of one specific identified vulnerability, fully adaptive party corruption. For a study that recommends combining TCG with other solutions to plug identified security issues see e.g. Aslam, M., Gehrmann, C., & Björkman, M. (2013). *Continuous security evaluation and auditing of remote platforms by combining trusted computing and security automation techniques*. Paper presented

nonetheless the costs of computing, as even its most ardent supporters acknowledge.⁹ Consumers will only buy TC protected computers if they think the investment is worthwhile – and that means for the vendor to emphasize the added security that it offers.¹⁰ An obvious conflict of interests arises – the advertising department will want to emphasize the protection that the product offers, the legal department will want to put as many liability exclusion clauses into the contract with the customer as possible.¹¹ But the more aggressive the advertising extolling the virtues of TC is, the more likely customers will believe they have bought actual security, and not just a “trusted” system. The systematic ambiguity between the everyday notion of “trusted” that identifies it with “trustworthiness” with the much more limited meaning that term has in computing circles, will likely exacerbate this problem. At some point, courts may

at the Proceedings of the 6th International Conference on Security of Information and Networks, Aksaray, Turkey (pp. 136-143),ACM.

- ⁹ See for a non-partisan analysis Vishik, C., Sheldon, F., & Ott, D. (2013). Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment. In H. Reimer, N. Pohlmann & W. Schneider (Eds.), *ISSE 2013 Securing Electronic Business Processes* (pp. 133-147): Springer Fachmedien Wiesbaden.
- ¹⁰ On the problem of cost benefit analysis in Internet security , see Anderson, R. (2001). *Why information security is hard - an economic perspective*. Paper presented at the Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual (pp. 358-365),IEEE. Particularly relevant for the point here his attempt to include psychological analysis of consumer behaviour in Anderson, R., & Moore, T. (2009). *Information security: where computer science, economics and psychology meet* (Vol. 367). On the empirical basis for making rational decisions on security investment see also Gordon, L., & Loeb, M. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, 8(5), pp. 335-337. doi: 10.1007/s10796-006-9010-7; This issue affects not only consumers, but also companies and public sector entities, see e.g. Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, 24(1), pp. 37-59. doi: <http://dx.doi.org/10.1016/j.jaccpubpol.2004.12.003>.
- ¹¹ On this problem see the hart-hitting presentation by Virvilis, N. (2015). *Advanced Persistent Threats: The Empire Strikes Back!* , pp. 16-19.

have to decide if the customer's understanding of what they bought should get precedence over liability exclusion clauses hidden deep in the terms and conditions – especially if any mistake on her side was caused by overselling the security benefits of TC.¹² Even more problematic, customers might engage in more risky behavior because they consider themselves safe. This problem is discussed in behavioral psychology as the “risk compensation problem”. This hypothesis, which postulates that people will often act more careful when they sense greater risk and less careful if they feel protected, originated in road safety research in the 1970s and is sometimes named “Peltzman effect”. Peltzman had argued that even though road safety regulation should have made driving much safer, in reality no such reduction in accident rates could be found. He attributed this to the fact that in the now theoretically safer environment, drivers were willing to take greater risks that compensated for any improvements the regulations may have had.¹³ While Peltzman had looked at the effect of safety regulation in particular, his idea was soon extended to other form of security, in particular security by design. The relative failure to reduce deadly bicycle accidents despite more widespread use of helmets has been attributed to risk compensation strategies by both bicyclist and car drivers.¹⁴ Some studies have indicated that the use of helmets in skiing had similar consequences, with

¹² Coming to a similar conclusion as we here is Oppliger, R., & Rytz, R. (2005). Does Trusted Computing Remedy Computer Security Problems? *IEEE Security and Privacy*, 3(2), pp. 16-19. doi: <http://dx.doi.org/10.1109/MSP.2005.40>, who argues on p.19 that in a TC world, courts will be more likely to hold manufacturers liable for faulty products.

¹³ Peltzman, S. (1975). The Effects of Automobile Safety Regulation. *Journal of Political Economy*, 83(4), pp. 677-725. doi: 10.2307/1830396.

¹⁴ Rodgers, G. (1988). Reducing bicycle accidents: A reevaluation of the impacts of the CPSC bicycle standard and helmet use. *Journal of Products Liability*, 11(4), pp. 307-317.

helmeted drivers taking greater risks of increased speed.¹⁵ The failure of condom distribution to stem the flow of AIDS as much as predicted was finally attributed by some to risk compensation, where condom wearers had more sexual partners than non-wearers.¹⁶ It should be noted that many of these findings are contested.¹⁷ It is probably safe to say that Peltzman's own initial idea of a "perfect" compensation where most if not all temporary reduction in risk is ultimately compensated by more risky behavior and a return to the status quo. As Vrolix on one of the most comprehensive meta-studies argued:

"Behavioural adaptation generally does not eliminate the safety gains from programmes, but tends to reduce the size of the expected effects".¹⁸

-
- ¹⁵ Ružić, L., & Tudor, A. (2011). Risk-taking Behavior in Skiing Among Helmet Wearers and Nonwearers. *Wilderness & Environmental Medicine*, 22(4), pp. 291-296. doi: <http://dx.doi.org/10.1016/j.wem.2011.09.001>
- ¹⁶ Wilson, N. L., Xiong, W., & Mattson, C. L. (2014). Is sex like driving? HIV prevention and risk compensation. *Journal of Development Economics*, 106(0), pp. 78-91. doi: <http://dx.doi.org/10.1016/j.jdeveco.2013.08.012>
- ¹⁷ On risk compensation and bicycle helmets, the figures have been questioned eg. by Phillips, R. O., Fyhri, A., & Sagberg, F. (2011). Risk Compensation and Bicycle Helmets. *Risk Analysis*, 31(8), pp. 1187-1195. doi: 10.1111/j.1539-6924.2011.01589.x; for skiing and risk taking, Ruedl, G., Pocecco, E., Sommersacher, R., Gatterer, H., Kopp, M., Nachbauer, W., & Burtscher, M. (2010). Factors associated with self-reported risk-taking behaviour on ski slopes. *British Journal of Sports Medicine*, 44(3), pp. 204-206. doi: 10.1136/bjism.2009.066779 concluded that "Safety helmets clearly decrease the risk and severity of head injuries in skiing and snowboarding and do not seem to increase the risk of neck injury, cervical spine injury, or risk compensation behavior". Mattson finally failed to replicate the findings that indicated that risk compensation played a role in certain HIV prevention strategies, see Mattson, C. L., Campbell, R. T., Bailey, R. C., Agot, K., Ndinya-Achola, J. O., & Moses, S. (2008). Risk Compensation Is Not Associated with Male Circumcision in Kisumu, Kenya: A Multi-Faceted Assessment of Men Enrolled in a Randomized Controlled Trial. *PLoS ONE*, 3(6), pp. e2443. doi: 10.1371/journal.pone.0002443.
- ¹⁸ Vrolix, K. (2006). Behavioral adaptation, risk compensation, risk homeostatis and moral hazard in traffic safety. *Transportation Research Institut Economics and Public Policy Report*, pp. 1-59.

Quantification of risk compensation is methodologically difficult and the results often contested.¹⁹ Nonetheless, Vrolix's meta-study indicates that the phenomenon is real, though its effects can range from the marginal to the substantive. Currently, there seems to be little knowledge on what type of risk environment is conducive or adverse to risk compensation strategies. Despite these difficulties, theories of regulation increasingly accept that empirical studies on the effects of risk compensation are necessary to find an efficient mix of regulatory tools, from law to technological design.²⁰ There are at present no studies done for cybersecurity.²¹ This raises the possibility that the game theoretical models to predict cybersecurity risks²² and appropriate responses are

-
- ¹⁹ see Dulisse, B. (1997). Methodological issues in testing the hypothesis of risk compensation. *Accident Analysis & Prevention*, 29(3), pp. 285-292. doi: [http://dx.doi.org/10.1016/S0001-4575\(96\)00082-6](http://dx.doi.org/10.1016/S0001-4575(96)00082-6). See also Streff, F. M., & Geller, E. S. (1988). An experimental test of risk compensation: Between-subject versus within-subject analyses. *Ibid.*, 20(4), pp. 277-287. doi: [http://dx.doi.org/10.1016/0001-4575\(88\)90055-3](http://dx.doi.org/10.1016/0001-4575(88)90055-3). Some of the problems are that ethical yet accurate methodologies are difficult to find: Underhill, K. (2013). Study designs for identifying risk compensation behavior among users of biomedical HIV prevention technologies: Balancing methodological rigor and research ethics. *Social Science & Medicine*, 94(0), pp. 115-123. doi: <http://dx.doi.org/10.1016/j.socscimed.2013.03.020>. A partial solution is offered in Thompson, D. C., Thompson, R. S., & Rivara, F. P. (2001). Risk compensation theory should be subject to systematic reviews of the scientific evidence. *Injury Prevention*, 7(2), pp. 86-88. doi: 10.1136/ip.7.2.86.
- ²⁰ Hedlund, J. (2000). Risky business: safety regulations, risk compensation, and individual behavior. *Ibid.*, 6, pp. 82-89. doi: 10.1136/ip.6.2.82.
- ²¹ at least the author was not able to find one after an exhaustive database search. The closest match for the purposes of this thesis is Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, 4(3), pp. 340-347. doi: 10.1177/1948550612455931, which however does not deal with cybersecurity directly, but the question of control over one's information in general.
- ²² authoritative Alpcan, T., & Başar, T. (2010). *Network security: A decision and game-theoretic approach*: Cambridge University Press. See also Grossklags, J., Christin, N., & Chuang, J. (2008). *Secure or insure?: a game-theoretic analysis of information*

based on mistaken empirical assumptions. Trusted Computing in particular is a plausible candidate for risk compensation, for the reasons identified above. To the extent that game theoretical models of cyberrisk are used to validate TC,²³ this should be a concern.

Risk compensation also poses a potential issue for legal regulation. Delictual liability will typically involve a “reasonable man on the street” or “reasonable foreseeability”. But it may be in the very nature of “trusted” systems to change our perception of what a “reasonable” person would do and what risks she is willing to take. Behaviour that would be deemed as obviously risky in a non-TC environment may well be deemed as “reasonable reliance on the TC certificate” by a future judge or jury, thus giving risk compensation a legal blessing. We will come back to this issue when we discuss the challenges that TC poses for the liability regime in general. Here we simply note that it is this type of issue in the interface of law and technology – germane to all approaches to cybersecurity that are based on certified trustworthiness – that this thesis ultimately tries to explore, using the TCG as an example.

In what follows we will discuss the history of TC from its beginning, the structure of the organization which developed the TC technology (Trusted Computing Group), and the aims and objectives of TCG.

As more and more of our activities are carried out online, it has become increasingly clear over the past decades that the internet, which was never

security games. Paper presented at the Proceedings of the 17th international conference on World Wide Web, Beijing, China (pp. 209-218),ACM.

²³ For an overview see Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Qishi, W. (2010, 5-8 Jan. 2010). *A Survey of Game Theory as Applied to Network Security*. Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on (pp. 1-10),IEEE. For a case study see e.g. Hoffmann, H., & Söllner, M. (2014). Incorporating behavioral trust theory into system development for ubiquitous applications. *Personal and Ubiquitous Computing*, 18(1), pp. 117-128. doi: 10.1007/s00779-012-0631-1.

intended for this type of commercial activity, is vulnerable to attacks and criminal activities. Infected computers are the main element of a botnet,²⁴ which in turn enables the type of large scale Denial of Service (DoS) attack that threatens the very existence of the net.²⁵ Additionally, botnets are a major source of spam, spyware, adware, click-fraud, access number replacements, and fast flux, mostly driven by the botmasters' financial interests and secondly used in political or military contexts.²⁶ Recent statistics presented by Eurostat, demonstrate that 31% of internet users in the EU27 caught a computer infection which resulted in loss of information in the last 12 months.²⁷

²⁴ Botnets are networks formed by infected compromised machines which connect to a central server and compromise the host system. The European Network and Information Security Agency (ENISA) – the EU's cyber security agency, provided a comprehensive report. See also on how to assess botnet threats including various types of best-practices to measure, detect and defend against botnets and recommendations on how to neutralise them, preventing new infections and minimising cybercrime profitability from botnets use. The document also examines the role of governments in the fight against botnets, and points out what legislation is needed and what investment is required Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, Measurement, Disinfection & Defence. In G. Hogben (Ed.), *ENISA's Emerging and Future Risk programme* (pp. 153): European Network and Information Security Agency (ENISA). Rajab et. al present challenges on botnet detection and tracking and an approach to infiltrate large numbers of botnets in Rajab, M. A., Zarfoss, J., Monroe, F., & Terzis, A. (2006). *A multifaceted approach to understanding the botnet phenomenon*. Paper presented at the Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, Rio de Janeiro, Brazil.

²⁵ Bayer, U., Habibi, I., Balzarotti, D., Kirda, E., & Kruegel, C. (2009). *A view on current malware behaviors*. Paper presented at the LEET'09: Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more, Boston, MA, USA. http://www.eurecom.fr/people/vs_bayer.en.htm

²⁶ Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, Measurement, Disinfection & Defence. In G. Hogben (Ed.), *ENISA's Emerging and Future Risk programme* (pp. 153): European Network and Information Security Agency (ENISA), Wikipedia. (2011, 16/7/2011). Botnet. Retrieved 28/6/2011, 2011, from http://en.wikipedia.org/wiki/Botnet#Types_of_attacks

²⁷ Eurostat. (2011). Nearly one third of internet users in the EU27 caught a computer virus 8 February 2011: *Safer Internet Day*. Luxembourg: Eurostat Press Office.

Recently, most frequently than ever, powerful organised crime gangs target as victims uninformed and unprepared consumers and exploit weaknesses in their computer systems. Attempts to deal with the growing number of reported cybercrime incidents include legislation, user training, public awareness, and other technical security measures.²⁸ The UK government recognizes the detrimental impact that a cyberattack can have on the economy and the social well being of the country²⁹ and the effect of how nations deal with internet freedom and security. While the legal system struggles to keep up with technology developments and their enforcement and prosecution, the regulation through technology took increasingly center stage.³⁰ Rather than prosecuting

-
- ²⁸ EU fights against cybercrime and has implemented a strategy European Commission. (2013a). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. In T. C. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS (Ed.): European Commission. EU elaborates more in its recent digital agenda European Commission. (2015, 2/3/2015). Cybersecurity. Retrieved 26/6/2015, 2015, from <https://ec.europa.eu/digital-agenda/en/cybersecurity#Article>. See also UK's strategy report Cm7642. (2009). *Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space*. London: The Stationery Office Limited.
- ²⁹ Cm7234. (2007). The Government reply to the fifth report from the House of Lords Science and Technology committee. London: The Stationery Office Limited, Cm7948. (2010). *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. London: The Stationery Office Limited. The Home Office minister Baroness Neville-Jones presented an estimation that cybercrime costs UK £27bn each year in UK Cabinet Office and National security and intelligence. (2011). *The Cost of Cyber Crime - full report*. UK: Detica Limited.
- ³⁰ See also Lessig, L. (1996). The Zones of Cyberspace. *Stanford Law Review*, 48(5), pp. 1403-1411. , Pagallo, U. (2015). Good onlife governance: On law, spontaneous orders, and design *The Onlife Manifesto* (pp. 161-177): Springer, Yeung, K. (2008). Towards an Understanding of Regulation by Design. In K. Yeung (Ed.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 79-108). Oxford: Hart, Yeung, K., & Dixon-Woods, M. (2010). Design-based regulation and patient safety: a regulatory studies perspective. *Social Science & Medicine*, 71(3), pp. 502-509.

crime, the focus shifted on communicating architectures that make it impossible to commit crimes in the first place.

One such architecture is Trusted Computing (TC), which has been in the centre of technical, social and legal interest over the past 15 years, aiming to be part of our lives in the near future. TC is an approach that aims to allow the computer user to trust his own computer and for “others” to trust that specific computer.³¹ In a more explanatory way, as Ross Anderson noted “TC provides a computing platform on which you can't tamper with the application software, and where these applications can communicate securely with their authors and with each other”.³²

Back in 2003, the Trusted Computing Group (TCG) (formerly known as the Trusted Computing Platform Alliance (TCPA)) – a non-profit organization – formed an alliance of promoters like AMD, Hewlett-Packard (HP), IBM, Intel Corporation, Microsoft, Sun Microsystems Incorporation, Fujitsu Limited and of contributors like Canon, Dell, Erickson, Google, Oracle, Samsung, and many more; and initiated the Trusted Computing (TC) project.³³ The TCG works on the creation of a new computing platform that would provide enhanced trust to the current platform and aims to develop, define and promote standards to achieve higher security levels for the Information Technology (IT) infrastructure between multiple platforms, devices and networks.³⁴

³¹ Lohmann von F. (2003). *Meditations on Trusted Computing*. Retrieved from http://www.eff.org/Infrastructure/trusted_computing/20031001_meditations.php

³² Anderson, R. (2003a). Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA – Version 1.1. (2003). <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

³³ Full memberships list can be found at: http://www.trustedcomputinggroup.org/about_tcg/tcg_members

³⁴ Berger, B. (2005). Trusted computing group history. *Inf. Secur. Tech. Rep.*, 10(2), pp. 59-62. doi: 10.1016/j.istr.2005.05.007, TCG. (2010). Trusted Computing Group. 2010, from <http://www.trustedcomputinggroup.org/>

2.2 Trusted Computing fundamentals

Computer Security is the subject dealing with fundamental security functionalities. Researched since the 1960's, it has by now created a substantial literature.³⁵ Trusted computing is a specific approach within the broader area of Computer security. While the term was coined in the late 1990s, some of the basic insights and ideas can be traced back to Lampson's seminal "Protection" paper from 1974.³⁶ Based on these initial studies, the rationale for the emergence of trusted computing has accumulated during the last two decades.³⁷ While computer systems have changed in nature and become more and more ubiquitous, many technical challenges came into sight and led to the realization that system designers must proceed to design new computing systems that offer a higher amount of trust than the currently implemented ones. Prevention of denial of service, the performance of access control and monitoring and the achievement of scalability are just some of the numerous technical challenges that need to be overcome by the current distributed systems. The need for such a platform becomes more imperative by the recognition that it is insufficient to rely on users taking the necessary precautions to protect their systems themselves (by frequently updating firewalls and anti-virus systems) and that the threats and attacks have amazingly increased due to automated attack tools, proliferation of vulnerabilities and increased mobility of users.³⁸ CERT

³⁵ Gollmann, D. (1999). *Computer security*. New York, NY, USA: John Wiley & Sons, Inc, Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in Computing* (4th ed.). Upper Saddle River, NJ, USA: Prentice Hall PTR.

³⁶ Lampson, B. W. (1974). Protection. *ACM SIGOPS Operating Systems Review*, 8(1), pp. 18-24. doi: 10.1145/775265.775268

³⁷ See e.g. Lampson's later paper England, P., Manferdelli, J., & Willman, B. (2003). A trusted open platform. *Computer*, 36(7), pp. 55-62. doi: 10.1109/MC.2003.1212691, that now uses the term of "trusted platform".

³⁸ See also Berger, B. (2005). Trusted computing group history. *Inf. Secur. Tech. Rep.*, 10(2), pp. 59-62. doi: 10.1016/j.istr.2005.05.007, Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security:

Coordination Center has reported the extremely large amount of vulnerabilities catalogued until 2008.³⁹

Furthermore, it has been found that software-only security mechanisms cannot provide sufficient protection for the whole system.⁴⁰ TC consequently mixes software and hardware based solutions – as we will see this constitutes another cause for legal concerns as the contractual regime for software and hardware differs. A related problem are existing unsecured operating systems that currently do not provide single application isolation - thus reducing to the minimum the platform security level – which is found in diverse environments following the same security requirements. It is not possible to rebuild the Internet from scratch. Rather, to use the metaphor von Neurath used to characterize the attempts by philosophers to clarify language:

“We are like sailors who on the open sea must reconstruct their ship but are never able to start afresh from the bottom. Where a beam is taken away a new one must at once be put there, and for this the rest of the ship is used as support. In this way, by using the old beams and driftwood the ship can be shaped entirely anew, but only by gradual reconstruction.”⁴¹

Legacy systems are a difficult issue for all cybersecurity strategies, and for TC in particular.⁴² At the core of TC is the idea that a computer should only communicate with a system that can proof its trustworthiness – something that

Pathways to vulnerabilities. *Computers & Security*, 28(7), pp. 509-520. doi: <http://dx.doi.org/10.1016/j.cose.2009.04.006>.

³⁹ CERT. (2009, February 12, 2009). CERT Statistics (Historical). *Cataloged vulnerabilities*. Retrieved April 2010, 2010, from http://www.cert.org/stats/cert_stats.html#vuls

⁴⁰ Berger, B. (2005). Trusted computing group history. *Inf. Secur. Tech. Rep.*, 10(2), pp. 59-62. doi: 10.1016/j.istr.2005.05.007

⁴¹ As explained by Quine, W. V. O. (1960). *Word & Object*. Cambridge: The MIT Press.

⁴² See e.g. Schellekens, D., Wyseur, B., & Preneel, B. (2008). Remote attestation on legacy operating systems with trusted platform modules. *Science of Computer Programming*, 74(1-2), pp. 13-22. doi: <http://dx.doi.org/10.1016/j.scico.2008.09.005>.

requires an account of its software and hardware. While it is at least possible to update old software that is not TC compliant, this will typically not be possible with the necessary hardware component. As a consequence, the TC revolution, were it to happen, could make a significant number of existing hardware obsolete. This is not just a problem for public acceptance; it also raises legal and regulatory issues. TC is inherently also a problem for competition law.⁴³ These problems become heightened if TC is “discriminatory” not just against newly developed non-TC systems, where open standards can at least mitigate this problem (and be it at a cost and, as we will see later, never perfectly), but also against past systems that predate TC and can’t be easily upgraded in their hardware part.

In addition to the increasing security threats, the ease with which to write and spread malicious code (even ubiquitously), the vast number of personal computers along with the substantial use and incredible evolution of the Internet during the last 15 years,⁴⁴ have led to the conclusion that systems with increased security, high confidentiality, integrity, non-repudiation, high-availability and authenticity should be deployed.⁴⁵ Thus the three basic conditions that a trusted environment, in the computer science sense, must fulfill are: protected capabilities; integrity measurement; integrity reporting, all creating and ensuring

⁴³ See e.g. Anderson, R. (2003b). ‘Trusted Computing’ and Competition Policy—Issues for Computing Professionals. *Open Knowledge*, pp. 35. , Anderson, R. (2004). Cryptography and Competition Policy - Issues with ‘Trusted Computing’ *Economics of Information Security* (Vol. 12, pp. 35-52): Springer US.

⁴⁴ Stats, I. W. (2009). Usage and Population Statistics. from <http://www.internetworldstats.com/stats.htm>

⁴⁵ Oppliger, R., & Rytz, R. (2005). Does Trusted Computing Remedy Computer Security Problems? *IEEE Security and Privacy*, 3(2), pp. 16-19. doi: <http://dx.doi.org/10.1109/MSP.2005.40>

platform trust.⁴⁶ Systems covering these aspects are described as “trustworthy”.⁴⁷

2.3 Trusted Computing Group – The History

The Trusted Computing Group (TCG) is a non-profit corporate organization whose stated aim is “to develop, define and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals and devices”.⁴⁸ It was originally formed as an industry working group, by Compaq, Hewlett-Packard, IBM, Intel and Microsoft in January 1999 with the name Trusted Computing Platform Alliance (TCPA). From 1999 until 2003 TCPA released a number of specifications which mainly focused in enhancing trust and security in computing platforms. In early 2001 the first specifications were released, defining the Trusted Platform Module (TPM) as the fundamental component of a trusted platform.

In April 2003, TCPA was renamed to TCG adopting all the specifications released by TCPA and continuing its original development with broader horizons⁴⁹ and extending the invitation for other companies to join the alliance. TCG is headquartered in Portland, Oregon, but has an international membership.

⁴⁶ Burmester, M., & Mulholland, J. (2006, April 23 - 27). *The advent of trusted computing: implications for digital forensics* Paper presented at the Proceedings of the 2006 ACM symposium on Applied computing, Dijon, France (pp. 283-287),ACM Press.

⁴⁷ Kallath, D. (2005). Trust in trusted computing - the end of security as we know it. *Computer Fraud and Security, 2005(12)*, pp. 4-7. doi: 10.1016/S1361-3723(05)70283-9, Shirey, R. (2000). *RFC2828: Internet Security Glossary*: RFC Editor.

⁴⁸ TCG. (2010). Trusted Computing Group. 2010, from <http://www.trustedcomputinggroup.org/>

⁴⁹ Berger, B. (2005). Trusted computing group history. *Inf. Secur. Tech. Rep., 10(2)*, pp. 59-62. doi: 10.1016/j.istr.2005.05.007

2.4 Trusted Computing Group – Structure

Most computing industry bodies are structured based on organization structures and governance models defined by bylaws,⁵⁰ and TCG is not an exception to that. As mentioned by Berger, the structure includes an open membership model, a board of directors, promoters and contributors, and a reciprocal reasonable and non-discriminatory (RAND) patent licensing policy among members. Thus, this structure enables the expansion and the promotion of open industry specifications. Membership requires a membership fee. This was later reduced for small companies, to enable them to benefit from the work of the group.⁵¹ As we will see in more detail later, in addition to the usual monopoly and competition problems that comes with the territory of standard setting, TC by its very nature risks to exclude “outsiders” from the market. We indicated above the potential competition issues with a TC approach: entities that are not TC certified will be unable to communicate with other TC systems. Our research could not establish if the late concession of a reduced membership fee was an example of enlightened altruism that recognized genuine advantages to have smaller companies “on board”, to preempt competition law challenges, or if it was even the result of external pressure. It is however important to note that this model still potentially deters many developers, especially non-commercial, open source and creative commons programmers.

Potentially exacerbating this issue of exclusions, is the internal structure of the TCG. Currently the members are divided into three main hierarchical groups: at the top are the promoters – essentially the organizations that took the preliminary steps necessary for the formation of the corporation; the contributors – organizations that contribute to the corporation; and the adopters

⁵⁰ *ibid.*, p.59

⁵¹ Rosteck, T. (2008). Die Trusted Computing Group. In N. Pohlmann & H. Reimer (Eds.), *Trusted Computing* (pp. 15-20): Vieweg+Teubner.p17.

– organizations that may adopt some of the technological outcomes of the organization. The last two groups in 2009 numbered more than 130 members, however currently this number has dropped⁵² while TCG is still inviting active member participation.⁵³ There is however no legally enforceable “right” to member TCG, let alone to be part of any specific one of the three levels, and no judicial review were a company to be excluded.

Leading members (i.e. promoters) govern TCG via a board comprised of AMD, HP, IBM, Intel, Microsoft, CISCO and Fujitsu. Members (i.e. contributors and adopters) cover a variety of companies drawn from areas like computing, software developers, systems vendors and network and infrastructure companies.

TCG distributes a number of key deliverables containing hardware and software specifications, white papers and other materials that help the promotion and adoption of the specifications. The deliverables aim to help the data management and the digital identities increase security and protection from external software attack and data theft. Furthermore, these specifications offer the ability to be used for more secure remote access.

2.5 Trusted Computing Group and the creation of trust

TCG was formed as a result of the concerns on data exposure on systems; system compromise as part of software attack; and lack of methods to prevent identity theft.⁵⁴ TC is an idea which has evolved from the need to address these

⁵² e.g. Sun Microsystems and Sony Corporation have been withdrawn from their membership in TCG. The first has been acquired and later merged with Oracle and has not renewed their TCG membership since.

⁵³ TCG. (2006a). Membership. Retrieved 4th May, 2011, from http://www.trustedcomputinggroup.org/about_tcg/tcg_members, TCG. (2006b). Membership Levels. Retrieved 4th May, 2011, from http://www.trustedcomputinggroup.org/join_now/

⁵⁴ Berger, B. (2005). Trusted computing group history. *Inf. Secur. Tech. Rep.*, 10(2), pp. 59-62. doi: 10.1016/j.istr.2005.05.007, TCG. (2006c). More Secure Computing TCG.

issues with security solutions that will mitigate the risks and dangers; and help to increase data management and identity security. Furthermore, its aim is to protect the software and data in computer platforms (servers, desktops, laptops, PDA's, mobile phones and many more)⁵⁵ from external attacks and physical theft and hopes to improve security for remote access. Trusted Computing aims to add on computer hardware's functionality to "enable entities with which the computer interacts to have some level of trust in what the system is doing".⁵⁶ This protection is provided by implementing isolated execution environments where software and data will be protected from any interference – not just by third parties but also the owner of the computers. Trusted platforms provide such environments and define the applications that will be permitted to operate on selected data.⁵⁷ Additionally, trusted platforms can offer assurances about their behaviour both in hardware and software.⁵⁸

As we indicated above, 'Trust' has different interpretations in different disciplines –relevant for "techno-trust" is the definition of trusted systems according to RFC 2828⁵⁹ and discussed further by Balacheff et al. and Mitchell.⁶⁰

⁵⁵ Proudler, G. (2005). Concepts of trusted computing. In C. J. Mitchell (Ed.), *Trusted Computing* (Vol. 6, pp. 11-27). London, UK: The Institution of Engineering and Technology (IET).

⁵⁶ Mitchell, C. J. (2008). What is Trusted Computing? In C. J. Mitchell (Ed.), *ibid.* (pp. 1-10). p.3

⁵⁷ Proudler, G. (2005). Concepts of trusted computing. In C. J. Mitchell (Ed.), *ibid.* (pp. 11-27).

⁵⁸ Gallery, E. (2008). *Who are the TCG and what are the Trusted Computing concepts?* Paper presented at the TRUST2008, Villach, Austria. Presentation retrieved from <http://dblp.uni-trier.de/pers/hd/g/Gallery:Eimear>

⁵⁹ Shirey, R. (2000). *RFC2828: Internet Security Glossary*: RFC Editor.

⁶⁰ Balacheff, B., Chen, L., Pearson, S., Proudler, G., & Chan, D. (2000). Computing Platform Security in Cyberspace. *Information Security Technical Report*, 5(1), pp. 54-63. doi: 10.1016/S1363-4127(00)87631-1, Mitchell, C. J. (2008). What is Trusted Computing? In C. J. Mitchell (Ed.), *Trusted Computing* (Vol. 6, pp. 1-10). London, UK: The Institution of Engineering and Technology (IET).

Thus, Trusted Systems are systems that can be relied upon to perform certain security policies in an expected manner and in the sense of behavioral consistency: TC “refers to a computer system for which an entity has some level of assurance that (part or all of) the computer system is behaving as expected”⁶¹ for a particular purpose. The outcome ultimately would be to allow the user to ‘blindly trust’ his computer again, without a constant need for self-monitoring. The TCG project is pursuing to allow the computer user to trust his own computer and for “others” to trust that specific computer.⁶²

This very specific conception of trust is not the same as the sociological concept,⁶³ even though they share some characteristics. We will get back to this analysis below, but first we try to give an explanation of how TC tries to build complex dynamic trust networks “bottom up”,⁶⁴ without central, let alone state, oversight or control.

A very concise account of how Trusted Systems give rise to trust networks was recently given by Rosinger and Beer within the project “Smart Nord”, which aims at providing a multi-agent infrastructure for the electric grid of the future. In this complex market, the relevant actors (electricity consumers, producers, storage facilities etc) are represented by autonomous software agents.⁶⁵ These

⁶¹ Mitchell, C. J. (2008). What is Trusted Computing? In C. J. Mitchell (Ed.), *Trusted Computing* (Vol. 6, pp. 1-10). London, UK: The Institution of Engineering and Technology (IET).

⁶² Lipson, H. F. (2002). Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. In C. M. University (Ed.), *CERT Coordination Center, Special Report CMU/SEI-2002-SR-009*.

⁶³ E.g. Fukuyama, F. (1995). *Trust: The Social Virtues and The Creation of Prosperity* (1st ed.). New York: Simon & Schuster Free Press Paperbacks book. that evoke concepts of “social capital”.

⁶⁴ Using base elements to build up a larger system.

⁶⁵ Rosinger, C., Uslar, M., & Sauer, J. (2013). *Threat Scenarios to evaluate Trustworthiness of Multi-agents in the Energy Data Management*. Paper presented at the EnviroInfo (pp. 258-264),

agents coordinate their activities and thus can give rise to self-organizing alliances and conglomerates.

In the process of forming coalitions, several factors need to be taken into account by the software to decide “whom to talk to”. One of them is the decision if another agent or machine can be trusted. The very same mechanism that will enable “benevolent” agents of consumers to build a coalition that then negotiates a bulk discount with a supplier can also be used to form a Denial of Service attack against that very supplier if the agents are malevolent or infected. A model of “trust” then becomes central for the attempt to ensure network security – TC as a security service.

In everyday life, we often base similar decisions on the reputation of the people we interact with – has the person whom we trust with our keys while on holiday a reputation for reliability and will remember watering the plants, or a reputation for dishonesty and will sell our silver?

Since in everyday language, reputation and trust are therefore often synonymous, here an attempt at a clarification for the purposes of “techno-trust”:

In computing, *reputation* describes the general “objective” understanding of an entity by a community. Within a reputation system, every entity is assigned a unique reputation value, which leads to a centralized approach.

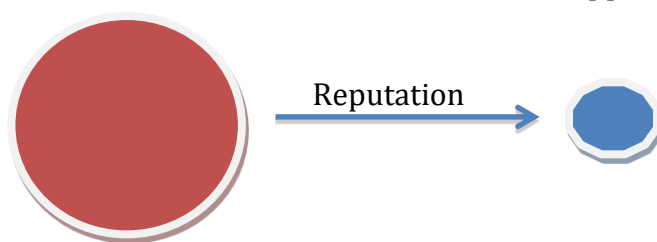


Figure 1: Reputation representation

In the technology-oriented definitions above, *trust* was implicitly understood differently. Trust describes the local and subjective opinion of an entity about the behavior of another entity, in particular, as we have seen, if it can be predicted by that entity. For trust formation, we can then crucially distinguish between

direct and indirect trust, making the “trust relation” transitive. This is a highly problematic assumption to make, both for sociological and technological conceptions of trust.⁶⁶ In this type of trust network, every entity has a unique “trust value” or “opinion” about every other entity, which corresponds to a decentralized, dynamic and potentially chaotic network approach.

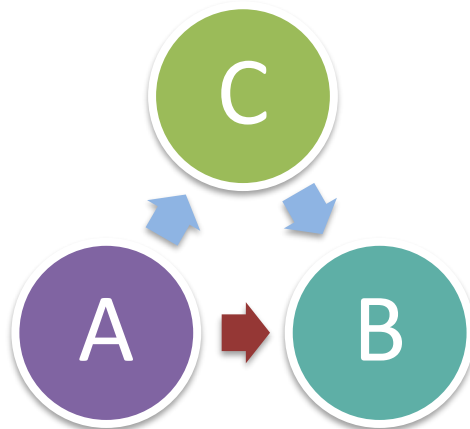


Figure 2: Direct (blue arrows) and Indirect (red arrows) trust

Here the red arrow symbolizes indirect trust, the blue arrows direct trust. If we accept that it takes a network to control a network, this decentralized model is much better suited for controlling security on the Internet, for the reasons Guadamuz noted.⁶⁷ A centralized reputation model by contrast corresponds to a traditional perception of the state as “top down” guarantor of security – the reputation is determined by the central control agency (in analogy one can think of the criminal records bureau). All TC systems, independent of the specific

⁶⁶ In the field of cryptography and in particular PGP that relies on transitive trust networks, the influential study by Christianson, B., & Harbison, W. (1997). Why isn't trust transitive? In M. Lomas (Ed.), *Security Protocols* (Vol. 1189, pp. 171-176): Springer Berlin Heidelberg. analysed just how problematic that assumption can be. For a discussion of the technical implications, with some references to social reality, see Liu, G., Wang, Y., & Orgun, M. A. (2011). *Trust Transitivity in Complex Social Networks*. Paper presented at the AAAI (pp. 1222-1229), AAAI Press.

⁶⁷ Guadamuz, A. (2011). *Networks, Complexity and Internet Regulation: Scale-free Law*: Edward Elgar Pub.

technological implementation, try as much as possible to emulate the decentralized Trust model.

In the above definition, two aspects are crucial: TC, in the software sense, is importantly a form of “blind trust” – the user doesn’t make a personal decision any longer, but relies on his computer to identify other machines as trustworthy, and tell them about its own trustworthiness in return. Second, this trust in the machine is to a degree enforced, and not volitional. To this extend, Lipson’s definition that says that we are “allowed” to trust our machines again is potentially misleading. Rather, we *have to* trust our machines. To the extent that this approach requires trust in the sociological sense, it is the relation between the user and the TCG. The user (buyer of a product) has to trust the vendor/manufacture that the TC system works as advertised, as she cannot override it any longer (because TC enforces blind trust). So TC regulates/enforces “techno-trust”⁶⁸ between the owner and her computer on the one hand, and also techno-trust between the computer and any machine it communicates with on the other. Social trust by contrast is required between the buyer and the TCG that certifies that the product is “trusted” for TC purposes.

Here we encounter a first idea why the specific approach to trusted computing promoted by the TCG may be insufficient, in the absence of positively enabling legislative interference. The disappointing uptake of TC that Proudler et al. identified when he wrote that introducing TC was like “a tug boat to change the course of a supertanker”⁶⁹ indicates for us that this social trust was lacking – the market voted with its feet against something that was perceived as a power grab under the pretense of enhanced security. Tellingly and significantly,

⁶⁸ “techno trust” will be used in the thesis as a shorthand for “trust as understood by computer scientists” whenever the context might make it unclear if “sociological trust” could also be meant.

⁶⁹ Proudler, G., Chen, L., & Dalton, C. (2014). *Futures for Trusted Computing Trusted Computing Platforms* (pp. 21-36): Springer International Publishing. p.2.

Proudlar et al.'s own analysis is different. In their view, reluctant users of TC either did not understand the technology well enough and were misinformed by malicious or ignorant detractors; or understood the technological limitations only too well and waited out for even more mature solutions.⁷⁰ In either case, the solution is essentially one of technology: communicate its features better, or improve it to the required standard. The main thrust of this thesis is that this analysis falls short. It doesn't understand that at least a certain degree of social trust, rather than techno-trust, is still needed if we want complex and dynamic security networks to self-organise, which as Guadamuz indicates is the necessary condition for efficient Internet regulation.⁷¹ TC requires a shift of power to the TCG (or similar organisations). Such a shift in turn requires trust, which can never get fully derived from techno-trust alone, but requires also a modicum of social trust.

For numerous reasons, some indicated above, the TCG never had the social capital on which social trust is based to supplement this foundation. As discussed above, is a cartel, and initially a rather exclusive one. It started as a group of industries heavy hitters, some of which with a notoriously bad public reputation as purveyors of inferior products and bully behavior, deservedly or undeservedly.⁷² Some of them faced lawsuits for abuse of market dominant

⁷⁰ see also e.g. Biddle from Microsoft: "We believe our biggest challenge is educating people about the facts of what we are doing. There are many misconceptions about NGSCB, so we are engaging many stakeholders in a collaborative dialogue." Cited in Vaughan-Nichols J. S. (2003). How Trustworthy is Trusted Computing? *IEEE Computer Society Press*, 36 (3), pp. 18-20. at p.18.

⁷¹ Guadamuz, A. (2011). *Networks, Complexity and Internet Regulation: Scale-free Law*: Edward Elgar Pub.

⁷² for a balanced analysis from the perspective of PR management, see e.g. Chapman, M. R. R. (2006). *In Search of Stupidity: Over Twenty Years of High Tech Marketing Disasters*: Apress., especially chapter 2, "Ripping PR Yarns: Microsoft and Netscape."

positions, especially in the EU,⁷³ reinforcing the perception that they are willing to use their near-monopoly position to force products and solutions on unwilling users. One of the “victims” of a TC revolution could be “amateur” or other open source developers, who cannot afford the TCG accreditation, resulting in a traditional narrative which pitted the romantic heroes of the computing age as David against the Goliath of heartless multinational predators.⁷⁴ As indicated above, TC grew out of DRM technologies, another techno-fix for Internet regulation with an exceedingly bad reputation.⁷⁵ TC retains the ability to enforce copyright, and some of the consortium members are right holders, undermining any attempt to publicly disassociate TC from DRM.⁷⁶ Technological solutions that increase user choice while maintaining the security benefits exist, but they were developed at a stage when the reputation damage had already occurred.⁷⁷

⁷³ Economides, N. (2001). The Microsoft Antitrust Case. *Journal of Industry, Competition and Trade*, 1(1), pp. 7-39. doi: 10.1023/A:1011517724873, Hazlett, T. W. (1999). Microsoft's Internet Exploration: Predatory or Competitive. *Cornell JL & Pub. Pol'y*, 9, pp. 29-60. , Wright, J. D. (2011). Does Antitrust Enforcement in High Tech Markets Benefit Consumers? Stock Price Evidence from FTC v. Intel. *Review of Industrial Organization*, 38(4), pp. 387-404. doi: 10.1007/s11151-011-9297-5. For a general analysis of some of the issues at stake see MacKie-Mason, J. K., & Netz, J. S. (2006). Manipulating interface standards as an anti-competitive strategy. *Standards and public policy*, pp. 231-259.

⁷⁴ Vaughan-Nichols J. S. (2003). How Trustworthy is Trusted Computing? *IEEE Computer Society Press*, 36 (3), pp. 18-20. Citing Richard Stallman as saying that one reason he opposes TC is that it may threaten open source operating systems and applications by viewing them as nonstandard and untrustworthy and thus not letting them run.

⁷⁵ See authoritatively, May, C. (2007). *Digital rights management: The problem of expanding ownership rights*: Elsevier.; for a detailed study of issues related to TC, see also Mulligan, D. K., Han, J., & Burstein, A. J. (2003). *How DRM-based content delivery systems disrupt expectations of personal use*. Paper presented at the Proceedings of the 3rd ACM workshop on Digital rights management (pp. 77-89),ACM.

⁷⁶ Vaughan-Nichols op cit p. 19

⁷⁷ For one such technological solution, see e.g. Cooper, A., & Martin, A. (2006). *Towards an open, trusted digital rights management platform*. Paper presented at the

If social capital is lacking to marshal social trust, why should buyers accept the TCG business proposition? This finally brings in law, as an additional factor. As we will discuss in more detail below, Max Weber famously suggested that in modern, individualistic, pluralistic and market driven societies, personal trust between individuals can or has to be replaced by trust in institutions, most importantly in the law.⁷⁸ In the type of society he described, people were not any longer able to base e.g. investment decisions on personal knowledge, bond of loyalty and other emotional relations between borrower and lender, of the type that dominated small-scale rural economies where everybody knew everybody else, and non-repayment would face swift social ostracism. Rather, people learned to trust in laws, and the bureaucracies that enforced them. I can lend you money even if I don't know you, personally, and have no reason to trust you, because a judge (whom I also don't know personally) will if necessary order some other public officials to enforce my claim against you. This requires trust in systems of law and administration, rather than people (or companies). In the case of a security initiative such as TC that is driven by the private sector, this gives a prominent role in particular to contract law. However, as we will see this creates a dilemma, as the very conceptual foundations of contract law, at least classical liberal contract law, are ill suited for underpinning and sustaining complex dynamic networks.

Nonetheless, the relative failure of TC does give a salutary lesson to the wider sociological debate. In recent decades, market and indeed network based models of governance have been postulate as the replacement of legal-bureaucratic

Proceedings of the ACM workshop on Digital rights management, Alexandria, Virginia, USA. Another solution which maintains the DRM element, but tries to mitigate its "overreach" and enhance as a result its public reputation is Erickson, J. S. (2003). Fair use, DRM, and Trusted Computing. *Communications of the ACM*, 46(4), pp. 34-39.

⁷⁸ Misztal, B. (2013). Trust in modern societies: The search for the bases of social order: John Wiley & Sons. p. 69ff

modes of organization. The end of the nation state with its clear hierarchies and expanding bureaucracy was seen as the problem, market and network driven solutions the answer. We lose trust in governments, but trust our Facebook friends, organized and home delivered courtesy of Facebook Inc. However, even our initial short discussion of TC shows that Johan Olsen was making an invaluable insight when he recently argued from a neo-Weberian perspective that legal rationality and bureaucracy should not be seen as a defunct alternative to markets and networks, but an overlapping and enabling mode of organization:

“[this article] questions the fashionable ideas that bureaucratic organization is an obsolescent, undesirable, and non-viable form of administration and that there is an inevitable and irreversible paradigmatic shift towards market- or network-organization. In contrast, the paper argues that contemporary democracies are involved in another round in a perennial debate and ideological struggle over what are desirable forms of administration and government: that is, a struggle over institutional identities and institutional balances. The argument is not that bureaucratic organization is a panacea and the answer to all challenges of public administration. Rather, bureaucratic organization is part of a repertoire of overlapping, supplementary, and competing forms coexisting in contemporary democracies, and so are market-organization and network-organization. Rediscovering Weber's analysis of bureaucratic organization, then, enriches our understanding of public administration.”⁷⁹

TCG, so we argue here, got “the balance wrong” when relying exclusively on market and network driven solutions, with scant regards of the institutional-legal framework. Or rather, the desired network effect failed to materialize also because the market, in the absence of both a credible institutional-legal framework and a pre-existing social trust rejected the model. What is needed

⁷⁹ Olsen, J. P. (2006). Maybe It Is Time to Rediscover Bureaucracy. *Journal of Public Administration Research and Theory*, 16(1), pp. 1-24. doi: 10.1093/jopart/mui027

then is in Meuleman's words a "metagovernance" for networks and markets,⁸⁰ an enabling regulatory framework that helps to plug the conceptual gaps between the societal and the technological conception of trust. The third and fourth parts of this thesis will identify two of the "choke points" that such a meta-governance will need to address.

So far, we have focused as a preliminary conceptual clarification on the differences in the way in which computer scientists, psychologists and sociologists understand the term "trust". On some level, this should not be surprising. Different disciplines develop their own theoretical vocabulary, and as long as everybody knows which definition is operative in a given context, efficient communication is possible.

However, the argument here is somewhat more involved. The claim is that the mismatch between "techno-trust" and social conceptions of trust is a problem for the TCI (Trusted Computing Initiative). The TCI needs, for its product to be successful, social trust. The techno-trust that it delivers instead, falls short of what is needed, and in doing so creates two separate but causally connected issues for law and regulation. First, it causes potentially legal problems for users and wider society, problems that the law may need to rectify. Second, to achieve its aims it needs a more sympathetic regulatory framework that gives consumers better reasons to invest in TC. The two issues are connected: As long as potential users feel that TC exposes them to technical risks without legal redress, or legal risks without giving them the control to mitigate these risks, they will refrain from investing into the TCI model.

The dual challenge that TC poses for law, needs further explanation. We noted above that "trusted" in the computer sense only partially matches the

⁸⁰ Meuleman, L. (2008). Public management and the metagovernance of hierarchies, networks and markets: the feasibility of designing and managing governance style combinations: Springer Science & Business Media.

concept of “trustworthiness” as understood in social life: “trusted” is what the technology gives us, “trustworthy” is what we want.

This raises an immediate legal problem in an environment that relies on contracts as the legal form of social connectedness – that is to say the way customers and TC providers relate with each other on the open market is not by bonds of kinship, shared ideology or tribal solidarity, but through contracts formed freely and through mutual consent. But if a product is sold as “trusted computing” to laypeople, it seems an obvious danger that they will misread it as “trustworthy”. As we discussed above, this might expose them to risk, misreading the level of protection that they are buying. If this is the case, does their expectation merit protection through the law, was it “reasonable”?

This is a classical contract law question, and we will return to it later in Chapter 4. Hidden underneath however is a much more fundamental issue: can *any* classical, liberal contract law provide the type of relation that is needed for TC to create the networks of security and trust that they intent? In the classical concept of contract law, “privity of contract” implies that contracts are between two parties and two parties only.⁸¹ They are crucially lacking the transitivity that extends a binary relation to third parties – but this is crucial for models of trust as we have seen above. The atomism of contract law that flows from the principle of privity, is in theory inimical to this type of network effect. This was analyzed masterfully by Lewis and Weigert who contrast the Hobbesian “social contract” model as a quintessentially atomistic vision of society with the “holistic” model that is based on trust:

“Trust functions as a deep assumption underwriting social order and is not reducible to individual characteristics. Changes in trust alter

⁸¹ For a classical exposition see Lilienthal, J. W. (1887). Privity of Contract. *Harvard law review*, 1(5), pp. 226-232. doi: 10.2307/1321337; for a more recent discussion of the problems of this concept see e.g. Adams, J. N., & Brownsword, R. (1993). Privity of Contract. That Pestilential Nuisance. *The Modern Law Review*, 56(5), pp. 722-732. doi: 10.2307/1096875.

social relationships. The study of power, exchange, family, and politics illustrates how trust constitutes social reality as emergent and holistic.”⁸²

By framing (with necessity) their relation with their customers as one governed by classical contracts, TCI from the beginning counteracts the very network effects its product aims to create. It reduces trust to binary, non-transitive relations that cannot in principle form the basis of a complex and dynamic system. They can't be complex, because they are lacking transitivity and with that holistic network effects, and they can't be dynamic because classical contract law focuses exclusively on the “magic point in time” when the contract is concluded through the meeting of the minds. Once the contract is concluded, it remains static, a historical event that lacks the flexibility to adopt dynamically as the network grows. This brings back the more empirical point we made above. TCI, so we argued, lacked the social capital, the public trust; that they would have needed to make their approach a success. But it also goes in radical way beyond the TCI, and affects all attempts to generate social trust through techno-trust. Even if the TCI had been run by the Creative Commons movement and been chaired by Mother Theresa (or even Linus Torvalds himself) and mustered the necessary social capital so that people trust the product, this would still have meant a personal relation between TC provider and individual customers only, not, as is needed, an ensuing trust between customers. Or, as again Lewis and Weigert put it:

“This “social trust” helps us understand the formation of interpersonal relationships, the difference between economic and social exchange, and the discrepancy between attitudes toward society and toward particular institutional actors.”⁸³

⁸² Lewis, J. D., & Weigert, A. J. (1985). SOCIAL ATOMISM, HOLISM, AND TRUST. *Sociological Quarterly*, 26(4), pp. 455-471. doi: 10.1111/j.1533-8525.1985.tb00238.x at 455.

⁸³ *ibid.*, p. 455.

It is not, therefore, just the trust relation towards a particular institutional actor, here the TCI, that is the issue. Rather, holistic trust, and that is trust in the form of a network where everybody is ultimately connected with, and trusting in, everybody else is at stake. Economic exchange relations (“buying the TC product”) and the (contract) law that governs it cannot in principle achieve this, there will always be, so Lewis and Weigert, a “discrepancy” between the two.

Where we depart however, from their analysis, is in our instance that there is an important and indeed constitutive role to play for law. This is the neo-Weberian aspect we mentioned above. Formal rationality and “trust in institutions” is not sufficient, it needs also a “thick” substratum of pre-existing trust, even in modern, particularized and pluralistic societies. However, in this type of society, trust will never be all-encompassing enough to work entirely without a legal system to reinforce it. We therefore still need the law but the right type of law, one that does not dissect holistic relations and reduces them to binary ones, but one that “follows” and even “enhances” transitive and dynamic network foundations. On the level of specific legal instruments, we will argue that “reliance liability” is exactly the type of private law concept that can turn intransitive contract relations into transitive, network-supporting ones. On the level of legal theory, “relational contract theory” has opened up a way to think about contract relations that is not any longer a one-off, static and atomistic relation.⁸⁴

⁸⁴ For an introduction to relational contract theory, see Gudel, P. J. (1998). Relational Contract Theory and the Concept of Exchange [comments] (pp. 763). For a comprehensive discussion that focuses on the economic exchange relation and its role in sociology discussed here see in particular Macneil, I. R. (1987). Relational Contract Theory as Sociology: A Reply to Professors Lindenberg and de Vos. *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft*(2), pp. 272-290. An important critical voice to which we will have to return is Fox Jr, J. W. (2003). RELATIONAL CONTRACT THEORY AND DEMOCRATIC CITIZENSHIP. *Case Western Reserve Law Review*, 54(1), pp. 1-67.

In the remainder of this chapter however, we will continue to lay the foundations for this analysis, by attempting a “parallel reading” between the technical aspects of TC and the sociological reflection on the interaction between trust and law.

To recap, we identified in the introduction the problem of network complexity as the “hard challenge” for Internet regulation. If social trust relations in complex modern societies also organize themselves in dynamic complex networks, **and** if in addition, security “travels along” the trust pathways (the edges) in this network - because we only trust those whom we can securely trust, those who are “trustworthy” - the result would be an environment with ubiquitous security, which is the ultimate aim of the TCI. In this world, security is not imposed top-down through central fiat, but is itself an emergent network property which, as we understand by Guadamuz, is likely to be the only efficient way to “tame” complex dynamic systems.

As we argued, this however raises several problems. The first two relate to the antecedent of the above claim, and raise issues of sociology:

- a) are social trust networks self-organizing, complex dynamic systems?
- b) does “security” in these systems follow trust?
- c) If we can answer these two questions in the affirmative, the next question addresses the relation between the two conceptions of trust:
- d) are the network effects that Trusted Computing aims to create, despite the different conception of trust, isomorphic to the trust networks we find in society?

If the answer to this question is yes as well, then we would have good reasons to believe that TC-type solutions can indeed result in ubiquitous security as an emergent feature of the communication network (at least if they come from a provider who is in turn both trustworthy and trusted). However, we have reasons to doubt all three of these premises, at least to a degree. This, in our view, is where *law* as a mode of regulation comes into the picture and plays a crucial role.

Trusted Computing is associated to two of the four modes of the square of regulation proposed by Larry Lessig.⁸⁵

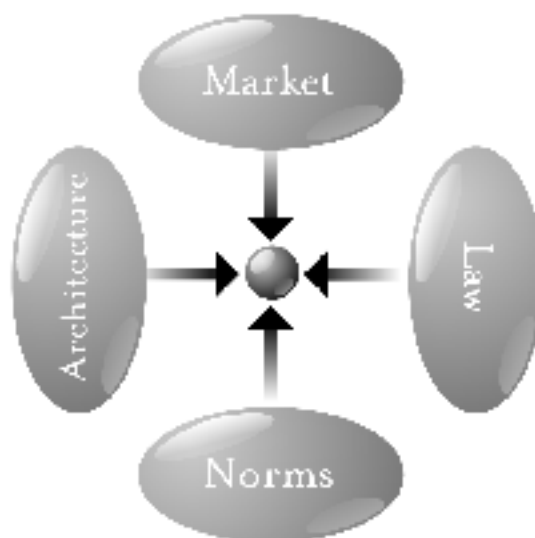


Figure 3: Square of regulation proposed by Larry Lessig

It is, first and foremost, a paradigmatic form of regulation through Code. The software architecture itself will tell you (or rather, your computer) what you can and cannot do and to which other machines you can or cannot speak to. However, at the same time it is also a form of regulation through markets – or at least depends on market rationality supplementing it. The relative lack of success of the TCG was less a result of technological problems, more a lack of market enthusiasm and uptake. As discussed above, the underlying idea of the TCI here was to compete initially with non-TC products on a mix of security and costs: more secure than its competitors, but not as much more expensive, than a secret solution of the type developed for the military and critical infrastructure. Since this compromise, so the TCI, has a rational balance between costs and benefits at least for some actors, a rational market should take up TC for some applications – those that are not so critical that they require more than TC, but not so trivial

⁸⁵ Lessig, L. (1999). *Code and other laws of cyberspace*: Basic books. esp. p.123; Marsden, C. T. (2000). *Regulating the global information society*: Psychology Press. p.19.

the additional costs of TC are prohibitive. Only when the market uptake reached a certain threshold would the network effect inherent in the technological model take over and push non-TC products out, resulting in ubiquitous security. Even the “trivial” applications, machines or products that do not merit on their own investment in TC need to be able to communicate with the more safety critical ones. But TC only allows trusted machines to communicate. This will eventually force all applications to be at least TC compliant, or risk to get isolated in some small “high risk” pockets.

We argue that part of the problem with TC and the TCG is that their technological conception of trust is on its own insufficient to develop the complex dynamic networks that the more substantial sociological concept of trust entail. What is needed in addition is an ecosystem of legal norms that supplement TC. Using ideas going back at the very least to Max Weber and his analysis of the role of formal law in modern, market driven societies, we will show that the TC network will only work when in addition to security and techno-trust, also legally enabled social trust “runs along” the edges that connect the nodes of the network. That is, if for any two connected nodes in the TC network, the parties can trust each other in the computer science sense described above, AND have as a fallback a shared trust in institutions that can apply legal sanctions; we will get dynamic complex networks that are isomorphic to the communication network of the Internet. However, as we will see, there are systematic problems with the very concept of law that makes this a difficult proposition to achieve.

2.6 Technical Analysis of Trusted Computing technology

2.6.1 How the Trusted Platform works

In this section, we look in more detail at some technical aspects of Trusted Computing as exposed by the TCG that will inform our discussion later on. At the same time, we will provide a “running commentary” on the relation between the

technological and sociological conceptions of trust, analyze the degree in which they match, and indicate legal implications. Trusted platforms provide a technological implementation and interpretation of the factors that must be simultaneously true in order to achieve “trust” and are defined by the TCG:⁸⁶

“Unambiguous Identity - In the words of the TCG:

In order for something to be able to be trustable it must be unambiguously identifiable, thus every component of a Trusted Platform must be known and identifiable. In the case of a software component, a hash of that software file provides a very useful and practical means to identify that component.”

The emphasis on unique identities as a source of trust illustrates several important issues and highlights some of the conceptual problems that bedevil the TCI approach to trust. Indeed, the sociological concept of trust could be argued to arise in situations where unique identifiers are the least relevant criterion. Often, I will trust a person not as an individual, but as a member or representative of a specific group. Theories of the evolution of cooperation for instance have postulated that we can understand the emergence of religion as a means to establish trust in situations where there is no previous personal relations, no “identification” in this sense, and no past experiences that could form the basis of trust.⁸⁷ Remember in the discussion above, we suggested that “trust” for TCI is ultimately a Popperian, “past experience” based approach. I trust a person because I can (re)identify him as the agent of past, benevolent behavior – he carries a good reputation. This indeed makes the ability for re-identification essential. However, this already presupposes a considerable degree of closeness. He must trust me enough, and I must trust him enough, to be allowed close up to observe his actions. (We note in passing that the privacy concerns that have been

⁸⁶ TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.).

⁸⁷ so e.g. Atran, S. (2002). *In gods we trust : the evolutionary landscape of religion*: Oxford ; New York : Oxford University Press, 2002.

raised about Trusted Computing have in part their root in this need to share information about past behavior that can be traced back via unique identifiers to an agent).⁸⁸

However, in an Internet context, why should I allow even this level of disclosure about me to third parties, who I do not know personally, who can be in a different jurisdiction and for all I know can be a dog? Early societies, before the modern administrative state and the rule by formal laws, faced the same dilemma. Trust was a given to the small number of family members who knew each other intimately. But as soon as a stranger approached, problems began. How can he be trusted, when we do not know him, have no way to identify him and also can't risk to have him close enough for an extended period of time to observe if he consistently behaves benevolently? According to some influential sociological theories, this is where a new form of trust emerged, born out of necessity. When it is impossible to identify the stranger as an individual, a method must be found to identify him at least as a member of a group that shares certain normative commitments. If I can identify the stranger therefore as a member of my religious group, then a "trusted third party" ensures mutual rule compliance - in this case of course an omniscient and highly punitive observer, who ensures that any gain one of us can make by cheating or injuring me, the other is outweighed by divine punishment.⁸⁹ Crucially for our topic, this new form of trust is not any longer a binary relation between just two people based on personal

⁸⁸ See e.g. Reid, J., Gonzalez Nieto, J., Dawson, E., Okamoto, E. (2003). *Privacy and Trusted Computing*. Paper presented at the Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03) (2003), Washington (pp. 383-388), IEEE. section IV.

⁸⁹ so Johnson, D. D., & Bering, J. M. (2006). Hand of God, mind of man: Punishment and cognition in the evolution of cooperation. *Evolutionary Psychology*, 4(1), pp. 219-233. On the relation between intra-group cooperation, trust and religion, see Sosis, R. (2000). Religion and Intragroup Cooperation: Preliminary Results of a Comparative Analysis of Utopian Communities. *Cross-Cultural Research*, 34(1), pp. 70-87. doi: 10.1177/106939710003400105.

acquaintance or prior observation, but forms a holistic network. The neophyte whom I recruit to the religion acquires instantaneously trust, and with that cooperation, from all other members of the group, since the “recruitment” relation is transitive.⁹⁰ Since group membership earns cooperation and trust from all other group members, there is an obvious danger that a free rider will try to fake membership. Trusted computing, unsurprisingly, faces the same problem:

“Therefore, attacks that result in the compromise of the endorsement secret key (or any other key) should be expected to occur frequently, when trusted platforms are used, for example, in high value transactions or DRM applications. Recovery of this key allows attackers to create a virtual trusted platform that is entirely under their control. Publication of a valid endorsement key pair would allow widespread impersonation of the trusted platform, without the trust.

The TCPA specification acknowledges that “the trustworthiness of the architecture is vulnerable to the compromise of a single TPM endorsement private key”.⁹¹

Societies however found an ingenious solution to this problem, which at the same time also made unique identification of a person unnecessary. It was typically possible to deduce the relevant group membership of a stranger from what he wears (or not wears) and eats (or not eats). He demonstrates seriousness by forgoing certain benefits, e.g. by refraining from eating types of food (pigs, cows etc.) despite scarcity, so giving a “costly signal” that he is not a free rider.⁹²

⁹⁰ This is of course also the model of Pretty Good Privacy – more on which below.

⁹¹ Reid, J., Gonzalez Nieto, J., Dawson, E., Okamoto, E. (2003). *Privacy and Trusted Computing*. Paper presented at the Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03) (2003), Washington (pp. 383-388), IEEE. section 3.2.

⁹² see e.g. Henrich, J. The evolution of costly displays, cooperation and religion. *Evolution and Human Behavior*, 30(4), pp. 244-260. doi: 10.1016/j.evolhumbehav.2009.03.005, Watanabe, J. M., & Smuts, B. B. (1999). Explaining Religion without Explaining it Away: Trust, Truth, and the Evolution of Cooperation in Roy A. Rappaport's "The Obvious Aspects of Ritual". *American Anthropologist*, 101(1), pp. 98-112. doi: 10.2307/683344.

These “taboos” then become internalized and form the substratum of holistic, society wide trust. TC, by contrast, has no method to re-create this costly signaling. Rather, it follows the solution that the modern nation state adopted as an *alternative* approach to the same challenge. The modern, centralized nation state became a competitor for trust relations build on blood ties, religious or other “tribal” affiliation. In that environment, state issuing of Identity cards that give each citizen a unique identifier (e.g. the national security number) became necessary. The role of the citizen, her entitlements and status, is now fully determined by formal laws – Max Weber’s modern bureaucratic model of governance. In that environment, being able to identify myself as myself is sufficient and necessary to trigger a broad range of legal consequences and reactions. The need for personal trust diminishes proportionally – I trust the ID issuing authority, my relation to the person is thus identified, my obligations and rights towards him follow suit.⁹³

It was only recently, with postmodernity becoming a major topic for sociology, that sociologists rediscovered the irreducible importance of personal trust relations. Trust became important precisely because formal rational law, top down bureaucracies and the understanding of personhood as one of “formal equality before the law” reached its limits.⁹⁴ “Identity politics” introduced a very different notion of identity, one where the individual is identified not through unique personal identifiers that are as a matter of regulation assigned to

⁹³ Caplan, J. (2001). “This or that particular person”: protocols of identification in nineteenth-century Europe. *Documenting individual identity: The development of state practices in the modern world*, 1, pp. 49-66.

⁹⁴ For an illustrative example see e.g. Bosniak, L. S. (1988). Exclusion and Membership: The Dual Identity of the Undocumented Worker Under United States Law. *Wis. L. Rev.*, pp. 955-1042. Illegal immigrants are an ideal test case for this system – they lack the right type of identification certificate, and hence become “invisible” in such a system. Personal or “thick” relations of trust do not matter for the way in which they communicate with the state or their employer.

everybody, but highly contextual properties that are used to negotiate group membership (“me” as a mother, a person of colour, a Christian/ Muslim/ Hindu). *Who* I am is less important than *what* I am – or, maybe crucially for this thesis, which networks I am a member of.

That sociology after the 1950s rediscovered trust as a major theme for study⁹⁵ which was partly caused by an increasing recognition that the Weberian model of the liberal state under the rule of law, was insufficient to account for the actually observed social dynamics: pre-modern modes of trust had never fully disappeared, but continued to underpin much of societal interaction. The idea that social exchanges require at least some non-contractual element can be traced back at least to Durkheim’s work in the 1880s and his analysis of the interaction between law and religion.⁹⁶ But it was the post-modern, heterogeneous societies that make this type of trust increasingly fragile, contested and problematic – rekindling in some of the foremost sociologists of this era such as Talcot Parson’s the interest in Durkheim’s work and the role of trust.⁹⁷ Parson thought that “trust” was an essential ingredient to guarantee social stability and order. He realized however that in pluralist societies, this was a potential problem – how could trust be maintained in a society of increasingly isolated and atomistic individuals who might feel allegiance to certain group interests, but not society as a whole? ⁹⁸ This

⁹⁵ In that sense, “trust” was advocated as an alternative to the Weberian model of modern capitalist society e.g. by Luhmann, N., Davis, H., Raffan, J., Rooney, K., & Luhmann, N. (1979). *Trust and Power : two works by Niklas Luhmann*: Chichester : Wiley, 1979.

⁹⁶ in particular in Durkheim, E. (2014). *The division of labor in society*: Simon and Schuster.

⁹⁷ See e.g. Parsons, T. (1967). Durkheim’s contribution to the theory of integration of social systems *Sociological theory and modern society* (pp. 3-34). New York: Free Press. On Talcott’s conception of trust see Misztal, B. (2013). *Trust in modern societies: The search for the bases of social order*: John Wiley & Sons., op cit chapter 3

⁹⁸ This is another aspect of the “hard” problem of trust for the Internet, which is discussed intensely in e-commerce literature. It is not possible to do justice to this

Janus face of trust as a network of intra-personal relations based on things other than nationality came to the fore with the civil rights movement and the “identity politics” that it foregrounded. Taking again religion as our example, the Westphalian peace accord had created homogeneous societies where the head of state determined the religious identity of the entire polis. But religious conflict below the level of the nation state continued, and some might argue, increased, in the modern state – see the example of Northern Ireland, or the Shia-Sunni violence in nation states in the Arabic world. A tool (religion) that has its evolutionary roots in fostering cooperation had increasingly become a hallmark for divisiveness and fragmentation. Liberal societies reacted to this by recognizing some of these groups also in law, e.g. in affirmative action programs. But for the rule of law and legal regulation, this poses a challenge, as this concept of trust seems to rely on a conception of identity that in turn is incompatible with the rule of law and the idea of formal equality.⁹⁹ This led to a second wave of sociological thinking about trust, one that did not take any longer its stabilizing role for granted. The most important contribution to this discussion was itself based on systems theory and the early cybernetics of Norbert Wiener, Niklas Luhmann’s system theoretical analysis of modern society.¹⁰⁰

discussion within the confines of this thesis, though we will revisit it briefly when we discuss reliance liability in chapter 4. There, we will look at trustmarks as the analogue for TC in an e-commerce setting. For the general debate on the generation of trust in e-commerce, the reader is referred to one of the most widely cited contributions, Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, 27(1), pp. 51-90.

⁹⁹ See on this Knight, J. (2001). Social norms and the rule of law: Fostering trust in a socially diverse society. *Trust in society*, 2, pp. 354-373.

¹⁰⁰ Most importantly: Luhmann, N., Davis, H., Raffan, J., Rooney, K., & Luhmann, N. (1979). *Trust and Power : two works by Niklas Luhmann*: Chichester : Wiley, 1979. For an application of his ideas in an internet context, see e.g. Gefen, D., & Straub, D. W. (2003). Managing user trust in B2C e-services. *E-service Journal*, 2(2), pp. 7-24. and McKnight, D. H., & Chervany, N. L. (2001). What Trust Means in E-Commerce

With Luhmann, we encounter a sociological thinker who is probably most attuned to frame the issues we encountered in terms of complexity and networks. For Guadamuz, Luhmann's concept of autopoietic law shows how we can think of regulation in ways other than top-down, "command and control" regulation:

"It is easy to see how the concept of autopoiesis is useful from a regulatory perspective, as it helps to explain how regulatory processes emerge, evolve and act as self-organising agents in society. Autopoietic regulation could be seen as an internal ordering force; organic, dynamic, and self-organising. This would contrast a more structured and hierarchical view of regulation known as "command and control" regulation, where governmental bodies serve as the organising force exerting control in a top-down manner."¹⁰¹

While appreciating Luhmann's contribution, he urges nonetheless caution:

"Having said this, it is essential to note that there appears to be a clear split between the understanding of autopoiesis in legal systems and the concepts of self-organisation and emergence studied in the previous chapter. While Luhmann repeatedly uses examples from biology to describe autopoiesis, and his concept of self-organisation matches that used in the physical sciences, it is clear that autopoiesis is very much a social theory. With few exceptions, the theoretical study of autopoiesis is devoid of the mathematical treatment and the wealth of evidence into self-organisation involving information theory, phase transitions and emergence described in Chapter 2. It is almost as if the social sciences and the physical sciences arrived at the same conclusion following entirely different paths."¹⁰²

We cannot here attempt the cross pollination that he calls in as a desiderata. For our purpose, what is important is the role that Luhmann assigned to trust in the constitution of social systems and the autopoietic emergence of order:

Customer Relationships: An Interdisciplinary Conceptual Typology. *International journal of Electronic Commerce*, 6(2), pp. 35-59.

¹⁰¹ Guadamuz, A. (2011). Networks, Complexity and Internet Regulation: Scale-free Law: Edward Elgar Pub. p. 55.

¹⁰² Guadamuz, A. (2013). Networks, complexity and internet regulation scale-free law: The University of Edinburgh.

“Trust, by the reduction of complexity, discloses possibilities for action which would have remained unattractive and improbable without trust - which would not, in other words, have been pursued.”¹⁰³

Trust is one of the ways complexity is reduced. Reduction of complexity, by distinguishing an “inside” from an “outside”, is in Luhmann’s sociology the main function of systems. We have seen how trust can reduce complexity above – when encountering a stranger, instead of dealing with the infinitely many possibilities that his “identity” presents, I can reduce the complexity of my decision making process on whether to cooperate with him by seeing him as a mere representative of a group – a group that is either “inside” my own system or “outside” it (in which latter case, I stop caring). The moment I bring in this way “the outside in”¹⁰⁴ and relabel the stranger as a component of my system, I have also reproduced that system – one of the key functions of systems being their constant. With other words, communication within a system selects a limited amount of all information from the outside that is available in theory. The stranger has a specific height, size, eye colour, manner etc. None of these infinitely many attributes matter, only those that have a specific “meaning” (in German, *Sinn*) – here those attributes that identify him as member of my religious group. This way the distinctive identity of each system is constantly reproduced in its communication, by distinguishing between what is and what is not considered meaningful. This is what Luhmann calls auto-poiesis, literally, self-creation, reproduction from elements previously filtered from an over-complex environment. Identity then, is not a condition for trust as it is in Trusted Computing. Rather, the converse is true: trust creates identity by allowing

¹⁰³ Luhmann, N., Davis, H., Raffan, J., Rooney, K., & Luhmann, N. (1979). *Trust and Power : two works by Niklas Luhmann*: Chichester : Wiley, 1979. p. 25.

¹⁰⁴ Bańkowski, Z. (2007). Bringing the outside in: the ethical life of legal institutions *Law and legal Cultures in the 21st Century: Unity and Diversity (Wolters Kluwer Polska, 2007)* (pp. 193-217).

systems to selectively ascribe meaning to the information that it acquires from its environment.

Against this background, the focus of TC on unique and “official” modes of identification reads like a throwback into times where trust, as understood in sociology, was precisely not what was needed to ensure security. It bears the marks of top down, bureaucratic regulation, not bottom up network centric emergence through self-assembling network interactions. When it talks about trust, it means in fact something more akin to reputation, and as we discussed above, reputation systems do not form natural networks. In the context of the Internet, we can see this also by contrasting “Trusted Computing” with an approach that matches much more closely the transitive trust relation described above. There we used as an example how a trusted member of a group can “bring in” strangers by trusting them – proselyting in the pre-modern society. In the Internet society, we find the very same model in the Web of Trust that underpins Pretty Good Privacy. As Zimmerman put it:

“As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.”¹⁰⁵

This is the direct digital equivalent of joining a religion through e.g. a baptism by a trusted member of that religion, or joining an exclusive club on the recommendation of a member. Trust travels in this model along the nodes of the network, creating a “web of trust”.

We face with other words a conceptual paradox: to build (what it perceives as) trust, TC relies on a concept that is in sociological terms seen as a

¹⁰⁵ Zimmermann, P. R. (1995). *The official PGP user's guide*: MIT Press.

diametrically opposed mode of regulation. While the Web of Trust has been described as a network centric approach that *beat* governments and their traditional mode of regulation,¹⁰⁶ the TCI reproduces traditional modes of governance, just with a private sector conglomerate taking the role of the executive. This is not just an abstract philosophical speculation. It helps us to understand better the legal and regulatory issues that TC creates, and also its relative failure. If TC is despite its name more similar to traditional forms of regulation than network centric, self-organizing regulation, then the legal system needs to take account of this – reproducing e.g. the constraints under which governments operate. This will be a key theme of chapter 3, where we will indeed argue that TC is best understood as privatization of centralized government functions, not a decentralized, emergent network governed by free contractual association only.

Unhindered operations: The next core concept of TC is that of “unhindered operation”, which we encountered already above when discussing the techno concept of trust. According to the TCI, something can be trusted:

“if it behaves in an expected manner for a particular purpose. A component of a Trusted Platform has been designed to perform a particular task and follow a designed behavior. That component must be able to operate without interference from other components or processes within the platform. In order for a given component to even begin to operate, it must not be (allowed to be) subjected to tampering within the platform.”¹⁰⁷

We discussed the “Popperian” element of trust above. With its epistemological counterpart, it shares the problem that the more complex a system is, the more interlocking parts it has, the more chaotic and unpredictable it can become. The idea behind this concept is seemingly simple and based on the

¹⁰⁶ Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age*: Penguin.

¹⁰⁷ TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.). section 2.2 pg. 9.

lessons learned with popular computer systems such as Windows. A typical security problem for Windows was Privilege Escalation.¹⁰⁸ Privilege Escalation essentially means that a computer is only as secure as its weakest link. Once a bug or configuration oversight in one component was identified and the component taken over by an adversary (say a flaw in the media player application), it was often possible to gain elevated access to resources that are normally protected from an application or user and thus control the entire machine. TC addresses this issue by preventing access to parts of the system that are not needed for the operation of another.

To use a societal analogy: I might be able to trust you, personally, on the basis of your past behavior. I might not trust in the same way the people you associate with in your social circle. If I now have reasons to worry that they will influence your behavior towards me, I cannot any longer predict if you will be benevolent or malevolent. To extend this analogy even further, I might trust you and your wife. But I also know that there are “hostiles” in the environment who might have kidnapped your wife to force you into malevolent behavior against me. This was the reality for computer security in the past: a hostile agency could get access to one component part such as a media player (the wife, in our analogy), through escalation of privilege gain access to the root of the entire computer and from there control all its component parts, eventually using it for a Denial of Service attack.

TC restores the ability to trust a computer by reducing this complex interaction – to be trusted, operations have to show that they are unhindered. In our analogy, you have to show first that your insalubrious contacts did not and could not affect the way you will fulfill your obligation towards me.

¹⁰⁸ See e.g. King, S. T., Tucek, J., Cozzie, A., Grier, C., Jiang, W., & Zhou, Y. (2008). Designing and Implementing Malicious Hardware. *LEET*, 8, pp. 1-8.

Above we argued that the TC understanding of trust does not lead to organic, self-organizing networks as it is not based on a transitive trust relation. Here TC goes a step further, and actively prevents (certain forms of) transitivity, preventing this way the spread of harm.

Attestation: We encountered the final core component of TC above. There, we argued that if we want to predict future good behavior, we need a way to certify past good behavior. In the words of the TCI:

“In order for something to be trusted, there must be some way of verifying consistent good behavior of that thing. That is, for a Trusted Platform to be trustworthy, there needs to be some means for that platform to report (to the external world) its integrity state (as a whole), which is a function of the integrity state of each component that make-up that Trusted Platform.”¹⁰⁹

TPs are optimized for the protections and processing of private or secret data. They have isolated execution environments, where software/data is protected from external interference and they can offer assurances about their behavior (hardware and software environment).¹¹⁰ The need to build attestation into a TC solution, immediately leads to one of the core legal issues of this thesis. If someone acts in reliance of such an attestation, and the attestation was unwarranted (as we discussed above, TC does not guarantee perfect security) is there any redress for the reliance placed on that attestation? Here, more than in the other two core ideas, legal and technological issues are not only closely linked, but structurally isomorphic. In the TC world, security should follow trust along the arcs of the network. Given the “imperfection by design” that the cost-benefit analysis of TC entails, does liability follow the same arcs, and if so, does it have

¹⁰⁹ TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.). Section 2.2, pg. 9.

¹¹⁰ Gallery, E. (2008). *Who are the TCG and what are the Trusted Computing concepts?* Paper presented at the TRUST2008, Villach, Austria. Presentation retrieved from <http://dblp.uni-trier.de/pers/hd/g/Gallery:Eimear>

the potential to enhance or even create the trust? Due to the centrality of the concept of attestation for this thesis, we will now look into it in more detail.

2.6.2 Direct Anonymous Attestation Protocol

The core of the TCI hardware is the protocol which implements attestation, known as Direct Anonymous Attestation (DAA). From its name we can derive the basic logic of the initially planned protocol which implied:

- proof without a Trusted Third Party (TTP) involvement (Direct);
- non-disclosure of the identity of the signer (Anonymous);
- requirement of statement or claim from a TPM (Attestation).

It is capable of “remotely prov[ing] that a key is held in some hardware device and provid[ing] a strong authentication combined with privacy protection”.¹¹¹ The DAA is standardized by the Trusted Computing Group and implements a number of applications, such as use of a cryptographic key for authentication of the OS as secure, secure access to networks and services, and ease of key management in companies.

Furthermore, the DAA is based on a state-of-the art group signature scheme; it relies on the Diffie-Hellman cryptographic key-exchange to protect the user’s privacy.¹¹² Diffie-Hellman key exchange is a method to exchange cryptographic keys over a public channel, and one of the earliest examples of such a key exchange in cryptography. Crucially, it allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure

¹¹¹ Camenisch, J. (2004). Direct Anonymous Attestation: Achieving Privacy in Remote Authentication. *ZISC Information Security Colloquium*.

¹¹² Introduced first in Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6), pp. 644-654. doi: 10.1109/TIT.1976.1055638. A good account for its use by the TCI can be found in Brickell, E., Camenisch, J., & Chen, L. (2004). *Direct Anonymous Attestation*. Paper presented at the Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS 2004) (pp. 132-145),ACM.

channel. Once again we see here the very specific understanding of “trust” in TC at work: we mentioned above from a sociological perspective the challenge for modern societies with their high degree of heterogeneity, isolation and anonymity to sustain the trust levels needed to allow transactions to take place. They posed a fundamental paradox: In order to trust you, I have to know you. In order to know you, I have to communicate with you. In order to communicate with you, I have to disclose some things about myself. But in order to be able to disclose things about myself to you, I need to trust you. How then, is “social control of impersonal trust” even possible?¹¹³ From the field of sociology, a for us interesting answer was given by Mark Granovetter, who argued that "concrete personal relations and structures (or 'networks') of such relations" in which economic action in modern industrial society is embedded remain an indispensable element to explain security and economic stability in modern societies.¹¹⁴ For him, examples of such embedded structures are social networks such as trade associations, professional organizations and also “quasi-firm arrangement that reflect long term associations between contractors and subcontractors”.¹¹⁵ The TCG, as an institution, is of course just such a “quasi-firm arrangement that reflects a long term association between contractors and subcontractors”. However, as we argued above, this embedded network does not extend to the outside and “brings in” the customer of the TCI – a problem to which we will return later. Rather, that external relation is governed by a reliance on classical contract law.

¹¹³ Shapiro, S. P. (1987). The Social Control of Impersonal Trust. *American Journal of Sociology*, 93(3), pp. 623-658. doi: citeulike-article-id:6111856.

¹¹⁴ Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *Ibid.*, 91, pp. 481-510. doi: 10.2307/2780199. p. 499

¹¹⁵ Shapiro, S. P. (1987). The Social Control of Impersonal Trust. *Ibid.*, 93, pp. 623-658. doi: citeulike-article-id:6111856 p. 623.

Granovetter contrasts this “embeddedness approach” against both “neoclassical” and “reformist” conceptions of economic action. The former relies, so Granovetter, on an “undersocialized”, the latter on an “oversocialized” explanation. In a nutshell, we can make sense of this idea when we go back to Lessig’s square of regulatory modes introduced above. “Undersocialised” regulation is regulation by law only, the classical, Weberian model of the formal rational law. “Oversocialised” regulation is regulation that relies mainly or exclusively on appeals to morality – the “social norms” aspect of Lessig. Instead, Granovetter argues that we are always already embedded in social networks which ensure that we unthinkingly always interact with others, without having to reflect on either type of normative system.

For the Internet, this poses a problem – while there are of course numerous “embedded” networks, in particular social media, we cannot take such a pre-existing connection for granted. This becomes particularly problematic for Trusted Computing. The one thing TC does NOT trust in, are human users. Rather, the tendency of humans to make the wrong “risk decisions” when dealing with technology and security (not updating anti-virus software, disabling firewalls when they slow down performance etc.) is a problem that TC tries to address through automation. This is one aspect of the “unhindered operation” discussed above: a system that is supposed to have a firewall has to prove to a communication partner that the security operates “unhindered by its human owner”. Machines decide which other machines can be trusted. But machines lack social embeddedness of the kind Granovetter describes. Regulation by code then has to replace this embeddedness. It ensures that we, or in the case of TC, our computers “do the right thing” and communicate without having to rely or to think about any set of rules external to that communication.

The specific element of regulation by code discussed here, secure cryptographic exchange protocols such as Diffie-Hellman, break in particular the “trust paradox” outlined above. They allow two parties that have no reasons to

trust each other whatsoever to communicate nonetheless, protecting their privacy in the process, and thus opening up a channel that can then lead to lasting trust based on observed past performance.

The aims of the TCG are materialized by integrating a trusted hardware module (TPM) into a platform (e.g. a mobile phone, a laptop). Security is essentially a combination of hardware and software. The hardware forces secure behavior that is not subject to “hacking”. The software (also) certifies that the secure hardware is in place and has not been physically tampered with. This mutual interdependence between hardware and software causes some legal problems if we try to classify “Trusted Computing” as a commercial product – is it a service, hardware or software? From the computing perspective, this distinction becomes meaningless – security is the union of these three. But law’s categories are not best suited to handle this type of interdependent entity, as we will discuss later.

Here, we discuss some of the more abstract issues that this approach generates. A user of the platform communicates with a verifier who wants to assure that the user uses the platform containing the specified TPM. However, the user wants his privacy to be protected and therefore requires that the verifier only learns that he uses a TPM, but not which particular one. Initially, TC tried to avoid any third party - the security of a system resides in its hardware, and the system’s own software guarantees this. As it runs on a secure hardware, this self-attestation in turn cannot be manipulated or forged, resulting in the theory of a “virtuous circle”.

However, it soon became obvious that this approach was not possible. Full anonymity and “trust” seemed to be irreconcilable. We encounter here another version of the paradox of trust discussed above. In “trusted mode” a party (typically called “Bob” in the informatics literature), wants to communicate with another computer (Alice) so that Bob can trust Alice to run only un-tampered hardware and software. This will assure Bob that Alice will not be able to use

malicious software, either intentionally or because she in turn was victim of a malicious hack, which could in turn, infest his computer and compromise sensitive information. But to do this, Alice has to inform Bob that she is using registered and probably safe software and hardware, thereby potentially uniquely identifying herself to Bob. In essence, Alice tells Bob everything that runs on her computer in a way that can be verified by Bob. As a real world analogy, we can think of allowing a potential business partner to have his staff search our house before he visits us for contract negotiations.

Sometimes, this is surprisingly unproblematic. During online banking transactions over the Internet for instance, I want my bank to be able to identify me anyway. Here, pre-existing social trust fills the gap technology alone can't fill. Several of Granovetter's factors for embedded social relation come into play – from the Financial Service Authority to a more nebulous belief in the professionalism of a large bank. But in many other types of communicating activities people require the anonymity that the computer provides. The compromise that TCG proposed to keep Bob anonymous with regards to Alice, while assuring her, that she is communicating with a “trusted” party was through a “trusted third party”. This entity acts as intermediary between a user and her own computer, and at the same time between her and other users. The latter, called *remote attestation* is of particular importance.

TCG provided a solution to this problem by making use of a trusted third party which in this case was called the *Privacy Certification Authority (PCA)*. Every TPM creates a key pair using the RSA algorithm and this key pair is called *Endorsement Key (EK)*. The EK is created only once and PCA keeps a record of the Endorsement Key of every valid TPM. Whenever a TPM wants to verify itself to a verifier, it creates another pair of RSA keys which is called an *Attestation Identity Key (AIK)* and sends that key pair to the PCA. The PCA then authenticates this public key which refers to the EK. Then the PCA will check if the EK is contained in its list of valid EKs. If it is contained in the list, the PCA issues to the TPM a

certificate for the AIK. The TPM can now send the AIK's certificate to the verifier and actually authenticate itself. Consequently, a TPM can only be uniquely identified by its EK which becomes known only to the PCA. So only the PCA, and not the verifier, can uniquely identify the TPM which is something that does not bother us, since the PCA is trustworthy. The verifier is only getting the TPM's AIK, which is different each time and consequently the verifier cannot uniquely identify the TPM.

In the solution described above we have two possibilities to detect a rogue TPM. These are:

1. If someone manages to obtain a TPM's secret key (EK), and distributes it, then this key can be detected and announced as a rogue secret key. Detection is achieved via a code that is executed at the very beginning during boot process and is known as Core Root of Trust for Measurement (CRTM). This code is an immutable part of the TPM that should be trusted; it is placed in the BIOS and cannot be threatened by any known software attacks due to difficulties to manipulation.¹¹⁶ The Privacy CA can then compute the corresponding public key and remove it from its list of valid Endorsement Keys.
2. If there are many enquiries at the PCA with the same EK and PCA issues certification for that specific EK, then the PCA might not want to continue issuing certificates for that EK.

Although this is a solution for the trusted computing problem, it has a major disadvantage: the PCA is involved in every transaction and thus it must be highly available, but at the same time provide as much security as an ordinary certification authority which would normally operate off-line. Moreover, if the PCA and the verifier join together, or the PCA's transaction records are revealed to the verifier - by some other means - (this can be solved using blind signatures),

¹¹⁶ Pearson, S. (2002). Trusted Computing Platforms, the Next Security Solution: Prentice Hall PTR.

the verifier will still be capable of uniquely identifying a TPM. Consequently, the problem with the PCA's availability endures.

A better solution was proposed by Ernie Brickell, Jan Camenisch and Liqun Chen. This solution was adopted by the TCG in the new specification of the TPM (1.2) in 2003. It associates techniques "developed for group signatures, identity escrow, and credential systems".¹¹⁷ The proposed scheme can be described as a group signature scheme,¹¹⁸ but one which does not have the opportunity to open signatures but with a mechanism to detect fake TPMs.¹¹⁹ "Group signatures" as a method to find a technological solution to the trust problem, allows another comparison with sociological conceptions of trust. A Group signature scheme allows a dedicated member of a group to "act on behalf" of that group and sign anonymously messages for it. For example, a group signature scheme could be used by an employee of a large company "on behalf of" the company. The verifier only needs to know that it was *an authorized* employee who signed the message, not which one. The collective provides an additional degree of anonymity, but requires internally a pre-existing degree of trust and solidarity.¹²⁰

¹¹⁷ See Brickell, E., Camenisch, J., & Chen, L. (2004). *Direct Anonymous Attestation*. Paper presented at the Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS 2004) (pp. 132-145), ACM. Adopted in TCG. (2003). TPM - Part 1 Design Principles, Specification v.1.2 (Revision 62 ed.).

¹¹⁸ on group signatures see Bellare, M., Micciancio, D., & Warinschi, B. (2003). Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions *Advances in Cryptology—Eurocrypt 2003* (pp. 614-629). Warsaw, Poland: Springer.

¹¹⁹ Brickell, E., Camenisch, J., & Chen, L. (2004). *Direct Anonymous Attestation*. Paper presented at the Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS 2004) (pp. 132-145), ACM.

¹²⁰ a similar point on the importance of solidarity for privacy protection has been made in Kwecka, Z., Buchanan, W., Schafer, B., & Rauhofer, J. (2014). 'I am Spartacus': privacy enhancing technologies, collaborative obfuscation and privacy as a public good. *Artificial intelligence and law*, 22(2), pp. 113-139.

Key to a group signature scheme is a *group manager*. That person plays a role we discussed above in the context of PGP: he is in charge of adding new members to the group and in case of disputes can reveal the original signer. This is important from a legal perspective: in case of a dispute, parties may want to rely on the third mode of regulation, formal laws, to seek redress. For this avenue to be available though, some evidence needs to be preserved in a forensically sound way. This will be at the center of the next chapter, where we will discuss the consequences of TC for evidence law. At this point we merely note the intricate balance between security and privacy on the one hand, modes of regulation on the other hand. TC uses regulation through code to increase privacy, but at the same time provides an infrastructure for litigation purposes (and if necessary at a cost to privacy) to enable the legal system to take over in a case of conflict, thus increasing, potentially, the trustworthiness of the overall approach. Many schemes have been proposed, however all should follow these basic requirements.

The scheme described in Bajikar's 2002 White Paper, also employs a signature scheme to issue certificates on a membership public key generated by a TPM.¹²¹ In order to authenticate as a group member, or valid TPM, a TPM must prove that it possesses a certificate on a public key for which it also knows the secret key. To allow a verifier to detect rogue TPM's, the TPM is further required to reveal and prove correct of a value $N_V = \zeta^f$, where f is its secret key and ζ is a generator of an algebraic group where computing discrete logarithms are infeasible. As before, there are two possibilities for the verifier to detect a rogue TPM. The first is by comparing N_V with ζ^f for all f 's that are known to stem from rogue TPM's. The second is by detecting whether he has seen the same N_V too many times. This only works when the same ζ is used many times. Yet, ζ

¹²¹ Bajikar, S. (2002). Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper. In M. P. G. I. Corporation (Ed.): Intel Corporation.

should not be a fixed system parameter or else the user will not gain any privacy. As an alternative, ζ should either be randomly chosen by the TPM each time when it authenticates itself or every verifier should use a different ζ and change it with some frequency. But, we assume that with the use of an appropriate hash function, we can derive ζ .

The scheme described above, employs the Camenisch-Lysyanskaya signature scheme, the respective discrete logarithms based proofs to prove possession of a certificate, the strong RSA assumption guarantees the memorability of certificates, and privacy and anonymity are assured by the decisional Diffie-Hellman assumption. The Fiat-Shamir heuristic is also used to turn proofs into signatures.

2.6.3 Technology / Protocols On Trusted Computing

2.6.3.1 Platforms

Both hardware i.e. the Trusted Platform Module (TPM) and software i.e. the Trusted Support Services (TSS) are combined in a Trusted Computing System. The software must contain TC-enabled applications, and hardware's role is emphasized in the 'Fritz' chip. The latter is a smartcard chip - named after the Senator Fritz Hollings, a US politician with a long history of legislative attempts to ensure that PCs do not support production of "unauthorized content"¹²² - and it is placed on the motherboard which constantly checks the software and hardware that are running on the machine. If both are found to be authorized, the operating system (OS) boots and assures any third parties that the machine is the

¹²² See Davis, Peter T. "TCPA: who can you trust." *EDPACS: the EDP Audit, Control and Security Newsletter* (2002) 15-19 p, 16

machine that claimed to be and the software that is running on it, is the software claimed to be.¹²³

An early description of the Fritz chip by the TCI is both interesting and revealing:

“When you boot up your PC, Fritz takes charge. He checks that the boot ROM is as expected, executes it, measures the state of the machine; then checks the first part of the operating system, loads and executes it, checks the state of the machine; and so on. The trust boundary, of hardware and software considered to be known and verified, is steadily expanded. A table is maintained of the hardware (audio card, video card etc) and the software (O/S, drivers, etc); if there are significant changes, the machine must be re-certified. The result is a PC booted into a known state with an approved combination of hardware and software. Control is then handed over to enforcement software in the operating system [...] Once the machine is in this state, Fritz can certify it to third parties: for example, he will do an authentication protocol with Disney to prove that his machine is a suitable recipient of ‘Snow White’. The Disney server then sends encrypted data, with a key that Fritz will use to unseal it. Fritz makes the key available only so long as the environment remains ‘trustworthy’. For this purpose, ‘trustworthy’ means that the media player application won't make any unauthorised copies of content.”¹²⁴

First, we see here how hardware and software act indeed in unison – for the product “security”, they are inseparable. As we noted above, that raises issues from a legal perspective what exactly a consumer is buying - hardware, software, a service, a combination of these two, and what legal regime is applicable. Second, we see the degree of “force” that TC products exercise over the user – If Fritz decides that there is something untoward on your machine, it will not boot. That would still be fine if “untoward” was restricted to malware that can harm me. But as the example shows, it can as well be “unauthorized” software that I added to

¹²³ Anderson, R. (2003a). Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA – Version 1.1. (2003). <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

¹²⁴ *ibid.* p.3, Question 4

rip video files. The TCI later attempted to disassociate TC from its origin as essentially a Digital Rights Management system, but here we can see just how problematic this approach could be: Not only does it either prevent third party software that “could” be used for copyright violation to run in the first place (and there can of course be many legitimate uses for such software), or alternatively prevents to communicate with (download) music files. More worrying, a chip on my own computer communicates the finding that “there is ripping software on this system, don’t trust this computer” to a third party. I have to put blind trust in this party and rely on it not disclosing the information – even though, as we just mentioned, it is preserved in a forensically sound way. The whole system is set up by companies who are also major copyright right holders. We will argue in chapter 3 and 4 that this creates a significant imbalance in procedural law and evidence, making the TCI police, prosecution and jury all in one. This imbalance asks in our opinion for regulation through law – rebalancing through the rules of admissibility and procedure, the relation between customer and TC provider.

Currently TC is a composite of five main components: the ‘Fritz’ chip; a ‘curtained memory’ – which is explained further below in section 2.6.3.1.2 – in the CPU; a security kernel in the operating system; a security kernel in each TC application; and a back-end infrastructure of online security servers. Furthermore, Safford stated that TC architecture supports two important security functions:

- Secure storage of the key pairs generated, along with public key signatures, verifications, encryptions and decryptions and
- System software integrity measurement.¹²⁵

¹²⁵ Safford, D. (2002a). Clarifying Misinformation on TCPA. *White paper*. from http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

Minimum functionality which is necessary to describe the properties that influence the trustworthiness of a computing environment is represented by Roots of Trust.¹²⁶ There are three core Roots of Trust:

- a root of trust for measurement (RTM)
- a root of trust for storage (RTS)
- a root of trust reporting (RTR).

In order for any misbehaviour within the system to be detected, all three Roots of Trust must be trusted. Roots of Trust are expected to function correctly without any external interactions. In conjunction with the Trusted Building Blocks (TBB), Roots of Trust achieve trust, while measurement, storage and reporting are done with minimal configuration.¹²⁷

To the following sub-sections we give a description of the basic protocols that were used, or are still currently in use.

2.6.3.1.1 Palladium (now NGSCB)

“Next Generation Secure Computing Base” (NGSCB) is a set of features for Microsoft Windows operating system. Initially this platform was named Palladium and is still widely known by this name. According to its promoters, Palladium provides users with greater data security than they already have, strong process isolation, sealed storage, personal privacy and system integrity. Enhanced practical user control; emergence of new server/service models; and potentially new P2P (peer to peer) or fully peer-distributed service models are some of the benefits that the platform gives to its users.¹²⁸ This system was planned to be embedded in the Windows Vista operating system, and would

¹²⁶ Burmester, M., & Mulholland, J. (2006, April 23 - 27). *The advent of trusted computing: implications for digital forensics* Paper presented at the Proceedings of the 2006 ACM symposium on Applied computing, Dijon, France (pp. 283-287),ACM Press.

¹²⁷ *ibid.* p.284

¹²⁸ Carroll, A., Juarez, M., Polk, J., & Leininger, T. (2002). Microsoft Palladium: A Business Overview: Microsoft Press Release.

become available in January 2007.¹²⁹ However, this was not possible after all, considering the low significance that third parties depicted for this implementation.

New features provided by Palladium run on existing Windows systems.¹³⁰ They require no changes, as the platform is not programmed to work on a separate operating system than Windows, and in co-operation with the same kernel, computer hardware, peripherals and chipsets.

TC's idea is to keep keys secret with the use of a digital encryption and signature device. In addition, it prevents identity theft and unauthorised access to personal data on the user's own device, while connected to the internet or to any other network.¹³¹ Overall, what this platform provides to the user is: protection to personal data, to sensitive communications and to e-commerce transactions, from attack to either the system's software or to a network's software.

2.6.3.1.2 TCPA (now TCG)

TCG proposed a technology that makes use of four main features. Along with these, new hardware installation on existing PC's is required. The features can work individually, but can also work in conjunction with each other.

Memory curtaining

¹²⁹ BBC. (2006, 30/08/2006). Amazon begins taking Vista orders, *BBC News*. Retrieved from <http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/5297892.stm>

¹³⁰ e.g. BitLocker Drive Encryption, and a new version of the Microsoft Cryptography API.

¹³¹ Carroll, A., Juarez, M., Polk, J., & Leininger, T. (2002). Microsoft Palladium: A Business Overview: Microsoft Press Release.

This refers to a “strong, hardware-enforced memory isolation feature”¹³² in order to avoid reading and writing memory between several programs. In TC the operating system should have access to this type of memory, so if an adversary enters the operating system it would not be possible for him to enter and interfere with any program and its memory. The advantages of using a hardware feature instead of software – which could operate in a similar fashion – are the: backwards compatibility; the reusability of code; and the fact that fewer changes need to be made to hardware drivers and application software.¹³³

Secure I/O

This provides a secure hardware path from the keyboard or mouse (i.e. the user) to an application and vice versa. By doing this, none of the software programs will know what the user typed as a command or input to another program and how the application responded. Protection from physical attacks is provided and any programs that intentionally “corrupt, modify, or mislead the user, will be prevented from running or operating”.¹³⁴

Sealed Storage

Until recently, any keys and passwords used by applications were stored locally on the hard-drive. This was not so secure, because keys could be accessible by any intruder or virus. So, it is important to ensure that only legitimate users can access these valuable and secret data. This is exactly what sealed storage does. It is characterised as “an ingenious invention that generates keys based in

¹³² Schoen, S. (2003). *Trusted Computing: Promise and Risk*. Electronic Frontier Foundation. Retrieved from http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.pdf

¹³³ Burmester, M., & Mulholland, J. (2006, April 23 - 27). *The advent of trusted computing: implications for digital forensics* Paper presented at the Proceedings of the 2006 ACM symposium on Applied computing, Dijon, France (pp. 283-287),ACM Press.

¹³⁴ *ibid.* p. 285

part on the identity of the software requesting to use them and in part on the identity of the computer on which that software is running".¹³⁵

Furthermore sealed storage can cooperate with memory curtaining and secure I/O in order to ensure that a user's data can be read on their computer, and only by the particular computer that were initially created on. If a different application than the one that was originally used to create the data tries to decrypt or unseal the data, the operation will end up in failure.

Remote Attestation

This aims to allow "unauthorized" changes to software to be detected. It remotely traces any changes made to any application and allows a third party to decide whether the platform is considered trustworthy.¹³⁶ This feature helps to prevent the sending of data to or from a compromised or untrustworthy computer and certifies that no unauthorised program installs, updates or that modifications are made in the hardware or software on the user's machine. Moreover, "this allows an entity to authenticate the software configuration of a platform that is not under its control".¹³⁷ This is the most significant of all features mentioned.

The TCG chip provides three main groups of functions. These are:

- public key functions: which are used for key pair generation, public key signature, verification, encryption and decryption purposes.
- trusted boot functions: which ensure that data are "trusted" if the data stored while booting are the same with the data at the time of sealing.

¹³⁵ Schoen, S. (2003). *Trusted Computing: Promise and Risk*. Electronic Frontier Foundation. Retrieved from http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.pdf

¹³⁶ Reid, J., Gonzalez Nieto, J., Dawson, E., Okamoto, E. (2003). *Privacy and Trusted Computing*. Paper presented at the Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03) (2003), Washington (pp. 383-388),IEEE.

¹³⁷ *ibid.* p. 385

Trusted booting combines both authentic booting which creates a log containing the programs that are loaded on the computing device and secure booting which ensures that the computing device is in a secure state.

- initialization and management functions: which allow the user to switch on or off the functionality, to reset the chip and take ownership.¹³⁸

TCG provides protection to sensitive authentication information from attacks by hackers and this is achieved by providing protection to the user's private key. In addition, by sealing the master encryption key under a TCG register, it is possible to protect a user's sensitive files and data.¹³⁹

TCG and Palladium have similar architectures and similar goals, but they are two different projects. One important similarity between the Palladium design and the existing TCG is that both contain the "remote attestation" feature. Palladium, in order to achieve full functionality in hardware and software, uses TCG's hardware functionality.¹⁴⁰

2.6.3.1.3 LaGrande Technology (LT)

LaGrande technology provided by Intel (recently renamed as Trusted Execution Technology (TXT)) as a response to the Trusted Computing trend – which is not a substitute of the TCPA, rather it lies heavily on the TCPA features. It is a protection model that embeds Palladium's features as mentioned above. The main features that exist in LaGrande are the I/O of data, the sealed storage, the attestation and the protected execution. Mainly, LaGrande enables to run applications in an isolated environment, which means that prevents other

¹³⁸ Safford, D. (2002a). Clarifying Misinformation on TCPA. *White paper*. from http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

¹³⁹ Safford, D. (2002b). The Need for TCPA. from http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf

¹⁴⁰ Safford, D. (2002a). Clarifying Misinformation on TCPA. *White paper*. from http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

applications to intervene or compromise data. ‘Standard partition’ and ‘Protected partition’ are two new features that this technology uses. The first applies when the users are able to run applications and other software just as they did in the ordinary PC. The second applies when different applications can run secluded by any other software running on the same PC.

2.6.3.1.4 AMD Pacifica

At this point, it worth mentioning that apart from Intel’s LaGrande technology, AMD is working on one called formally Secure Execution Mode (known as SEM) and then called Pacifica and later marketed under the trademark AMD Virtualization, abbreviated AMD-V. These two projects are hardware-related and provide hardware support to all major features of Window’s Palladium which is software-oriented.

In particular AMD develops a security and virtual machine architecture which enables a single operating system to run in parallel numerous operating systems. This architecture supports Virtual Machine Architectures both for servers and clients,¹⁴¹ and allows a third party operating system to access the host’s operating system directly, resulting in higher performance.

2.7 Recap and summary

This first substantive chapter tried to achieve several goals. It tried to give the reader a general understanding of what “Trusted Computing” means, and why it is a good prima facie candidate to address the cyber security problem: It is a paradigmatic example of regulation through code, where the freedom of the user to reconfigure her machine is restricted in exchange for greater, but not perfect, security. It protects the user, the integrity of her machine and also her privacy

¹⁴¹ McDowell Steve, S. G. (Producer). (2005). Pacifica – Next Generation Architecture for Efficient Virtual Machines. Retrieved from http://developer.amd.com/wordpress/media/2012/10/WinHEC2005_Pacifica_Virtualization.pdf

against other computer users to a degree, but at the cost of disclosing more of her information to a trusted third party, and by exposing her to greater security risks should that third party in turn be compromised. It aims to create a decentralized, bottom up solution to security where security follows along the arcs of an emergent “network of trust”. If it were successful especially in the latter, we would have found a form of code based regulation that is strictly isomorphic to the Internet itself, making a significant contribution to the problem of regulation of complex and dynamic systems that Guadamuz had identified.

We introduced the general idea of Trusted Computing or TC by looking in more detail at the technical details of the specific implementation of this concept that is promoted by the Trusted Computing Initiative. The TCI has pushed the concept of TC closer to implementation, but nonetheless uptake so far remained disappointing. The reasons that are given for this relative failure differ. According to its critics, TC is an attempt at empire building by a cartel of big international businesses to foster their own agenda, exclude competitors (especially open source), help right holders to enforce their copyright even more brutally and in the process ride roughshod over consumer privacy. The security they promise is not the appropriate in light of their market share, reputation and brand name: pay us and we will protect you – but hand over your weapons first. In the long run, consumer security can as a result suffer even more, as we lose the ability to look after our own security, with products of our choice whether TCI certified or not. According to its promoters, TC remains the last best hope for a secure Internet, with the Internet of Things if anything requiring more radical versions

of TC,¹⁴² “TC on steroids” as one commentator put it.¹⁴³ The relative lack of uptake then is the result of misconceptions – either due to miscommunication on the side of the TCI, or even maliciously spread by its detractors.

We tried in this chapter to lay the groundwork for a more nuanced assessment. In our analysis, the problems the TCI faces are grounded in the intentional, systematic but sometimes misunderstood and miscommunicated difference between the conception of trust in informatics, what we termed “techno-trust”, and the concept of trust that is more commonly used in sociology, including the sociology of law. To deliver the benefits it intends, and that for us means to bring about a self-organizing, complex and dynamic network of trust that is isomorphic to the Internet infrastructure, and allow security to follow trust along the arcs or nodes of the network, the sociological understanding of trust is needed, or at least an understanding of trust that shares with it certain fundamental characteristics, such as transitivity and holism. But techno-trust is designed to be different. It is based on a concept of “predictability” that shares only some overlap with the sociological concept of “trustworthiness”, and even less with the concept of “trust” simpliciter. It aims to calculate, for a specific interaction, the degree of trust that one can rationally place on this one

¹⁴² see eg. Ukil, A., Sen, J., & Koilakonda, S. (2011, 4-5 March 2011). *Embedded security for Internet of Things*. Paper presented at the Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on (pp. 1-6), IEEE. For a more sociologically driven approach similar to the one developed here see Kjøien, G. (2011). Reflections on Trust in Devices: An Informal Survey of Human Trust in an Internet-of-Things Context. *Wireless Personal Communications*, 61(3), pp. 495-510. doi: 10.1007/s11277-011-0386-4.

¹⁴³ Franz, M. (Producer). (2005). Practical Language-Based Security From The Ground Up “Verify Everything, Every Time & Prove It Remotely”. [ppt] Retrieved from <http://www.doi.ics.keio.ac.jp/CIIP05/26/11-Franz.pdf>.

transaction, by predicting the chances of malevolent behavior. But for the sociologist, “Trust begins where prediction ends”.¹⁴⁴ Lewis and Weigert conclude:

“In groups for which trust exists as a social reality, interpersonal trust comes naturally, and is not reducible to individual psychology [...] like the Durkheimian collective representation, the sentiment of trust is manifest in the psyche of individual group members, but this must not lead us to the common, but erroneous inference that trust is fundamentally an individual and behavioral phenomenon produced by rational machinations of autonomous, calculating individuals.”¹⁴⁵

If we replace in the quote above “calculating individuals” simply by “calculators”, then of course we would have a description of the TCI approach to trust in a nutshell. It is much more akin to the Weberian, rule based model of formal rationality and the type of “trust” it engenders: a trust in the predictable behavior of institutions as third parties.

We then tried to show that this is not just an abstract sociological interpretation. Rather, the different understandings of trust result directly in certain design choices for TC. In a close reading of the technical specifications, we tried to “translate” or “give meaning to” as many of the design choices into the language of sociology. In the case of enforcing unique identities and their attestation remotely by third party, we saw the clearest parallel to the Weberian bureaucratic state under the rule of law, with centralized government. Just as the government in the modern nation states issues unique IDs and then ensures their attestation against centrally held registers such as the criminal record register, so does TC (attempt to) build trust on the basis of identifiers that allow parties in a communication to predict future benevolent behavior on the basis of a record of past wrong (and right) doing. But trust, as a sociological concept, tries exactly to fill the gaps left by the Weberian formal rationality, plug the holes that this

¹⁴⁴ Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, 63(4), pp. 967-985. doi: 10.1093/sf/63.4.967 p. 976.

¹⁴⁵ *ibid.* p. 975

concept of human interaction can't fill on its own. So in the same way in which societies in addition to predictability and Weberian "rational reliance" still need social trust as a supplementary yet distinct feature, so does a TC approach require "something else" in addition to the rule based predictability that it enforces by code.

The absence of this "something else", so we argue, contributes in two ways to the failure of TC so far. One is specific to the TC: there is insufficient trust *in them* to bring about what would be a massive shift of power from consumers to the TC provider. The second problem is more fundamental: every implementation of TC that has the generic features outlined above will still face the problem that it atomizes the trust relation to a bi-polar relation between them and a customer, not a network of trust. *In principle*, TC on its own cannot create the social trust that it needs to work as intended.

If this analysis is correct, then we face a serious problem: The sociological concept of trust, as we tried to show, has evolutionary origins, evolved in humans in complex interaction with social institutions such as religion, kinship and ideology, and became in the process both deeply ingrained in our individual psyche, our emotional responses to others and the way we deal with risk in everyday situations, but also and most importantly automatic, taken-for-granted, non-reflective and in the words of Granovetter "embedded". TC though is regulation by code, here ultimately machines "trust each other" (which then allows the human customer to trust his own machine, as a side effect at best). Computers are not the result of organic evolution over millennia and carrying their evolutionary roots with them at all times – a point Joanna Bryson has made forcefully to argue why we need not be afraid of the Artificial Intelligence (AI) apocalypse.¹⁴⁶ Computers also don't have religious or ideological convictions,

¹⁴⁶ Bryson, J. (2011). AI robots should not be considered moral agents. In N. Berlatsky (Ed.), *Artificial Intelligence*. Detroit: Greenhaven Press.

kinship based loyalty or other emotional attachments to other machines. Nor can they take things “for granted” or embedded in their world – quite on the contrary everything they know must be explicitly represented and taught. All this, on balance, is a very good thing. But does it mean that TC is doomed from the very beginning, and regardless of who the TC provider is?

We don’t think so, and the next two chapters will outline a way out of the dilemma. At first glance, it will look counterintuitive, for we will argue that traditional laws (as opposed to laws embedded in code) can play an important contribution to fill the gap between “techno-trust” and “social trust”. This should indeed raise some eyebrows – did we not just argue that Weberian formal rational law can at best create an abstract “trust in institutions” by rational actors who (only) want to predict the behavior of their commercial partners, the shortened and “thin” version of trust that the “thick” concept of social trust wants to supplement? We obviously need to qualify to a degree that analysis. In doing so, we draw our inspiration from some of the sociological thinkers discussed above. In particular, we aim to combine Luhmann’s system theoretic view, Johan Olsen’s attempt to reinvigorate the role of bureaucracies as regulatory tool in the network society, and the evolutionary account of trust that we touched upon above. The evolutionary account of trust reminds us that the emergence of social trust is not only shaped by the environment, it is at the same time shaping that very environment. Early normative systems such as religion evolved in response to and as a reflection of social practices of cooperation. The same type of self-reflective hyper cycles is generalized in Luhmann’s work as a general constitutive factor of the way in which systems maintain themselves.¹⁴⁷ This puts a paradox

¹⁴⁷ applied to law in particular by his student G Teubner. See Teubner, G. (1997). Breaking Frames: The Global Interplay of Legal and Social Systems. *The American Journal of Comparative Law*, 45(1), pp. 149-169. doi: 10.2307/840962.

at the very heart of the emergence of law and legal order.¹⁴⁸ In our case, this means more specifically that the post-Weberian recognition of the irreducible importance of social trust for the maintenance of order in social systems in turn “reflects back onto” the Weberian concept of formal rational law. Formal rational law is then not the irreconcilable opposite of social trust, rather, they engage in a dialectical relation. Social trust enabled the emergence of formal laws, formal laws then stabilize the societies and their trust relations, while being in the process “translated” and changed into something new. This system’s theoretical idea of “imperfect translation” between normative systems has been described by Zenon Bankowski, who in doing so carved out a place for “the ethics of being a legal formalist”, merging two previously antagonistic concepts.¹⁴⁹

To put this into slightly more concrete terms, we can re-think the Weberian concept of law by asking the question: how could specific legal rules look like who do not just try to enhance predictability for atomistic individuals, but which are drafted as a result of the experience of having encountered the conceptual limitations of the Weberian approach? This can then provide a regulatory environment where the problems of TC’s reduced conception of trust are at least ameliorated.

We touched above on two specific problems: TC shifts power from customer to TC provider, who in the process takes on roles previously reserved for the nation state. How then, in a democratic state, can we trust those that make the rules? Law, in particular constitutional and human rights law, play at least a part of the answer. This is a topic we will take up in the next chapter, where we will

¹⁴⁸ See e.g. Luhmann, N. (1988). The Third Question: The Creative Use of Paradoxes in Law and Legal History. *Journal of Law and Society*, 15(2), pp. 153-165. doi: 10.2307/1410051

¹⁴⁹ Bańkowski, Z. (2007). Bringing the outside in: the ethical life of legal institutions *Law and legal Cultures in the 21st Century: Unity and Diversity (Wolters Kluwer Polska, 2007)* (pp. 193-217).

look at those functions of TC that makes the TCI provider most state-like, and ask what minimal legal guarantees need to be in place to accept, trustingly, this shift of power.

Secondly, traditional liberal contract law, the epitome of Weberian formal rationality and his paradigmatic example, has the problem that it reduces complex social relations to binary exchange relations. Binary relations that are not transitive, so we argued, disrupt rather than create networks. Contract law will have to play a central role for the way in which the TC provider interacts with his customers – but can we think of a contract law that does not result in atomism, which “brings in” potentially affected third parties and results in holistic networks? This will be the topic of the fourth chapter.

Taken together, they can be seen as an attempt at “reflexive law”, another concept developed within the system theoretical paradigm and based on an evolutionary account borrowed from the biological study of emergent normative behavior.¹⁵⁰ The result is not a law that aims to directly ensure desired social outcomes, rather, it “restricts itself to the installation, correction and redefinition of democratic self-regulatory mechanisms.”¹⁵¹ In the same vein, we will look mainly at specific ways in which law can correct or redefine the implicit and democratically not validated shift of power from customer to TC provider, in the process enhancing the social environment and its social trust within which TC must operate.

¹⁵⁰ Classically, Teubner, G. (1983). Substantive and Reflexive Elements in Modern Law. *Law & Society Review*, 17(2), pp. 239-285. doi: 10.2307/3053348. For an application to the legal issue of privacy, central also to TC, see Dorf, M. C. (2003). The Domain of Reflexive Law. *Columbia Law Review*, 103(2), pp. 384-402. doi: 10.2307/1123697. For a critical evaluation, see Blankenburg, E. (1984). The Poverty of Evolutionism: A Critique of Teubner's Case for "Reflexive Law". *Law & Society Review*, 18(2), pp. 273-289. doi: 10.2307/3053405.

¹⁵¹ Teubner, G. (1983). Substantive and Reflexive Elements in Modern Law. *Ibid.*, 17, pp. 239-285. doi: 10.2307/3053348 p. 239

CHAPTER 3 :

TRUSTED COMPUTING AND THE DIGITAL CRIME SCENE (FORENSICS COMPUTING AND CRIME PREVENTION)

3.1 Whom to trust with crime prevention and detection

In the last chapter, we argued that TC brings a significant shift of power away from customers to industry. We also described how an increase in privacy towards third party (and the security this brings with it) is balanced against an increase of exposure towards the TC provider. In this chapter, we follow up on this idea in an aspect of TC that epitomises this shift in power and responsibility more than any other – crime prevention and detection. This chapter analyses the future of digital forensics in an environment where control is increasingly taken away from PC users and remotely managed by trusted third parties, typically to improve Internet security. The TCI is used again as the most developed example to illustrate some of the possible legal issues that arise.

In recent years, politicians have begun to take cyber crime more seriously. For instance, the UK government recognizes the detrimental effect that a cyber attack could have on the economy and the social well being of the country.¹ In 2011, cyber crime remained the one field of policing that not only survived the recent spending cuts, but benefited from substantial additional investment as a result of reports that estimate the loss due to cyber crime for the UK at £27

¹ The Government reply to the fifth report from the House of Lords Science and Technology committee, Cm7234. (2007). *The Government reply to the fifth report from the House of Lords Science and Technology committee*. London: The Stationery Office Limited.; Securing Britain in an Age of Uncertainty: The Strategic Defense and Security Review, Cm7948. (2010). *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. London: The Stationery Office Limited.

billion.² The threat of cyber attack is now classified as a “tier one risk”, next to international terrorism using chemical, biological, radiological or nuclear attack by terrorists, a military crisis or an influenza pandemic.³

An influential House of Lords report in 2007 described the shortcomings of present approaches to Internet security.⁴ It critically discussed in great clarity and detail, the regulatory alternatives that governments are facing and their respective shortcomings:

- Shift the risks and responsibilities even further to users. This could happen for instance by leaving the user with any losses incurred because their computer is not sufficiently secured, or creating a strong evidential presumption that they were negligent if their data is stolen.
- Invest in conventional approaches to crime prevention and deterrence, that is a better resourced police and more specialist units, more aggressive prosecution of cybercrime and stiffer sentences.
- Make it a state priority to provide considerable new investment in the IT infrastructure and thus reduce crime from happening “by design”.
- Provide incentives to the private sector to provide software programs that are more secure. This could happen by imposing more, and more

² The Cost of Cyber Crime, Office of Cyber Security and Information Assurance (OCSIA), & Detica. (2011). *The Cost of Cyber Crime*. Cabinet Office and Detica Retrieved from <http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime>.

³ Cm7953. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: The Stationery Office Limited Retrieved from http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy. p. 27

⁴ House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm>.

easily enforceable, liability on the software vendor for writing programs that are vulnerable to attacks.

The Internet was not originally intended as a platform where people spend a substantive percentage of their lives, engage in commercial activity on a large scale, work, play and socialize, and interact in various forms with their governments. As the Internet becomes more central to the lives of most people, it was inevitable that criminals began to exploit its weaknesses to a much greater extent than previously. At one brief point in time, the main threat seemed to come from overenthusiastic teenagers designing viruses, but the risks are now from highly organized criminal groups with significant resources, both in terms of expertise and computing power.⁵ In addition, entire nation states can be subject to successful cyber attacks, possibly with the tacit approval or open participation of foreign states, or at the very least “rough agencies” close to state security agencies or the military.⁶ With hindsight, the development of the Internet might usefully have included security as a design feature. Starting again from the beginning is not a feasible option, which means that any response is likely to be a patch added to the existing system rather than a complete rebuild. Attempts to deal with the increasing number of reported cyber crime incidents include more

⁵ Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), pp. 528-535. doi: 10.1016/j.clsr.2009.09.005

⁶ For an example see the attack on the cyber infrastructure on Georgia by (probably) Russia US-CCU Special Report. (2009). Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008. In J. Bumgarner & S. Borg (Eds.): US Cyber Consequences Unit. (pp. 9). Or the attack on the Iranian nuclear facilities through Stuxnet, described eg. in Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *Security & Privacy, IEEE*, 9(3), pp. 49-51. doi: 10.1109/MSP.2011.67. For a comprehensive overview see Andress, J. (2014). *Cyber warfare techniques, tactics and tools for security practitioners* (Second edition.. ed.): Waltham, Massachusetts : Syngress, an imprint of Elsevier.

legislation, user training, public awareness, and other technical security measures.⁷

However, the Internet will remain imperfect, and things will go wrong. Indeed, as we argued in the previous chapter, the futile search for perfect security may ultimately do more harm than good, by creating a misplaced sense of security in technology that might increase the use to take greater risks. This in turn raises two related questions from a legal perspective:

1. Who should be given the role of minimizing the harm, together with the rights and authority that comes with such a role?
2. Whoever that entity or person is, can or should they be held legally liable if harm occurs nonetheless?

These two questions are connected. In a radical answer to question 2, software producers could not only be held liable for the harm done to one of their customers, when flaws in the software enable a hacker to steal sensitive data.⁸ Rather, they could also be held liable if the computer subsequently becomes part of a botnet and harms third parties, outside the contractual nexus. This, obviously, would be a strong incentive for software developers to invest in program safety. However, if there was such a radical change of the liability regime, it would be necessary to give them the rights and privileges necessary to enforce, the new safety features that they have developed, if necessary against their own customers. Similarly, owners of computers could also be held liable for

⁷ Cm7642. (2009). Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space. London: The Stationery Office Limited.

⁸ Existing liability regimes for faulty software have largely failed to provide an incentive to software producers to make safety an overriding concern. While in theory, contractual liability for negligent design flaws does exist, it rarely results in successful actions. For the US, see Phillips, D. E. (1994). When Software Fails: Emerging Standards of Vendor Liability Under the Uniform Commercial Code. *The Business Lawyer*, 50(1), pp. 151-181.

third party harm if their computer was used in a botnet attack. In both cases, the treatment of computers would be analogous to the way in which some jurisdictions treat ownership of guns – legal to own, but where a third party comes to harm, the owner faces liability if they are negligent.⁹ Even closer to TC in this respect is the regulation of electronic signatures under the Electronic Signatures Directive, where the certifying authorities are held liable when third parties rely on a negligently issued certificate (or, under national implementation of the law, possibly even stricter).¹⁰ A final example presents negligently prepared audit reports by chartered accountants which can also trigger third party reliance.¹¹ We will come back to this use of private law and delictual liability in the next chapter. There, we will discuss if TC providers could or should be held liable for third party reliance on their product. Here, the point to note is that even in the absence of TC, the possibility to impose delictual liability on software developers for security risks in their products even outside the contractual nexus with their customers is one of the regulatory options governments have in principle to improve the security of the Internet.

As mentioned above, the House of Lords' report identified three possible answers: to rely on laws and policing by the state, with a general responsibility similar to that as exists for other critical infrastructures; to provide incentives by requiring users to protect themselves, or to treat it as a technological problem that is left best to software professionals in the “enabling” industries, from PC

⁹ McClurg, A. J. (2000). Armed and Dangerous: Tort Liability for the Negligent Storage of Firearms. *CONNECTICUT LAW REVIEW*, 32, pp. 1189-1246.

¹⁰ Balboni, P. (2004). Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication. *Information & Communications Technology Law*, 13(3), pp. 211-242. doi: 10.1080/1360083042000219074

¹¹ Feinman, J. M. (2003). Liability of Accountants for Negligent Auditing: Doctrine, Policy, and Ideology. *FLORIDA STATE UNIVERSITY LAW REVIEW*, 31, pp. 17-66.

manufacturers to ISPs.¹² Edwards offers a helpful analysis of these different regulatory strategies.¹³

The first option is funded by the taxpayer for the benefit of a very specific segment of the economy, in effect a hidden subsidy for bad software design – analogous to asking the government to use our taxes to construct even safer roads, so that vehicle manufacturers can spend less on designing safer braking systems. In addition, governments only act within national borders, which seriously limit their efficiency in addressing what is a global problem. Making users responsible for their own safety was traditionally, as the report notes, the preferred option by government and business alike – but as security experts have noted, this is an entirely unrealistic notion: the average user does not have the technological sophistication to protect himself, and, as one response to the report stated, “consumers were not required to purify or boil water, when the source of contamination was within the water supply infrastructure itself. Instead suppliers were required to maintain a secure network, and treated water up to exacting standards. The end-user simply had to switch on the tap to get pure, drinkable water”.¹⁴ Finally, there is the option of holding the private sector and the software industry responsible for the safety of the Internet.¹⁵

For several reasons, the strategy of holding the private sector and the software industry responsible for the security of the Internet has much to

¹² House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm>.

¹³ Edwards, L. (2006). Dawn of the Death of Distributed Denial of Service: How to Kill Zombies. *Cardozo Arts & Entertainment Law Journal*, 24(1), pp. 23-62.

¹⁴ House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm>. at 3.30.

¹⁵ *ibid.* at 3.20.

recommend itself to policy makers. Internet service providers, hardware developers and software vendors enjoy the commercial benefits from the Internet, and their know-how and expertise means they are best placed to protect the user against the most common dangers. Furthermore, many of these companies already operate globally, avoiding some of the limitations that governments would inevitably face, and thus also avoiding the need for an international treaty that take a long time to negotiate. Putting the industry at the centre of the effort to create a secure Internet is indeed one of the recommendations of the report, if necessarily backed by legal sanctions. Releasing inherently vulnerable software and hardware to consumers, in this view, should carry at least the same liability that a water vendor would incur for the safety of the glass bottles used in storing the water – in a UK context, the Donoghue snail striking again, at both vendors and manufacturers.¹⁶

This course of action would, naturally, create a significant risk to technology companies, exposing them to potentially costly litigation. Arguably, a much better strategy for the industry is to pre-empt any additional legislation by improving security voluntarily. The TC initiative can also be seen as a first response to this threat, with software companies and hardware developers taking on the responsibility for (aspects of) the Internet infrastructure. From an industry perspective, this self-regulatory approach has the advantage of much more fine-tuned cost/benefit analysis. Where the law can only operate in broad categories of “negligence”, “gross negligence”, leaving it to more or less technologically aware judges (or in the US, juries) to determine if a specific software fault was due to such a below-par performance by the developers, industry has a much more fine grained understanding where further investment in security creates

¹⁶ Donoghue v Stevenson 562 (A.C. 1932). On the legal principle see MacCormick, N. (1991). Donoghue v. Stevenson and legal reasoning. *Donoghue v. Stevenson and the Modern Law of Negligence, Continuing Legal Education of British Columbia, Vancouver*, pp. 191-213.

measurable benefits.¹⁷ As we discussed in the previous chapter, the crucial distinction between “safe” software, “trusted” and “trustworthy” software that is based on different degrees of safety was developed precisely to enable such a balancing approach. It is at least debatable how legal concepts of liability “match” this risk management approach, creating a degree of uncertainty for software developers that in turn can have a negative impact on another crucial sector to balance incentives for investing in security with litigation risks - the insurance sector.¹⁸

Legal liability regimes in this way interact with markets as form of regulation, stepping in where market failures are apparent and it is too easy for actors to externalize costs to the wider community – the situation we see pretty much consistently in the field of Internet security today, where the costs for security flaws tend to fall everywhere but the developers. We will come back to this issue in the next chapter. Here we take a slightly different take on the issue.

Ensuring “security”, long before the Internet, has always been a mix of two aspects. If we take the police as a classical institution employed by the state to ensure that societal peace is maintained, we can distinguish between reactive

¹⁷ See the influential early study by Gordon, L., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), pp. 438-457. doi: 10.1145/581271.581274, for a more recent analysis based on their work see Nagurney, A., & Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS: Economic Research and Electronic Networking*, pp. 1-22. doi: 10.1007/s11066-015-9094-7.

¹⁸ On the role of insurance industries for an optimal incentive structure in cybersecurity see Kesan, J., Majuca, R., & Yurcik, W. The Economic Case for Cyberinsurance: University of Illinois College of Law. and also Lelarge, M., & Bolot, J. (2009). Economic Incentives to Increase Security in the Internet: The Case for Insurance (pp. 1494-1502). A critical assessment on the disappointing uptake of cyberinsurance see Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, 52(11), pp. 68-73. doi: 10.1145/1592761.1592780.

policing, solving of a crime after one has occurred with the aim of prosecution, punishment and deterrence, and proactive or 'intelligence led policing' that attempts to prevent crimes before they occur.¹⁹ Both strategies have always been employed by modern police and law enforcement organizations, though the relative weight given to each strategy has changed through the ages. As a result of technological developments, recent decades saw a particularly high interest in "proactive" or 'intelligence led policing' that uses data analytics to predict and prevent crime.²⁰ Related to this and even closer to the topic of this PhD are attempts to reduce crime through architecture, measures that make it impossible to commit crime even without police interference.²¹ While technology has in recent years pushed crime prevention into the forefront of public debate, it is important to remember that first, these methods long predate modern ICT,²² and second post-crime analysis and investigation remains as important as ever.

One reason for this is an inherent tension between the two approaches. A simple example can illustrate this point. Imagine the police have received a tip off about a planned bank robbery. From a crime prevention perspective, the most

¹⁹ For a general discussion see Gilling, D. (1997). *Crime prevention : theory, policy and politics*. London: London : UCL Press.

²⁰ For a comprehensive analysis the reader is referred to Ratcliffe, J. H. (2012). *Intelligence-led policing*: Routledge.; for an application to cybercrime see in particular Van Brakel, R., & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Technology-led policing*, 20, pp. 165.

²¹ For a recent analysis of the state of the art in offline crime reduction through design, see Crowe, T. D. (2000). *Crime prevention through environmental design : applications of architectural design and space management concepts* (Second edition.. ed.). Boston, Mass.: Boston, Mass. : Butterworth-Heinemann.; For a cyberspace specific analysis see Katyal, N. K. (2003). Digital Architecture as Crime Control. *The Yale Law Journal*, 112(8), pp. 2261-2289. doi: 10.2307/3657476.

²² For an overview of early architecture-driven crime control offline, see Jeffery, C. R. (1977). *Crime prevention through environmental design*: Sage Publications Beverly Hills.

obvious response would be to inform the owner, and increase substantially the visible police presence. This will in all likelihood deter the criminals from even attempting the crime. The obvious disadvantage is that such a high profile intervention is likely to lead to a mere replacement of the criminal activity – the gang is either going to wait until the police scales down its presence, or move to another, less well protected bank. Especially technology driven approaches to crime prevention such as CCTV, often have the effect to simply move crime into other areas, leaving overall crime figures in the long run unchanged.²³ A different approach therefore could have been to maintain a low profile, allow the criminals even some initial success (and hence the completion of crime, such as breaking and entering e.g.) and only arrest them when they try to leave the bank with the money. From the perspective of a successful prosecution, this is close to ideal – the completion of the crime means evidence is created that has high probative value. This will prevent this specific gang from striking again (anytime soon, at least), and also send a deterring signal to other would-be bank robbers. On the other hand, this exposes the bank to a much higher risk, not just because they might get away with the money, but also because the security weaknesses of the bank come into open display, for the next robber to copy and to exploit.

²³ For a study close to our example see e.g. Clarke, R. V., Field, S., & McGrath, G. (1991). Target hardening of banks in Australia and displacement of robberies. *Security Journal*, 2(2), pp. 84-90. On CCTV and displacement see Armitage, R. (2002). To CCTV or not to CCTV. *A review of current research into the effectiveness of CCTV systems in reducing crime*. London: Nacro, pp. 1-8. For an analysis very similar to the economic and game theoretical approaches used above to evaluate incentives to invest in security: Cornish, D. B., & Clarke, R. V. (1987). UNDERSTANDING CRIME DISPLACEMENT: AN APPLICATION OF RATIONAL CHOICE THEORY. *Criminology*, 25(4), pp. 933-948. doi: 10.1111/j.1745-9125.1987.tb00826.x. A more optimistic view is taken in Johnson, S. D., Guerette, R. T., & Bowers, K. J. (2012). Crime displacement and diffusion of benefits. *The Oxford handbook of crime prevention*, pp. 337. which also mentions “benefit diffusion” as an often difficult to measure consequence of “crime prevention by design”.

The criminal law tries to mitigate this tension in several ways, for instance by creating “inchoate offenses”, the possibility to charge for mere attempts to commit a crime. Still, arresting the criminals with the money is more persuasive too than arresting them shortly before they enter the bank, but equipped with power tools for cutting into a safe – in this case they may still try to present an innocent explanation for the equipment and their activities. Difficult decisions will have to be made how far an attempt is allowed to proceed, to ensure sufficiently strong evidence is generated. Since both reactive and proactive strategies have advantages and disadvantages, crime control then is finding an appropriate mix and manages the inherent tension.

How can we apply these ideas to Trusted Computing and similar trust based approaches to Internet security? From what we discussed in the preceding chapter, TC is an obvious candidate for architecture-based, proactive crime control. This type of crime reduction through prevention is also historically the strategy most amenable to private sector actors. Long before the modern nation state, private security – from armed guards to castles with their moats and iron bars – dominated the scene. Indeed, the modern police force in Britain grew out of a mix of voluntarism – the citizen as police officer – and hired security guards.²⁴ Much less prominent is however the use of private agencies for crime investigation and “post-crime” security work.²⁵ While there are of course private detectives, their main role was traditionally in the preparation of civil litigation. While this could involve analyzing crimes – one can think e.g. of arson investigators employed by security companies – these roles remained for a long

²⁴ For an overview of the historical development and why it matters for contemporary discussions of crime control through technology see Schafer, B. (2013). Crowdsourcing and cloud sourcing CCTV surveillance. *Datenschutz und Datensicherheit - DuD*, 37(7), pp. 434-439. doi: 10.1007/s11623-013-0173-3.

²⁵ For a qualitative analysis of private investigators, including a historical overview, see Draper, H. (1978). *Private police*. Hassocks: Hassocks : Harvester Press.

time limited.²⁶ This is understandable when we consider that crime investigation benefits greatly from the availability of sovereign power that is exercised through the state, such as compelling witnesses, gaining access to dwellings or correspondence of citizens against their consent, and ultimately the power to arrest. These key functions were reserved in the modern nation state for public police as parts of the executive power, even though in particular in common law countries, this transition was never perfect and legal remnants of the old regime, such as the rarely used private prosecutions in English law or the elected “posse” in the US remained on the statute books.²⁷

This situation however changed over the past few decades, partly as a result of the neo-liberal, minimal state (“Washington”) consensus that pushed privatization deep into territory previously the reserve of the state, including all aspects of the justice system.²⁸ These developments let Bayley and Sheering talk about a “watershed” in the history of policing which radically alters not just our perception of the police, but that of the state as guarantor of safety and security in general.²⁹ Partly this development is also the result of an ever increasing

²⁶ There are sectorial exceptions. Some crime investigation requires specific subject knowledge that is most likely to be available through potential victims – e.g. economic crime that requires expertise in business and accountancy. See e.g. Williams, J. W. (2005). Reflections on the Private Versus Public Policing of Economic Crime. *The British Journal of Criminology*, 45(3), pp. 316-339. doi: 10.1093/bjc/azh083.

²⁷ For a comprehensive analysis of the transition of pre-modern proto-police to executive-centric police of today, see Rawlings, P. (2003). Policing before the police. *Handbook of Policing*, 2, pp. 46-72.

²⁸ see e.g. Sheering, C. D., & Stenning, P. C. (1981). Modern Private Security: Its Growth and Implications. *Crime and Justice*, 3, pp. 193-245. , Williams, J. W. (2005). Reflections on the Private Versus Public Policing of Economic Crime. *The British Journal of Criminology*, 45(3), pp. 316-339. doi: 10.1093/bjc/azh083; See also Gill, M., & Hart, J. (1997). Policing as a business: The organisation and structure of private investigation. *Policing and Society*, 7(2), pp. 117-141. doi: 10.1080/10439463.1997.9964768.

²⁹ Bayley, David H., and Clifford D. Sheering. "The future of policing." *Law and society review* (1996): 585-606.

specialization in the forensic field that made it difficult for police organizations to cover all aspects of an investigation with equal efficiency. Computer forensics in particular is often carried out by private subcontractors of police agencies.³⁰ Technology has generally been an enabling factor for greater involvement of the private sector in core policing functions.³¹ Unsurprisingly, we find increasing voices that argue that cyber-investigations, not just preventative cybersecurity, should make more comprehensive use of private sector participants.³²

What we can take from this debate is that TC fits strongly with the general push towards stronger private sector involvement in what was traditionally mainly a police and hence function. We will indeed argue that it can be understood as a particularly radical approach to assign state roles to the private sector, not just helping with, but as we saw in the previous chapter guaranteeing or certifying the safety of the Internet. We also note that increasingly, private sector policing stops to be limited to pre-crime protection and prevention, and moves into the field of post-crime investigation, especially in areas where technology plays a crucial role. The tension that we noted above between pre-crime prevention and post-crime detection then means, so we will argue in the rest of this chapter, that a move of TC into the field of crime investigation is not only in line with general developments in the field of policing, but indeed almost

³⁰ a comprehensive case study for Canada can be found in Schneider, S. R. (1998). Combating Organized Crime in (and by) the Private Sector A Normative Role for Canada's Forensic Investigative Firms. *Journal of Contemporary Criminal Justice*, 14(4), pp. 351-367.

³¹ A detailed case study of the technological drivers from the US perspective can be found in Dunbar, P. (1997). What will be the Impact of Civilianization on Police Investigations by 2002 at the Oakland Police Department? *Command College Paper*, 2, pp. 1-8.

³² See e.g. Phillips, A., & Nance, K. L. (2010). *Computer Forensics Investigators or Private Investigators: Who Is Investigating the Drive?* Paper presented at the Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on (pp. 150-157),IEEE.

inevitable. If TC were only a pre-emptive security measure, the crime displacement problems that we noted above are likely to arise, and in the light of the discussion of the previous chapter, with particular poignancy. In the first stage of uptake of the technology, the network effect or the immunity that TC offers will be limited, requiring investment with initially limited returns – one of the reasons we argued that are responsible for the relative lack of success of the TCI. Once however a sufficient number of machines are TC, we should expect that criminals will shift their attention to those machines not yet secured. This is in the typology of Johnson, Guerette and Bowers,³³ a replacement of targets, one of the socially and politically most problematic displacements since it tends to affect the poorest and most vulnerable the most. This is due to the additional costs of TC that we discussed previously likely to be an issue also for the TCI, their arguments that they are simply offering a service for those digital actors whose safety sensitivity demands higher investment, but is easily affordable since they will typically also make profit online much more problematic than maybe anticipated. Another effect of this likely target replacement will be that using TC will become even more inevitable, strengthening further what is already a powerful cartel with in-built monopolistic tendencies.³⁴ However, once TC uptake has achieved saturation, this type of replacement becomes impossible. Judging from the experience with CCTV, at this point criminals will “return” to the protected environment, due to a lack of alternative, easier targets. At this point criminological research predicts a different type of displacement, not of targets but methods.³⁵ Criminals will shift their activities to methods that are less

³³ Johnson, S. D., Guerette, R. T., & Bowers, K. J. (2012). Crime displacement and diffusion of benefits. *The Oxford handbook of crime prevention*, pp. 337. op.cit. p. 337

³⁴ as discussed in the previous chapter – one of the consequences of the TCI approach would be that unprotected machines lose the ability to communicate with protected machines.

³⁵ Johnson, S. D., Guerette, R. T., & Bowers, K. J. (2012). Crime displacement and diffusion of benefits. *The Oxford handbook of crime prevention*, pp. 337. op cit p. 338

affected by the protective architecture. In the case of TC, this could take (at least) two forms. On the one hand, criminals could use more sophisticated hacking methods. As we discussed, TC increases security, but cannot provide total protection, it is trusted, not secure computing. On the other hand, criminals might resort even more to non-technological forms of cybercrime such as social engineering which by definition is less impacted by technological counter measures – though in the case of TC, the fact that not even the owner has any longer full control over his machine but must trust it blindly, will also act against some forms of social engineering. Should this displacement of methods happen, the “false sense of security” that we discussed above will pose particular dangers and could at least initially increase the incidence of crime. In this case, taking on a compensatory role in crime investigation would be even more pressing.

In the remainder of the chapter, we will further develop this line of argument and show that TC is not just a form of privatization of state functions, not just in the field of pre-crime deterrence and prevention, but ultimately requiring also a role in post-crime investigation. There we will face however a particular difficulty that goes beyond the concerns already raised against privatization of police investigations.³⁶ Shearing and Stenning, in their influential analysis of privatization of policing, argue that:

“The development of private security has been facilitated by fundamental shifts in the nature of property relations. These changes have encouraged the development of a preventative mode of policing consistent with the principles and hopes of nineteenth-century police reformers, but they also suggest that we are moving in the direction of a new disciplinary society and raise fundamental questions with

³⁶ so e.g. from a political science perspective Loader, I. (1997). Thinking Normatively About Private Security. *Journal of Law and Society*, 24(3), pp. 377-394. doi: 10.1111/j.1467-6478.1997.tb00003.x; For the TCI, such a move also carries some reputation risks, given the general low esteem in which private investigators are helped – see e.g. Livingstone, K., & Hart, J. (2003). The Wrong Arm of the Law? Public Images of Private Security. *Policing and Society*, 13(2), pp. 159-170. doi: 10.1080/10439460308027.

respect to sovereignty, justice, and individual liberty now almost entirely unrecognized. In particular, the legal institutions regarding private property operate to enhance the potential threat to individual liberty posed by the development of modern private security.”³⁷

35 years on, their analysis has a new poignancy. The most important change in property relation that came with the Internet enabled knowledge economy – barely at the horizon when Shearing and Stenning were writing – is of course copyright. In the relation between copyright holders, the artistic works and the consumer of art, we find all of the elements they anticipate, in particular an often dramatic clash between regimes designed to protect the property interest and “sovereignty, justice, and individual liberty”. We find this conflict whenever copyright is used to curtail free speech.³⁸ We find it where copyright regimes are used to argue for increased surveillance, such as the Sony DRM fiasco where rightholders tried to install hidden backdoors on the computers of customers,³⁹ or more generally when privacy gives way to copyright protection.⁴⁰ It surfaces in the general debate around DRM regarding “over-protection”, the way in which

³⁷ Shearing, C. D., & Stenning, P. C. (1981). Modern Private Security: Its Growth and Implications. *Crime and Justice*, 3, pp. 193-245.

³⁸ Iconically Nimmer, M. B. (1969). Does copyright abridge the first amendment guarantees of free speech and press? *UCLA L. Rev.*, 17, pp. 1180 - 1204. ; For a more recent analysis from a US perspective see Tushnet, R. (2000). Copyright as a Model for Free Speech Law: What Copyright Has in Common with Anti-Pornography Laws, Campaign Finance Reform, and Telecommunications Regulation. *BCL Rev.*, 42, pp. 1. ; For an analysis from a continental European jurisdiction see Quint, P. E. (1989). Free speech and private law in German constitutional theory. *Md. L. Rev.*, 48, pp. 247.

³⁹ See e.g. Mulligan, D., & Perzanowski, A. K. (2008). The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident. *Berkeley Technology Law Journal*, 22, pp. 1157.

⁴⁰ see e.g. Cameron, A. (2004). Digital Rights Management: Where Copyright and Privacy Collide. *Canadian Privacy Law Review*, pp. 1-9.

it challenges conceptions of justice when imposing abusive on the use of digital objects that the legislator has deemed permissible.⁴¹

Just as with private policing in general, the shift in responsibility for Internet security to private sector organizations “raise fundamental questions with respect to sovereignty, justice, and individual liberty now almost entirely unrecognized”.⁴² In the case of TCI, this is made even more problematic by the fact that due to its origins in DRM, and its support by major Intellectual Property (IP) rightholders, here we have not merely an involvement of a private party to protect the property interests of a third party, rather, “private police” and “property owner” become one and the same person, at least for some crimes and delicts. This needs to be seen also within the context of an increased use of criminal law in copyright protection.⁴³ Together, these developments form a “perfect storm”: a general trend to more and more aggressive use of criminal law to act against copyright violations happens at a time when outsourcing of preventative and investigative policing powers to private sector actors is at a new high - actors who in the case of the TCI are also major IP right holders and have

⁴¹ with further references see Zingales, N. (2012). *Digital Copyright, 'Fair Access' and the Problem of DRM Misuse*. Paper presented at the Boston College Intellectual Property & Technology Forum (pp. 1-36),

⁴² Shearing, C. D., & Stenning, P. C. (1981). Modern Private Security: Its Growth and Implications. *Crime and Justice*, 3, pp. 193-245.

⁴³ See e.g. Manta, I. D. (2011). The Puzzle of Criminal Sanctions for Intellectual Property Infringement. *Harvard Journal of Law and Technology*, 24(2), pp. 2010-2030. ; For a specific enforcement strategy, see Martin, B., & Newhall, J. (2013). Criminal Copyright Enforcement Against Filesharing Services. *NCJL & Tech.*, 15, pp. 101. ; For an overview from the US perspective with a detailed discussion of relevant criminal statutes see Perahia, A., Dwoskin, S., & Goldman, L. (2013). Intellectual Property Crimes. *Am. Crim. L. Rev.*, 50, pp. 1199-1244. On an international level, ACTA, the Anti-counterfeiting trade agreement, contained aspects of criminal law measures that raise wider concerns for the justice system Bitton, M. (2011). Rethinking the Anti-Counterfeiting Trade Agreement's Copyright Criminal Enforcement Measures. *The journal of criminal law and criminology* 102, 1, pp. 67-118.

used in the past technologies very similar to those now suggested for general online security for the protection of their IP rights.

In this chapter, we also want to make a first tentative step to begin the discussion on the consequences for our conception of justice that Shearing and Stenning requested. We will try to show that a further shift of responsibility to post-crime investigation is in a TC environment probably inevitable. It is needed on the one hand to prevent the “displacement problems” discussed above. On the other hand, as we will see in more detail below, TC is also a potential obstacle to traditional, state-centric police investigations, since the very same measures that protect a computer from criminals also protects them against some legitimate (or at least legal) police investigation methods, such as remote forensic analysis. If therefore an increased shift of state powers to TC providers is inevitable, we need to think about the appropriate legal environment that can address the concerns regarding rule of law, justice and individual liberty. For public policing, this has been achieved traditionally (at least in common law jurisdictions) through a careful balance of powers within an adversarial setting – and we will have to investigate also if a private sector environment, with its emphasis on consensual and cooperative relations governed by contract, can replicate these adversarial features. Secondly, the law of evidence has been used to protect the rights of citizens, by e.g. suppressing information that was obtained in violation of procedural rules. Evidence law then became in effect a way to discipline police.⁴⁴ Again, we will have to analyze if a corresponding way to restrain private sector investigative activities can be found. This may also require legislative responses. In the past, private sector actors were in many jurisdictions free of some or most of the constraints faced by police officers when gathering evidence, giving

⁴⁴ So e.g. Wilkey, M. R. (1978). Exclusionary Rule: Why Suppress Valid Evidence, *The Judicature*, 62, pp. 214. ; For a more nuanced view critical of the effectiveness of this way to «reign in» police see Schlesinger, S. R. Ibid. Exclusionary Rule: Have Proponents Proven That It Is a Deterrent to Police, *The*. pp. 404.

additional incentives to police agencies to use the aid of private citizens.⁴⁵ Will TC, if understood as a privatized police function, face similar issues of circumvention of legal rules aimed to protect the citizen from the state? And how great can the responsibilities be that we impose on TC, in exchange for the great powers it wields? To answer these questions, we need first to get a much better idea of how post-crime investigation will be effected in a TC environment. As this side of TC has so far not gained any attention at all - previous studies focused exclusively on the preventative or pre-crime aspect of Internet security - we will try to chart out this new territory first through a couple of examples and analogies to “brick and mortar” investigations.

3.2 Crime investigation in a TC world

Consider the following physical world crime scene scenarios:

⁴⁵ A typical example are rules against entrapment – entrapment by a police officer can render any evidence that is subsequently obtained inadmissible. By contrast, when the entrapment is carried out by a journalist, as e.g. in the News of the world stings in Britain, no such consequences follow. The rationale behind this is that while the evidence is not necessarily unreliable, it is “inappropriate for the state” to generate even more crime than there is already – a concern that does not taint entrapment by private actors in the same way. “It is simply not acceptable that the *state* through its agents should lure its citizens into acts forbidden by law and then seek to prosecute them for doing so. That would be entrapment. That would be a misuse of state power, and an abuse of the process of the courts.” *Looseley and Attorney General's Reference 4* All ER 898-9,

For the US doctrine see e.g. DeFeo, M. A. (1966). Entrapment as a Defense to Criminal Responsibility: Its History, Theory and Application. *USFL Rev.*, 1, pp. 243. ; For the UK see Heydon, J. (1973). The Problems of Entrapment. *The Cambridge Law Journal*, 32(02), pp. 268-286. ; For an application to cybercrime and the investigation of online child abuse see Schafer, B. (2006). The taming of the Sleuth—problems and potential of autonomous agents in crime investigation and prosecution. *International Review of Law, Computers & Technology*, 20(1-2), pp. 63-76. doi: 10.1080/13600860600580959.

3.2.1 Scenario 1

The house of a suspect in a murder inquiry is searched. In a locked room, and a locked chest within that room, a bloodied knife is found that has the DNA of a murder victim on its blade. The room and the chest were securely locked, the owner of the house being the only one with a key that he never left out of his sight. There is no sign that either lock was tampered with, or that anyone other than the owner has ever been in the room.

3.2.2 Scenario 2

As above, but this time there are clear signs that someone had at least tried to force both locks, and there are some signs that someone other than the owner had been in the room and interfered with some of the furniture.

3.2.3 Scenario 3

As in 1 above, but this time, the owner had given a key to the room, but not the chest, to a cleaning agency. They had entered the room several times, but there is no reason to believe they had interest in the chest, or the ability to open it.

3.2.4 Scenario 4

As in 3, but this time, the owner has given copies to both the room and the chest to a security company that patrolled the house regularly and checked all rooms and storage facilities for intruders or explosive devices. The company had outsourced several of its activities to other partner companies, making copies of the key available to them as needed. Their records confirm without doubt that nobody but the owner and employees or agents of the company entered the room between the time of the murder and the police search that seized the knife.

3.2.5 Scenarios close up

What can we say in these four scenarios about the evidential value of the knife? Intuitively, it seems clear that the owner of the house in scenario 1 has some explaining to do. Objects found in his possession can be clearly attributed to him, and there is no obvious explanation for the knife other than that he hid it there.

Equally, it seems intuitively clear that the situation is considerably different in scenario 2. Someone other than the owner probably had access to the room and the chest, and not only that, the methods used to gain entry indicate the third party had criminal intentions.

In scenarios 3 and 4, the situation is much less clear. In scenario 3, much will depend on the details of the case: the trustworthiness of the employees of the cleaning company, their effectiveness in vetting employees, the degree of supervision of employees while they were in the room, and the number of people that could have entered the room. Where someone had the ability to enter the room, the difficulty of opening the chest becomes a factor. Even if the senior managers or directors of the organization did not have any reason to frame the owner, the position of the employees must also be considered.

In scenario 4, the situation is even more complex. On the one hand, the type of manipulation encountered in scenario 2 can be ruled out with much more confidence. This also affects scenario 1, or rather our justification to believe that the specific situation at the heart of an investigation falls into that category. It rules out the possibility that a burglar may have opened the chest (scenario 2), but was so good at his job that he did not leave any traces behind, making it look like scenario 1. On the other hand, a very high degree of trust is now placed with the security company and its employees. While in scenario 2, the owner and unknown third parties may have placed the knife in the chest, in scenario 4 there is a finite number of suspects: the owner and the people he employed for his security.

3.3 What is the relevance of all these for digital evidence?

To understand this, we have to transfer our scenarios into the virtual realm, where the house becomes a PC, the room an individual program running on the PC, and the chest contains the equivalence of individual files created by that program. Scenario 1 now exemplifies how lawyers, and arguably also the police, have often naively thought about the “crime scene computer”. In this view of the world, the owner (or password holder) is the only one with access to its content, and if illegal material is found on such a device, there is at the very least a strong assumption that it is there with the owner’s knowledge and consent. In England, aspects of this view have found their way into the law in the form of an evidential presumption: computers, as a mechanical instrument, are presumed to be in order.

The Law Commission, 11 years after its enactment, recommended total deletion of PACE’s Section 69 stating that it served “no useful purpose”:⁴⁶

We provisionally proposed that section 69 of PACE be repealed without replacement. Without section 69, a common law presumption comes into play:

“In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time. Where a party sought to rely on the presumption, it would not need to lead evidence that the computer was working properly on the occasion in question unless there was evidence that it may not have been – in which case the party would have to prove that it was (beyond reasonable doubt in the case of the prosecution, and on the balance of probabilities in the case of the defence). The principle has been applied to such devices as speedometers and traffic lights, and in the consultation paper we saw no reason why it should not apply to computers.”⁴⁷

⁴⁶ Evidence in criminal proceedings: hearsay and related topics ; a consultation paper (1995).

⁴⁷ The Police and Criminal Evidence Act 1984, c.69 C.F.R. § Part VII - Evidence from computer records (1984).

The provision was repealed finally by s.60 of the Youth Justice and Criminal Evidence Act 1999⁴⁸ and assumes, amongst other things, that programs are not corrupted by third parties.⁴⁹ For many reasons, this picture was always at best an overly simplistic version of reality that relied on numerous highly problematic assumptions, such as how many people are physically located within range of the computer that might have been able to use it if they wanted to; whether it really was protected by passwords; whether the computer was set up to ensure a password had to be put in each time the computer ‘went to sleep’; whether the wi-fi was on or not, and if it was on, whether the security provisions were sufficient enough to prevent a third party from entering the computer from outside.

It is this last aspect, the inability of a third party entering from the outside that concerns us in this chapter. The problems with this specific assumption came to the forefront of the attention of the law when facts similar to scenario 2 were the subject of prosecutions or civil actions. Scenario 2 is broadly the equivalent to the “Trojan defence” as used in the cases of Matt Bandy,⁵⁰ Aaron Caffrey and several others.⁵¹ Caffrey was acquitted by a jury of the charge of unauthorised

⁴⁸ Youth Justice and Criminal Evidence Act 1999 c.23 § c. 27 (1999). It has been a long discussion whether the abolition of s.69 was or was not necessary under the clarifications of the House of Lords and if it achieved its goal. Hoey, A. (1995). Analysis of the Police and Criminal Evidence Act, s.69 - Computer generated evidence *Web Journal of Current Legal Issues*, 5, *ibid.*, Quinn, K. (2001). Computer Evidence in Criminal Proceedings: Farewell to the Ill-Fated s.69 of the Police and Criminal Evidence Act 1984. *Int'l J. Evidence & Proof*, 5, pp. 174 - 187.

⁴⁹ For a critical discussion of this presumption and the often unrealistic assumptions it is based on, see Mason, S. (2010). *Electronic Evidence* (2nd ed.): LexisNexis Butterworth. Chapter 5.

⁵⁰ For an analysis of the Bandy investigation see Mason, S. (Ed.). (2008). *International Electronic Evidence*. London: British Institute of International and Comparative Law. pp. lxxv-lxxxiii.

⁵¹ Brenner, S. W. C., Brian; Henninger, Jef. (2004). The Trojan Horse Defense in Cybercrime Cases. *Santa Clara Computer & High Tech. L.J.*, 21(1), pp. 1-54. , *ibid.* pp.

computer modifications, which were part of a DoS attack against the Port of Houston's computer system in September 2001. Caffrey successfully argued that the evidence against him was planted on his machine by the real attackers, and that his computer had been "zombified" by an unspecified Trojan that gave the attackers control of his PC. Even though a forensic examination of Caffrey's PC found attack tools (our "bloody knife"), it did not find any traces of a Trojan infection (our "scratch marks on the lock"). Nonetheless, the jury accepted the defence argument that a Trojan could wipe itself – blurring the line between our scenario 1 and 2 above. To the extent that Caffrey's argument was convincing, we could never be certain if we are really dealing with an unproblematic scenario 1, or a problematic scenario 2.

Matt Bandy, a minor himself, was prosecuted for the possession of child pornography.⁵² Facing a possible sentence of imprisonment of up to 90 years, the ability of his defence team to show that his computer's protection had been disabled and that his computer had at the time been infected by more than 200 viruses and other malware, including Trojans that could have allowed third party access to his computer, allowed him to enter a plea bargain that resulted in an 18 month suspended sentence. His case illustrates two points that will be relevant later: first, the tendency by users to disable protective software (for instance to "free up" CPU) or to fail to update it is an enabling factor for cybercrime. Second, at least according to the defence team, the police was overly naïve in assuming a "scenario 1" type setting, without testing the necessary assumptions with sufficient rigour.

3-50. Links to several unreported uses of the Trojan defense can be found here: http://www.forensicswiki.org/wiki/Legal_issues

⁵² For an analysis of the Bandy investigation see Mason, S. (Ed.). (2008). *International Electronic Evidence*. London: British Institute of International and Comparative Law. pp. lxxv-lxxxiii.

Malicious outsiders are, however, not the only problem that demonstrates the problematic assumptions underlying scenario 1. Almost every computer user will have granted – knowingly or unknowingly – at one time or another, an automated update agent in the computer the right to obtain access to the Internet and to download updates. In this respect, we are almost always in a “scenario 3” type setting, where the digital equivalent of “domestics”, carry out largely unseen work on our computers all the time. While it is unlikely that anyone working for an anti-virus vendor would hold a grudge against a particular person, and could circumvent the internal auditing and security measures to use that permission to install an illegal program or file on their computer, it is equally true that at any given point in time, a large number of organizations can legitimately make changes on the owner’s computer system.

It is however scenario 4 that is at the centre of this chapter’s section. As with its offline counterpart, it allows us to rule out with a high degree of confidence, evidence planted by malicious third parties as described in scenario 2. On the other hand, every crime scene now becomes potentially tainted should the trust in the third party and its employees be misplaced. Trusted computing can be seen as such a security service, and to understand why it is nonetheless seen as an appealing model by many, we have to discuss in more detail the regulatory and risk assessment environment that gave rise to the TC initiative. Unsophisticated users have long been identified as the weakest link in any strategy to make the Internet more secure against cyber attacks. It is their computers that provide the raw material for botnets, the main tool for denial of service attacks, when they forget or fail to update their system with patches, let their anti-virus software expire or forget to update the virus signatures.⁵³ Once sufficiently large, these

⁵³ Bayer, U., Habibi, I., Balzarotti, D., Kirida, E., & Kruegel, C. (2009). *A view on current malware behaviors*. Paper presented at the LEET'09: Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more, Boston, MA, USA. http://www.eurecom.fr/people/vs_bayer.en.htm,

botnets in turn can also threaten the systems of more resourceful and sophisticated users, including servers that are crucial for the very functioning of the Internet.⁵⁴ An apparently obvious solution from the point of view of the technicians is to remove the responsibility of providing security for the computer from the general user, and assign it to a third party. This in turn creates several legal issues for the employees of these third parties, and several of them are discussed in more detail below. For instance, it is necessary to consider if exclusionary rules against illegal searches by the police are applicable by analogy, or if a third party employee finds incriminating material by accident, what the liability is if he chooses not to report it. For obvious reasons, any third party entering into a contract to perform such a service will need certain rights to obtain access to a computer or system to perform the contract effectively. As noted above, whether or not this is acceptable becomes a question of trust – there

Henderson, S. E., & Yarbrough, M. E. (2002). Frontiers of Law: The Internet and Cyberspace: Suing the Insecure?: A Duty of Care in Cyberspace. *New Mexico Law Review*, 32(11). It should be noted at this point that these solutions are themselves far from sufficient to provide perfect security – for a discussion, see e.g. Bilar, D. (2009). Known knowns, known unknowns and unknown unknowns: anti-virus issues, malicious software and internet attacks for non-technical audiences. *Digital Evidence & Electronic Signature Law Review*, 6, pp. 123 - 131. . However, the experience with available security measures shows that *no* technological solution, however sophisticated, can be expected to work if it relies ultimately on active user involvement and allow the override of automated protection mechanisms by the owner of the computer.

⁵⁴ While state agencies that should know better, have found themselves victims of hacking attacks, the damage in these cases was typically restricted to the computer system in question. With botnets, on the other hand, the victim is not just the user who lets his computer become infected, but also third parties and ultimately, the very functioning of the Internet can become threatened. It is this third party effect that changes the legal and practical landscape, and goes some way in explaining why the solution to sustainable Internet security is seen mainly in addressing the large number of relatively unsophisticated users. From a legal perspective, it is this involvement of parties other than the immediate victim that we think creates unique legal challenges.

is nobody a king or president has to trust more than his bodyguards, because they tend to be the only people allowed to carry weapons in her presence – but as history illustrates, such trust can be misplaced.

However, if the future of Internet security includes a shift of responsibility (and control) away from ordinary users to professional organizations, a number of issues need to be considered, such as:

- The conditions by which it can be considered to be rational to trust the security providers.
- When and if potential interference with the digital crime scene might become an issue.
- How the criminal law and the law of evidence should respond to such a shift in responsibility, especially if it is the private sector, as opposed to the state, that takes on the role of securing (parts of) the Internet infrastructure.
- Whether it is necessary to adjust laws that were written mainly at a time when policing was the epitome of sovereign authority.

To repeat at this point a caveat from Chapter 2: Trusted Computing serves to illustrate that the analysis discussed in this thesis are not mere speculation, but it should be kept in mind that the main interest is in the *type* of response to cyber crime, not the necessarily the TCI alone.

3.4 Consequences for the regulatory environment

As we've seen above, from the beginning, TC has been controversial within the academic and scientific world, the computer industry, and the end-user community.⁵⁵ The proponents of TC suggest that TC promises to provide four

⁵⁵ For an extensive discussion on the controversy and the reasons behind the controversial nature of TC see: Flick, C. (2004). *The Controversy over Trusted Computing*. (Bachelor of Science), The University of Sydney, Sydney. Retrieved from http://liedra.net/misc/Controversy_Over_Trusted_Computing.pdf

crucial advantages: reliability, security, privacy and business integrity. These, it is claimed, when taken together, guarantee a system that will be available when needed; will resist any attack by protecting the system and the data; will provide privacy to the user, and finally it will provide businesses with the ability to interact efficiently and safely with their customers. Additionally, TC should provide protection from viruses, because a check will be applied to all files trying to 'enter' the system, as well as the implementation of new applications aiming at providing greater protection. As we saw, critics of TC consider that restrictions will be imposed on users, because the owner of a PC does not have root access to cryptographic keys, and therefore users will no longer be in control of their own computer.⁵⁶ The validity of this argument is also confirmed by proponents of TC, but they claim that this is a feature, not an error, as it will restrict issues such as *user override*.⁵⁷ As noted above, the user has the ability to disable some of the safety features and where such features are rendered inoperative, the computer becomes open to cyber attack. The proponents' suggestion to rebalance the degree, by which users can override such features that are in place by the manufacturer and still remain trustworthy, is based on this exact reason.⁵⁸ Consequently, the user will no longer be in full control of their own computer because they are not permitted to obtain access to the private keys that purport to make the computer trustworthy, thus it is asserted that trust is based on what

⁵⁶ The reader can have an inside on the critics on TC considering the restrictions imposed on users: Green, L. (2002). *Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers. Presented in DEFCON 10.* from <http://www.cypherpunks.to/TCPADEFCON10.pdf>, Stallman, R. (2002). *Can you trust your computer?*, *NewsForge-The Online Newspaper for Linux and OpenSource*. Retrieved from <http://www.newsforge.com/business/02/10/21/1449250.shtml?tid=19>

⁵⁷ See Yung's view on the user overriding issue: Yung, M. (2003). *Trusted Computing Platforms: The Good, the Bad, and the Ugly*. Paper presented at the 7th International Conference, FC 2003, Guadeloupe, French West Indies (pp. 250-254), Springer.

⁵⁸ *ibid.* p.252

is promoted as being a 'well designed machine', not badly educated humans. This is normally analysed as a key feature of the "pre-crime" aspect of TC, its ability to enhance security. But our discussions show that it is just as relevant for post-crime and crime investigation purposes. The PC in this case becomes the crime scene. TC secures the crime scene against its human owner, be he victim or a suspect. It prevents him from interfering with at least some aspects of the evidence, either accidentally or intentionally. It may even prevent some types of "anti-forensic" software from running. Advanced anti-forensic software will not only delete files, it will alter the basic configuration of the computer so that no evidence remains that a deletion was carried out – this will in some cases change "integrity values" of the computer the way a rootkit does.⁵⁹ TC prevents however rootkits from running, and therefore by implication also some anti-forensic tools.

Richard Stallman, the founder of the Free Software Foundation and creator of the GNU Project, is one of the harshest opponents of TC. Stallman considers that 'treacherous computing' is a more accurate name for TC. His concern was the possibility content providers and computer companies to make computers obey them. It is possible for users' data to be edited and deleted remotely, without any notification to the user or owner of the computer.⁶⁰ However, our discussion indicates another way a TC computer can be treacherous – just as in the Tell-Tale Heart by Edgar Allan Poe, your computer keeps not only track of you, but now,

⁵⁹ on the relation between rootkits and anti-forensics see in particular Blunden, B. (2013). *Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System*: Jones & Bartlett Publishers.; For an overview of anti-forensics in general, the reader is referred to Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*, 3, pp. 44-49. doi: 10.1016/j.diin.2006.06.005. And also Garfinkel, S. (2007). *Anti-forensics: Techniques, detection and countermeasures*. Paper presented at the 2nd International Conference on i-Warfare and Security (pp. 77),

⁶⁰ Stallman, R. (2002). Can you trust your computer?, *NewsForge-The Online Newspaper for Linux and OpenSource*. Retrieved from <http://www.newsforge.com/business/02/10/21/1449250.shtml?tid=19>

there is nothing you can do about it. At this point, it is important to remember that there can be legitimate reasons to securely delete files in a way that makes them forensically irretrievable, and without even a trace of the deletion - selling a machine that carried sensitive information on the second hand market for instance.

TC thus poses a two-pronged dilemma in a forensic context: it prevents (almost) everybody from altering certain configurations on a computer, not just malicious third parties but also the owner – giving the computer evidence potentially much higher evidential value. At the same time, as per Stallman, it does open up the possibility to alter or add to that data by the TC provider as trusted third party. Or, translated back into the real world, not only do you have to give access to your house to someone who can plant a bloodied knife there, once the knife is in your house, there is no way you can get rid of it again. To permit this to anybody requires a considerable amount of trust in the sociological sense- trust that as we argued in the preceding chapter the TCI is unlikely to command.

In the context of this chapter, this possibility is central to scenario 4 above:

- The extent that a TC system provides for the Trojan defence, when remote access to files by a third party is a necessary prerequisite for the system to fulfil its function, and
- The legal duties, if any, that should be imposed on TC providers to maintain the integrity of “digital crime scenes”.

Programs that use TC when installed will be able to continually download new authorization rules through the Internet and levy those rules automatically on the computer. In such circumstances, it is claimed that computers may apply the new instructions that have been downloaded without the user being made aware of the new instructions, to such a degree that a user will no longer be able

to fully interact with his own computer.⁶¹ This shows that in the context of computer forensics and crime investigation, the Digital Rights Management (DRM) heritage of TC becomes a potential issue. Digital Rights Management, which was one of the original aim for developing TC technology, will be used for e-mail, documents and multimedia which can disappear or remain unreadable on certain computers, thus altering programs and files – with obvious consequences when the evidential value of such files and programs have to be evaluated. A practical application of this problem could be for instance when the police tries to determine if known child pornographic images are or have been stored on a machine. Known images are given a hash value as unique identifier and compared to the hashed files on the suspect computer.⁶² Manipulation of hash values by a third party could then incriminate an innocent user.

3.5 Legal responsibility in an age of TC

A significant aim of this chapter is to argue that if the Internet is to be made more trustworthy through technological rather than legal solutions, the provider of that security will need to obtain access to user's hard drives, and have the ability to extract information and to reconfigure the software on the machine. TC can be seen as a first step in this direction. In this analysis, in conceptual terms the TC approach amounts to a part privatization of what is, in the off-line world, an essential state function. Safety becomes a commodity, and its exchange is primarily governed by contract. Contract, and possibly the law of tort, has

⁶¹ Anderson, R. (2003a). Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA – Version 1.1. (2003). <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>, Stallman, R. (2002). Can you trust your computer?, *NewsForge-The Online Newspaper for Linux and OpenSource*. Retrieved from <http://www.newsforge.com/business/02/10/21/1449250.shtml?tid=19>

⁶² McIntyre, T. (2012). Child abuse images and cleanfeeds: Assessing Internet blocking systems. *RESEARCH HANDBOOK ON GOVERNANCE OF THE INTERNET*, Ian Brown, ed., Edward Elgar, pp. 277-309. p. 279

consequently been seen often as the obvious solution to the regulatory issues that TC raises and we will return to this avenue in the next chapter. However, this perspective leaves the re-balancing act between the customer or computer user and the software company to a mix of market forces, competition law and good faith interpretation of contractual terms that cannot adequately address the interest of third parties in the security of the Internet, and in particular fails to address the interest of the state and law enforcement agencies.

To the extent that scenario 4 is a realistic depiction of the new realities of investigative work in a trusted computing environment, several choices become available. One is to do nothing. In this case, the issue of access is similar to scenario 3. Since no legal challenge against the validity of digital evidence on the basis of an update agent or similar software on a computer that grants other organization access to it has been made to date, this could be considered as a mere theoretical concern. The risk is that should such a case ever arise, a large number of convictions could suddenly become unreliable in retrospect. Alternatively, if our analysis of TC as privatization of a core state function is considered seriously, it is necessary to create a legal duty on TC providers to ensure that any interaction with individual computers does not affect the integrity of the data for evidential purposes. Just as the police are required to observe the requirements of the chain of custody, and to document the chain appropriately, TC providers could be required to develop protocols with the explicit requirement of legal admissibility. This option would also highlight the potential privacy issues raised by trusted computing, making the quasi-policing role of TC more visible. This, arguably, could act as a deterrent for the uptake of the technology, but this assumes that consumers will be left with a choice in the matter.

A related issue is the use of forensic diagnostic tools. One of the problems with TC that is frequently raised in the literature is the possibility that it will not allow certain programs, especially open source programs, to run on a computer.

This could at least theoretically prevent commonly used forensic tools such as Encase running on a suspect's computer.⁶³ Any attempt to deal with this problem generically may be more difficult than it seems, given the dual nature of many hacking tools – the very software that a system administrator uses to ensure safe working of a computer, or that is needed for a forensic analysis, are also capable, in the wrong hands, to be used for malicious purposes – the difference between hacking and auditing or administration tools lies not in the code, but the use it is put to. This became visible in Germany's much criticized attempt to prohibit the possession of software that can be used for hacking purposes, and led one journalist to add as a by-line: "Will the last security expert to leave Germany turn off the lights?".⁶⁴ By the same token, many of the functions necessary to perform a forensic investigation on a computer – which by definition often means to 'force' the suspect computer to reveal its secrets by, for example, breaking passwords or searching for stenography – will look for all intents and purposes for the TC system, which is similar to the very type of process it is designed to prevent from running.

This in turn leads to another problem: *whether it is desirable in principle that TC provides the purported level of security from attacks.* At first glance this question might seem absurd, but it is necessary to understand that the entire field of Internet security is based on a fundamental paradox: *what works for the victim also works for the criminal, and what works for the criminal can also work for the police.* This was epitomized in the debate around secure encryption in the late 1990s: while strong encryption protects honest citizen against data thieves and

⁶³ Mason, S. (2005). Trusted computing and forensic investigations. *Digital Investigation*, 2(3), pp. 189-192.

⁶⁴ Leyden, J. (2007, 13/8/2007). Germany enacts 'anti-hacker' law - Will the last security expert to leave Germany turn off the lights? *The Register, Security*. Retrieved 19/7/2011, 2011, from http://www.theregister.co.uk/2007/08/13/german_anti-hacker_law/print.html

other criminals by protecting sensitive communication such as bank details, it also protects criminals, their clandestine communications and on-line money laundering activities.⁶⁵ Complex compromise solutions had to be designed, which typically combine restrictions on some technologies with legal requirements to hand over keys as part of an investigation.⁶⁶ One of the potentially strongest selling points for TC and proof of its potential to enhance privacy is that a number of oppressive regimes such as China and Russia prohibit their citizens from importing the related TPM technology.⁶⁷ However, the technology is neutral. That TC is considered to be suspicious by regimes that prefer its citizens to not discuss politics without the ability of the police to eavesdrop should also raise concerns for governments worried about organized on-line crime.

It is also not an option to provide the public with a 'weak' form of TC that remains vulnerable to being penetrated by the police or other state agencies. As indicated above, organized criminals, often with a background in the disintegrating security agencies of the Eastern European block, can match those of official agencies. More plausible is the idea that the state will impose requirement to leave sufficient weak spots so that when authorized by a court, the TC provider is in a position to obtain access to the data. This is very similar to

-
- ⁶⁵ Friedman, D. (1996). A World of Strong Privacy: Promises and Perils of Encryption. *Social Philosophy and Policy*, 13, pp. 212-228. doi: 10.1017/S0265052500003526 ; for examples of cases that have been prosecuted in relation to encrypted materials, see Mason, S. (2010). *Electronic Evidence* (2nd ed.): LexisNexis Butterworth., 1.34 and 10.228 – 10.250.
- ⁶⁶ Barth, R. C., & Smith, C. N. (1997). International Regulation of Encryption: technology will drive policy. In C. N. Brian Kahin (Ed.), *Borders in Cyberspace: Information Policy and the Global Information Infrastructure* (pp. 283-300). Cambridge: MIT.
- ⁶⁷ Microsoft. (2008, October 2008). Deployment Planning for BitLocker Drive Encryption for Windows Vista. from <https://technet.microsoft.com/en-us/library/dd126731.aspx>; See for China and the «HP case» Xia Yu and Matthew Murphy, M. G. (2011). The Regulation of Encryption Products in China. *Bloomberg Law Reports - Asia Pacific*, 4(2), pp. 1-6.

the provision of the Regulation of Investigatory Powers Act 2000 (RIPA) in the UK that creates obligations to reveal the password to encryption keys. In such an environment, TC providers face a stark choice: promise a lot, and risk liability when things fail, or make it clear in the contract that TC cannot guarantee safety – which would risk to undermine acceptance and take-up by users. It is noteworthy to mention at this point that Windows Vista, Windows 7, 8 and 10 are already using the Trusted Platform Module to facilitate the BitLocker Drive Encryption. It is undoubtedly the case that users are not aware of this, but even if they were aware, they would not be able to understand its features.

Even more directly relevant in considering police investigations in a TC environment, is that some investigative methods used by the police use the same technologies that criminal hackers use to exploit computer vulnerabilities. In Germany, the ‘Federal Trojan’ was a piece of software that opened back doors in the computers of crime suspects, to permit clandestine monitoring of their activities.⁶⁸ Even more controversially, the recent attack on Iran’s computer infrastructure for the nuclear industry was very likely the result of actions by a ‘friendly’ state power (friendly, that is, to the US and UK as main sponsors of TC) using a similar, Trojan based approach.⁶⁹ A technological solution such as TC that cannot distinguish in principle between good governmental Trojans and bad criminal Trojans and prevents both from functioning, creates potential for conflicts, both technological and legal, that need to be further explored. One answer, for instance, could be to create a further responsibility for the TC developers, that is, the duty to compromise their own product under certain circumstances. This in turn would require a set of legal instruments, on the one

⁶⁸ Abel, W., & Schafer, B. (2009). The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems - a case report on BVerfG, NJW 2008, 822. *SCRIPTed*, 6(1), pp. 106-123. doi: 10.2966/scrip.060109.106

⁶⁹ Falliere, N., Murchu, L. O., & Chien, E. (2011). W32.Stuxnet Dossier *Security Response* (1.4 ed., pp. 69). Cupertino, CA: Symantec Corporation.

hand to compel them to cooperate, and on the other a qualified privilege for any harm that might arise from such cooperation. Decisions also would have to be taken regarding the procedural requirements to be used to compel TC providers to cooperate with criminal investigations, in particular the degree (if any) of judicial oversight and warrant requirements. Hence, balancing the legal obligations, privileges, immunities and burdens in a way that is at the same time equitable to consumers and software vendors requires considerably more complex responses by the law than a change to the liability regime that the House of Lords envisaged.⁷⁰

A final issue arises from the DRM heritage of TC, and also how issues traditionally discussed in terms of privacy protection can take a new dimension in the context of criminal law and criminal investigations. As noted above, it seems that the TC providers can obtain sufficient information from the computers of TC users not only to prevent unauthorized programs or files from running (for instance to prevent the playing of an illegal copy of a music track), but also the possibility of removing programs. Given such power, it is possible to infer that the TC provider would at least have constructive knowledge about the content of the user's computer. Increasingly, legal systems create an obligation to inform the police if they have knowledge of illegal activity.

For instance, the Anti-Terrorism, Crime and Security Act 2001 in the United Kingdom makes it an offence to fail to disclose information to the police that would be "of material assistance in preventing or leading to the arrest of persons engaged in the commission of an act of terrorism".⁷¹ In Germany, even broader

⁷⁰ House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm>.

⁷¹ See section 117 Information about acts of terrorism in Anti-terrorism, Crime and Security Act 2001 c. 24 § c. 24 (2001).

duties exist to bring certain crimes to the attention of the authorities. Article 138 of the Criminal Code (StGB) mandates that failing to disclose information about a large number of offences, from terrorism and treason to murder, kidnap and dangerous interference with the railway, carries a sentence of up to five years.⁷² It is therefore of some relevance to decide what type of knowledge is required by these criminal offences, if fully automated processes that permit the identification and retrieval of information count as 'knowledge' for the purpose of these laws (and if not, if they should be included), and indeed how much actual knowledge TC providers could or should have about the content of their customers' hard drive. It could be possible for instance, to look for the hash value of movie clips known to have content of abusive images of children, in addition to clips that are merely illegally downloaded.⁷³

Similar arguments have been made – and in our opinion never satisfactorily resolved at least in the US – regarding constructive knowledge and possession of illegal content in the case of Internet intermediaries such as search engines or online platforms. Google is technically in possession of illegal images when their web crawlers create cached versions of the web sites they visited, stored on Google servers. To build up their index, the search engine's robots constantly crawl the Web, taking "snapshots" of every Web page they find accessible (i.e. not encrypted, or with a robot exclusion clause in its html code). These copies, also called "cached" copies are then stored on the search engine's server.⁷⁴ For the US, there is a patchwork of exemptions that indicate recognition of the problems for intermediaries that this can cause. The most famous one are the safe harbour rules under the DMCA, the Digital Millennium Copyright Act, which is codified in

⁷² Criminal Code (Strafgesetzbuch, StGB) § 138 (1998).

⁷³ US v. Cartier, No. No. 07-3222, 543 442 (Court of Appeals, 8th Circuit 2008).

⁷⁴ For more of the technical details and possible legal ramifications see Peguera, M. (2008). When the cached link is the weakest link: search engine caches under the Digital Millennium Copyright Act. pp. 1102-1157. , especially p. 1106-1108

sections across 17 U.S.C.⁷⁵ It exempts intermediaries from civil liability under copyright law provided they “cooperate” with legitimate takedown and notice requests. However, this is a specific exemption for copyright purposes and here arguably only for civil liability. In addition, 47 U.S. Code § 230 for instance creates a “good Samaritan” exemption for intermediaries that “do their best” in shielding the public from illegal or obscene material by using filters for blocking and screening, to ensure that this does not suddenly make them “publishers” of the material that nonetheless gets by their filters. It also exempts them from *civil* liability. However, 47 U.S.C. 230(e) reaffirms that this does not prevent *criminal* liability, and as 18 U.S.C. 110(4)(A) makes it a criminal offence to “knowingly possesses one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction [...] of a minor engaging in sexually explicit conduct”, it could at least be argued that the search engines commit a crime under that provision when their web crawlers create copies for the purpose of indexing.⁷⁶ Finally, Section 230 of the Communications Decency Act creates an exemption for intermediaries for certain type of speech related offences.⁷⁷

⁷⁵ The Digital Millennium Copyright Act of 1998 (1998). Pub. L. No. 105-304, 112 Stat. 2860 (1998). For a discussion see e.g. Scott, M. (2005). Safe Harbors Under the Digital Millennium Copyright Act. *NYUJ Legis. & Pub. Pol'y*, 9, pp. 99. and Holland, H. B. (2007). In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism. *Kansas Law Review*, 56(101), pp. 101-137. For a comparison to the European approach, see Peguera, M. (2009). The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems. *Columbia Journal of Law & the Arts*, 32, pp. 481.

⁷⁶ So argued forcefully by Byars, B., O’Keefe, T., & Clement, T. (2008). *Google, Inc.: Procurer, Possessor, Distributor, Aider and Abettor in Child Pornography*. Paper presented at the Forum on Public Policy: A Journal of the Oxford Round Table (pp. 1-7), Forum on Public Policy.

⁷⁷ See e.g. Ardia, D. S. (2010). Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act. *Loyola of Los Angeles Law Review*, 43(2), pp. 373-506.

What does this mean for TC? As we have argued, TC requires that the computer owner trusts the TC provider with some information at least – potentially giving them considerable access rights. Unlike in the examples of child pornography or copyrighted material discussed above, the TC provider does not become the owner of this information; it continues to reside solely on the user’s computer. Laws that proscribe possession therefore are – probably⁷⁸ – not affected. However, the information gathered will be sufficient to alert the TC provider of some forms of illegal activity, including copyright infringements or attempted participation in a Denial of Service attack. Where criminal laws make it an offence not to report knowledge of a crime, this should then create criminal liability for that specific offence – the above cited laws either only shield from civil liability, or are “offence specific”.

A possible argument in defense of TC providers could be that the relevant offences typically require “active knowledge”, not just a generic knowledge that “something” illegal is happening, somewhere. Since as we have seen in chapter 2, the information acquisition and processing that is required for TC is with necessity carried out automatically and by machines (“trust machines, not humans”), the argument could be made that the TC provider never acquires the relevant “knowledge”. This would certainly fit to the policy rationale that we find in the DMCA safe harbor provisions and the Intermediary Immunity provisions under Section 230 of the Communications Decency Act.⁷⁹ Google “knows” abstractly that it must have made copies of copyrighted material, and that some of its search results direct users to infringing sites. But unless a specific site is

⁷⁸ Depending on the configuration of the TC approach, some data may reside on the TC provider’s service, but from the details available to us, this will not normally be any “substantive” content – the TC provider can see from the hash files and the certification what types of file are on a machine, but not the files itself.

⁷⁹ The Digital Millennium Copyright Act of 1998 (1998). and Communications Decency Act of 1996, , Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996) C.F.R. (1996).

brought to its attention, the relevant “knowledge” is too diffuse to trigger legal responsibilities. Similarly, we know a priori that attacks against computers take place, and that therefore the TC provider will have “somewhere” on its system information that indicates illegal activities. But as long as no human identifies a specific computer or network, this does not amount to “actual knowledge”, at least not for the purpose of criminal law.⁸⁰ However, there are good policy and legal reasons not to make this defense available. From a policy point of view, it would enhance the “responsibility gap” that has already been identified as a more and more pressing problem in a world where we outsource more activities to machines.⁸¹ This would create dangerous incentives to avoid legal responsibility by using automated processes, something which becomes even easier to accomplish. Secondly, it would also raise systematic-legal problems. If automated data processing is decoupled from “knowledge”, then many automated functions that are crucial for e-commerce and the Internet society, are once again called into question – for instance, automated contracting through autonomous agents could result in void contracts, because there too, a degree of “knowledge” is required as a matter of law.⁸²

⁸⁰ For a more systematic discussion of different types of knowledge in criminal law than can be carried out here, see Edwards, J. L. J. (1954). The criminal degrees of knowledge *. *Modern Law Review*, 17(4), pp. 293-314. doi: 10.1111/j.1468-2230.1954.tb02157.x.

⁸¹ The term “responsibility gap” was coined by Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, 6(3), pp. 175-183. doi: 10.1007/s10676-004-3422-1; While he focusses on learning machines, the same problem arises also in other forms of AI – for applications close to those discussed in this thesis, , see e.g. Johnson, D. G., & Miller, K. W. (2006). *A dialogue on responsibility, moral agency, and IT systems*. Paper presented at the Proceedings of the 2006 ACM symposium on Applied computing (pp. 272-276), ACM.

⁸² A discussion of this problem would go beyond the scope of the thesis. For a discussion on the mental element in automated contracting, a discussion that goes back to the late 1980s, the reader is referred to Weitzenböck, E. M. (2001). Electronic agents and

In the US at least, and in line with its “fragmented” approach to regulate intermediary liability, special laws may be required to ensure that TC providers are not overburdened by reporting duties.

In Europe, we have a more systematic approach in the e-commerce Directive, which grants more generic exemptions:

First, we find in Article 12 a general “mere conduit” safe harbor provision:

Mere conduit

Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

- a) does not initiate the transmission;
- b) does not select the receiver of the transmission; and
- c) does not select or modify the information contained in the transmission.⁸³

Unlike in the US provisions, both civil and criminal liability are excluded. However, two legal issues remain. The first and most obvious is if TC providers are providing an “information society service” of the kind detailed in the Directive. As the interviews with some developers, to be discussed in more detail in the next chapter show, this is probably not how the TCI sees itself – they are selling “goods”, functionality embedded in hardware. However, our discussion in the previous chapter painted a rather different picture. TC at the very least makes transmission in a communication network safer, by interacting directly with the

the formation of contracts. *International Journal of Law and Information Technology*, 9(3), pp. 204-234. .

⁸³ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (2000). Section 4: Liability of intermediary service providers Article 12

communication process. Its ultimate aim is to build up “from the ground” a more secure internet – that part of this activity takes place on the computers of individual users, doesn’t change the picture. Furthermore, as we discussed, to create the necessary “herd immunity”, being “TC certified”, will become a pre-requisite for a computer to participate in the communication with other machines. This strongly indicates in our view that TC can be seen as providing “communication services”. While one could therefore argue that TC falls under the exemption of Article 10,⁸⁴ this last point also indicates a problem: TC decides which computers are allowed to communicate with other computers – and this looks perilously close to an activity under provision (c) of Article 10, which would deprive the TC provider from its protection.

Of particular relevance is furthermore Article 15:

Article 15

No general obligation to monitor

- 1) Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
- 2) Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.⁸⁵

Taken together, (1) and (2) mean that an Information Society Service Provider (ISSP) must not be compelled to actively monitor the information in their control, but *if* they obtain knowledge, it is permissible to obligate them to disclose the information, either pro-actively or as a result of a warrant or similar

⁸⁴ *ibid.* Article 10 on the information to be provided.

⁸⁵ *ibid.* Article 15

request. In light of the discussion about “active knowledge” above, we can see how this works for Google, YouTube or Twitter. All of these services, have to process data which “could” provide evidence of criminal activity, but as this is not the core of their activity, they can’t be compelled to take on this task *in addition*. Google is not looking actively for illegal material, we just know a priori that it will stumble across some. But if a specific suspicion is raised to them, this changes the nature of their knowledge and they then can be compelled to cooperate in this specific case. But with TC, the situation is fundamentally different. “Looking for trouble” is in a way what they are all about, identifying unsafe machines or communications, and blocking them. For them, identifying (also certain types of) illegal activity is part of their core business, as a “privatized police” as we argued above. Therefore, Article 15 (2) alternates point (1) which will be the norm rather than the exception, at the very least permitting member states to request active reporting of signs for illegal activity, if this is not already covered by the types of criminal law that we mentioned above.

To summarize: In our analysis, TC acts as a “privatized police”. This means they also get possession of information that is normally either unlawful for an ordinary citizen to have, or at least triggers reporting duties. This could expose TC to substantial criminal liability. Special privileges may have to be created by law to exempt them from an overly onerous reporting requirement, especially as this would make them even more visible as part of a surveillance operation on behalf of the state and in potential conflict with their customers. We identified so far two possible avenues to achieve this: bringing them explicitly under the umbrella created for ISSPs (which might mean to broaden the scope of this category) and give them the rights, privileges *and* duties of ISSPs, including potentially data retention duties to be discussed below. This seems in line in particular with the EU approach. Or create sector and offence specific new and tailor made exemptions, for “internet security providers”. This would be more in line with the US approach and have the advantage that any exemption can be

“tailor made” – as our discussion has shown, they are sufficiently different from Google or YouTube to make the EU directive a less than perfect fit. Further below, we will look also briefly at a third option that takes the idea of a “privatised police” more serious and extends rules to them that other professions that took on security functions are already subject to. Rather than seeing TC as a form of ISSP, in this approach they would be treated more like public notaries or volunteer police officers. First though, we will explore in some more depth the additional duties that could come from treating TC providers more like ISSPs.

3.6 A case study: Retention and Preservation of data

Collection of evidence from computers, networks, digital storage devices, servers and personal devices has been a standard practice in digital forensics. As stated earlier, TC originated as a form of DRM technology with the intent to control the use of digital content on user’s computer and prevent unauthorized and illegal use of the material. The data retained from users will be held in TC provider’s databases thus raising - amongst others - legal, privacy and forensics investigations concerns. There are two sides of the coin to be considered here – the duty to retain and preserve data for forensic purposes as long as required by law, and not to retain it any longer than permitted by data protection law. To gauge what exactly one’s duties under these conflicting provisions are, requires for entities that are engaged with the Internet (which may or may not be a wider group of ISSPs) to know exactly what type of entity they are for legal purposes – and as we have seen, for TC providers as “privatized police”, this may be more difficult to determine than one may have thought.

The EU Directive on data retention 2006/24/EC⁸⁶ had been introduced in an attempt to give the authorities the ability to cope with organized crime and

⁸⁶ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the

terrorism. Recently, early in April 2014 the European Court of Justice however, annulled the provision as being in irreconcilable conflict with the fundamental rights of privacy and protection of personal data⁸⁷ (since the restraints already in place are not enough to ensure that only the necessary information is stored and used without prior notification to the subscriber).⁸⁸ The Court emphasized the impermissibility of blanket retention of data without specific justification, as well as the possible abuse of the data that are not certain to be destroyed at the end of the retention period and concluded that a reform of their former decision should emerge; adding more pressure on the lawmakers to deliver vigorous data protection measures.⁸⁹

provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (2006).

- ⁸⁷ Court of Justice of the European Union. (2014). The Court of Justice declares the Data Retention Directive to be invalid [Press release]. Retrieved from <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>. CJEU Judgement in Cases C-293/12 and 594/12 for an academic analysis see Cole, M., & Boehm, F. (2014). Data Retention after the Judgement of the Court of Justice of the European Union. *University of Luxembourg*, pp. 1-107.
- ⁸⁸ Bautista, C. B. (2014, April 8, 2014). EU court dismantles law requiring phone companies to retain customer data, *Digital Trends*. Retrieved from <http://www.digitaltrends.com/mobile/eu-court-ruling-against-data-retention/#!DTzyQ>, BBC News. (2014). Top EU court rejects EU-wide data retention law, *BBC News*. Retrieved from <http://www.bbc.com/news/world-europe-26935096>, Breidhardt, A., & Strupczewski, J. (Apr 8, 2014). EU court rejects requirement to keep data of telecom users, *Reuters*. Retrieved from <http://www.reuters.com/article/2014/04/08/us-eu-data-ruling-idUSBREA370F020140408>, White, A. (2014, Apr 8, 2014). EU Data-Retention Law Tramples on Privacy, Top Court Says, *Bloomberg*. Retrieved from <http://www.bloomberg.com/news/2014-04-08/eu-data-retention-law-tramples-on-privacy-top-court-says.html>
- ⁸⁹ Bautista, C. B. (2014, April 8, 2014). EU court dismantles law requiring phone companies to retain customer data, *Digital Trends*. Retrieved from <http://www.digitaltrends.com/mobile/eu-court-ruling-against-data-retention/#!DTzyQ>, White, A. (2014, Apr 8, 2014). EU Data-Retention Law Tramples on Privacy, Top Court Says, *Bloomberg*. Retrieved from

However, the UK reacted to the decision by enacting emergency legislation (Data Retention and Investigatory Powers Act 2014 “DRIP”) which had for the time being (and subject to further legal challenges) kept the data retention regime in place for the UK.⁹⁰ These changes in the law create obvious uncertainty, which is a problem for ISSPs in general,⁹¹ but will affect TC in particular – as we argued above; here certain types of data collection and retention are in a way “core” to the business that aren’t for other actors in the digital economy.

ISPs in Europe have thus been until recently under a legal duty to retain data and to ensure the safety of those data for investigation, detection and prosecution of serious crime. Retention period, archival policies, categories of data, storage means, access control and encryption rules have been delineated regarding ISPs through the Directive 2006/24/EC of the European Parliament.⁹² In the US, no general data retention duty exists. Attempts have been made to introduce such duties, most notably the “Internet Stopping Adults Facilitating the Exploitation of Today’s Youth” (SAFETY) Act 2009 which was introduced in 2009 by Representative Lamar Smith, and which would have obligated providers of “electronic communication or remote computing services” to “retain for a period of at least two years all records or other information pertaining to the identity of

<http://www.bloomberg.com/news/2014-04-08/eu-data-retention-law-tramples-on-privacy-top-court-says.html>

⁹⁰ see also for a comparative analysis Kühling, J., & Heitzer, S. (2015). Returning through the National Back Door? The future of data retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere. *European law review*, 2, pp. 263-278.

⁹¹ Tracol, X. (2014). Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 30(6), pp. 736-746. doi: 10.1016/j.clsr.2014.09.008

⁹² Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (2006).

a user of a temporarily assigned network address the service assigns to that user.”⁹³

However, while the US is lacking a legal data retention duty, its police and security services have been highly successful in accessing data that ISPs keep voluntarily and/or for their own internal benefits. The Stored Communications Act⁹⁴ in conjunction with the PATRIOT Act regulates for instance how access to communication data can be gained through the use of national security letters (NSL), a form of administrative subpoena, by the Federal Bureau of Investigation.⁹⁵ In addition to the highly controversial and highly secretive NSLs, there are other procedures such as SCA warrants that enable access to communication data by law enforcement agencies, subject to warrant requirements.⁹⁶

⁹³ GovTrack.us. (2009). H.R. 1076 (111th): Internet Stopping Adults Facilitating the Exploitation of Today’s Youth (SAFETY) Act of 2009. *Bills*. Retrieved 22/8/2015, 2015, from <https://www.govtrack.us/congress/bills/111/hr1076>, from a position sympathetic to the bill, Ryan, K. V., & Krotoski, M. L. (2012). Caution Advised: Avoid Undermining the Legitimate Needs of Law Enforcement to Solve Crimes Involving the Internet in Amending the Electronic Communications Privacy Act. *USFL Rev.*, 47, pp. 291.

⁹⁴ 18 U.S. Code § 2709 - Counterintelligence access to telephone toll and transactional records (1986).

⁹⁵ For a discussion of the legal framework and the difficulties for civil liberties see Gorham-Oscilowski, U., & Jaeger, P. T. (2008). National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly*, 25(4), pp. 625-644. doi: <http://dx.doi.org/10.1016/j.giq.2008.02.001>; See also Garlinger, P. P. (2009). Privacy, Free Speech, and the Patriot Act: First and Fourth Amendment Limits on National Security Letters. *NYUL Rev.*, 84, pp. 1105. and Nieland, A. E. (2006). National security letters and the amended PATRIOT Act. *Cornell L. Rev.*, 92, pp. 1201.

⁹⁶ For a critical assesment of the scope of SCA warrantes, see Benedetti, D. T. (2013). How Far Can the Government’s Hand Reach Inside Your Personal Inbox?: Problems With the SCA, 30 J. Marshall J. Info. Tech. & Privacy L. 75 (2013). *The John Marshall Journal of Information Technology & Privacy Law*, 30(1), pp. 5. On SCA warrants in the cloud, which is of particular relevance to TC due to the distributed nature of the data

This means that independently of the specific legal framework that is used to access data, ISPs are increasingly acting as a proxy for police and security services in evidence acquisition. As von der Meulen and Lodder have observed, at the same time when the concept of ISP was considerably widened and now includes the likes of Facebook and Google in addition to the traditional “access providers” such as BT or VirginMedia, their role changed from a neutral thirds to private law enforcers.⁹⁷ Interesting for us in this respect is in particular von der Meulen and Lodder’s “sectorial analysis” of this phenomenon. In general, they note that not just the EU data retention duties, but generally legal cooperation requirements with the police or other third parties was consistently rejected by the ISPs, who sometimes succeeded in getting the legal collaboration requirements rescinded or at least watered down, as in the case of the French HADOPI law⁹⁸ or even more impressively the collective action against the proposed SOPA and PIPA legislation in the US, that pitted ISPs against copyright holders.⁹⁹ In other cases they found

it collects, see Schultheis, N. (2015). Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry. *Brook. J. Corp. Fin. & Com. L.*, 9(2), pp. 661.

⁹⁷ Van der Meulen, N. S., & Lodder, A. R. (2012). From Neutral Thirds to Private Law Enforcers: Toward a Critical Framework for Requests Placed on Internet Service Providers (pp. 1-18). Vrije University of Amsterdam

⁹⁸ *ibid.* p.3. see on the resistance against HADOPI see Mueller, M., Kuehn, A., & Santoso, S. M. (2012). Policing the network: Using DPI for copyright enforcement. *Surveillance & Society*, 9(4), pp. 348-364. , Muir, A. (2013). Online copyright enforcement by Internet Service Providers. *Journal of Information Science*, 39(2), pp. 256-269. doi: 10.1177/0165551512463992; on the use of deep package inspection as a necessary precondition for HADOPI, which would be an inbuilt feature of TC as we saw; See Guez, M. (Producer). (2010). Technical measures in the context of the Hadopi Law (France). . *Presentation before the Stakeholders*. Retrieved from <http://fr.readwriteweb.com/wpcontent/uploads/2010/09/Slides-SCPP.pdf>; Société civile des producteurs phonographiques (SCPP) for a more detailed analysis of the technical requirements – an in depth comparison with TC would go beyond the scope of this thesis.

⁹⁹ A detailed analysis of the interests at stake in this dispute, and the political environment in which it took place, is in Bridy, A. (2012). Copyright policymaking as

ingenious ways of abiding by the letter of the law while finding often ingenious solutions to undermine its efficiency. A particularly striking, and arguably illegal, example is “warrant canaries”. ISPs are prevented under the NSL warrants (discussed above) to disclose to their customers that a data request was made. Some found a workaround, or so they claim: They state on their website that they “never received a warrant” – and would take this note down if one were to be issued.¹⁰⁰ In more traditional territory, example abound where ISPs have fought warrants on behalf of their customers.¹⁰¹

As von der Meulen and Lodder show, not unsurprisingly ISPs were significantly more willing to fight or undermine attempts to co-opt them for law enforcement purposes if there was no direct benefit for them or their customers. As long as ISPs were not major copyright holders e.g. there was no benefit for them in alienating their customer base by penalizing some of them for copyright theft. Similarly, they had no direct benefit in disclosing customer details to law enforcement agencies if the victims of the alleged crime were not directly other customers – as would be the case both in child pornography prosecutions but also some hate speech cases. In these cases, their resistance to legal requirements for

procedural democratic process: A discourse-theoretic perspective on acta, sopa, and pipa. *Cardozo Arts & Ent. LJ*, 30, pp. 153. ; An analysis of an iconic event in this process, the Wikipedia blackout, is in Konieczny, P. (2014). The day Wikipedia stood still: Wikipedia’s editors’ participation in the 2012 anti-SOPA protests as a case study of online organization empowering international and national political opportunity structures. *Current Sociology*, 62(7), pp. 994-1016.

¹⁰⁰ For a positive assessment see e.g. Gilens, N. (2014). The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures. Available at SSRN 2498150, pp. 525-546. For a negative assessment see Wexler, R. (2014). Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders. pp. 158-179.

¹⁰¹ The Electronic Frontiers Foundation keeps records of such acts of resistance – noting e.g. that in 2014, Amazon had been willing to challenge warrants that targeted their customers. <https://www EFF.org/who-has-your-back-2014#courts>

cooperation was strongest.¹⁰² A different situation emerges when the target are the operators of botnets. Here, ISPs had a twofold motivation to cooperate, since botnets could attack them directly (and hence interrupt services to their customers) or expose their customers to attacks by a minority of criminals. Unsurprisingly, this example of “privatized law enforcement” turns out to be the most successful.¹⁰³

The above should not be understood as painting ISPs as selfless champions of their customers, willing to take on vested corporate interests at great personal risks and expenses, even though this was very much the picture the industry tried to paint of itself in the SOPA-PIPA wars.¹⁰⁴ Once an appropriate incentive structure is created, for instance through “safe haven” provisions that invited ISPs to pass on the risk of copyright litigation to others, compliance can be vigorous and potentially beyond what the law technically requires.¹⁰⁵ But what this analysis shows is that for at least some ISPs in at least some forms of co-

¹⁰² see on HADOPI compliance e.g. Meyer, T. (2012). Graduated response in france: The clash of copyright and the internet. *Journal of Information Policy*, 2, pp. 107-127.

¹⁰³ Meulen and Lodder op cit p. 7. See however also Van Eeten, M. J., & Bauer, J. M. (2008). Economics of malware: Security decisions, incentives and externalities: OECD Publishing. STI Working Paper 2008/1 who argues that action was taken by ISPs in no more than 10% of cases.

¹⁰⁴ See in particular the analysis by Benkler, Y., Roberts, H., Faris, R., Solow-Niederman, A., & Etling, B. (2015). Social mobilization and the networked public sphere: Mapping the SOPA-PIPA debate. *Political Communication*(ahead-of-print), pp. 1-31.

¹⁰⁵ See the analysis by Helman, L. (2010). Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement. *Tex. Intell. Prop. LJ*, 19, pp. 111. , in particular p. 183ff. Part of the reason for overcompliance is management of litigation risks, where vague drafting (possibly intentionally) enhances overcompliance, see Craswell, R., & Calfee, J. E. (1986). Deterrence and uncertain legal standards. *JL Econ. & Org.*, 2, pp. 279. An interesting reason for overcompliance is given by Gibson, J. (2007). Risk aversion and rights accretion in intellectual property law. *Yale Law Journal*, 116, pp. 882. where he shows how a feedback loop has caused overcompliance with copyright laws; see also Africa, M. (2000). The Misuse of Licensing Evidence in Fair Use Analysis: New Technologies, New Markets, and the Courts. *California Law Review*, pp. 1145-1183.

optation, the adversarial structure of the legal process and with that its checks and balances are preserved, however diminished they might be. The police still *has* to apply for a warrant that is served to a party which is *not* institutionally friendly to the police (the way judges seem to be, whose scrutiny of warrant applications seems limited),¹⁰⁶ and thus *might* decide to challenge it. Interests of police and ISP are not congruous unless an intentionally designed legal incentive structure makes them so.

Under these circumstances, the type of ethical-analytical framework that von der Meulen and Lodder suggest may well be sufficient to provide a sufficiently abstract mechanism for testing the legitimacy of co-opting ISPs into policing roles. It assumes unwilling ISPs, and then focuses on whether co-opting them is legitimate at all, and if so, just how far the state can go in providing an “incentive structure” through the threat of penal or civil sanctions.

We argue here, that the situation is radically different for TC providers, and that consequently, different methods need to be found to provide a legally justifiable regulatory environment. TC providers, when co-opted into policing tasks, are not any longer preserving even the vestiges of the adversarial structure that we find for other ISPs that are co-opted into policing functions.

Where ISPs have acted in protection of their customers against state interests, they seem to be motivated at least in part by competitive pressures: DuckDuckGo, the privacy preserving browser, saw for instance massive increase in customer numbers in 2013 after Snowden revelations showed how much Security Services had used access to search results.¹⁰⁷ Shortly after, Apple

¹⁰⁶ see e.g. Lee, C. (2011). Reasonableness with teeth: the future of Fourth Amendment reasonableness analysis. *Miss. LJ*, 81, pp. 1133. For a comparison of EU and US approaches to warrant scrutiny and their empirical impact on privacy see Slobogin, C. (2000). Empirically Based Comparison of American and European Regulatory Approaches to Policing Investigation, *Am. Mich. J. Int'l L.*, 22, pp. 423.

¹⁰⁷ The causal connection is made by Krieger, M. (2013). Search Engine "Duck Duck Go" Experiences Traffic Surge in Wake of NSA Scandal. *Liberty Blitzkrieg*.

announced to incorporate DuckDuckGo as an alternative to its own Safari browser, at the same time making strong encryption part of their new iPhones, to the dismay of the security services.¹⁰⁸ That privacy can serve as unique selling point, or at least a significant competitive advantage, has been argued before. According to the “Secure the Trust of Your Brand survey” conducted in 2006 by the Chief Marketing Officer Council:

- More than 50% of consumers said their security concerns were rising;
- 40% have actually stopped a transaction due to a security concern;
- Most importantly for our point, more than 30% said they would seriously consider taking their business elsewhere if they were dissatisfied with the protection of their data;
- and 25% were definite on transferring business in trade off for better security.¹⁰⁹

Data like this indicates that ISPs who work in a competitive market can and do use privacy as a selling point.¹¹⁰ This means they have good reasons to be seen to resist at least those demands by law enforcement personnel that fall short of national warrant requirements – or with other words test the validity of warrants occasionally in court. This remains true despite numerous surveys showing that

<https://libertyblitzkrieg.com/2013/07/10/search-engine-duck-duck-go-experiences-traffic-surge-in-wake-of-nsa-scandal/>.

¹⁰⁸ The response by law enforcement was reported here: Timberg, C., & Miller, G. (2014). FBI blasts Apple, Google for locking police out of phones. *The Washington Post*, pp. 1-7. Indirect evidence for our contention is provided in Donohue, L. K. (2015). High Technology, Consumer Privacy, and US National Security. *Am. U. Bus. L. Rev.*, 4, pp. 11. which analyzed economic data that showed that Post-Snowden, US ISPs were losing customers to providers that could guarantee better privacy

¹⁰⁹ Council, C. M. O. (2006). Secure the Trust of Your Brand, . CMO council webpage: CMO.

¹¹⁰ more comprehensive economic studies that back this point can be found in Cavoukian, A., & Hamilton, T. (2002). *The Privacy Payoff, How Successful Business Build Consumer Trust*: McGraw-Hill Ryerson Trade. See in particular pp. 13-14. For a summary of their evidence; see also Kenny, S., & Borking, J. (2002). The value of privacy engineering. *J. Inform. Law Technol.(JILT)*, 7(1), pp. 1-29.

many customers place only very limited *financial* value on privacy and are not normally willing to pay significant amounts of money for it.¹¹¹ These studies focus on a direct commercial exchange of money for added privacy, they only ask: “how much would you be willing to pay in addition for privacy”, not “would you - everything else being equal - go to a provider that indicates it is willing to fight for your privacy in court”.¹¹²

Now we have prepared the basis for our argument: Co-optation of ISPs into law enforcement, as described by von der Meulen and Lodder, preserves at least to a degree the adversarial structure of the legal process, which is a crucial “check and balances” safeguard for our liberties, but only because companies see a competitive market advantage in doing so. This however presupposes a functioning and highly competitive market. However, as we have seen, the entire philosophy of Trusted Computing is based on eventual herd immunity - *everybody* will have to use TC certified products or their computers won't be able to communicate any longer. A comprehensive legal analysis of the competition law issues that this raise is beyond the scope of this thesis, the crucial issue *that* TC

¹¹¹ Grossklags, J., & Acquisti, A. (2007). *When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*. Paper presented at the Online Proceedings of the Second Annual Workshop on Economics and Information Security.

¹¹² This is the argument in Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, pp. 94. See also for contrast their earlier study Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification*. Paper presented at the Proceedings of the 5th ACM conference on Electronic commerce (pp. 21-29), ACM. Here we can see clearly that customers reward and punish ISPs for news about recent privacy violations, even if they are unwilling to pay much “for their future security” – a result of our “bounded rationality” that is described in Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy. *Digital Privacy: Theory, Technologies and Practices*, pp. 363-377. See also the earlier study by Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12), pp. 65-74. which shows how heterogeneous our assessment of the value of privacy is.

inevitably requires a form of monopoly and hence causes competition concerns is however well documented and also follows from our discussion in the previous chapter.¹¹³ For our discussion, this demonstrates that co-opting TC providers into law enforcement is indeed a game changer that goes beyond previous attempts to leverage the ISPs as Internet gatekeepers for law enforcement purposes. Unlike other ISPs, TC providers, once herd immunity is achieved, will not be exposed to consumer pressure if they fail to protect legitimate consumer interests against law enforcement requests. As von der Meulen and Lodder's study shows, this will mean they are less likely to "fit" into the adversarial structure of our legal system with its checks and balances – they have all the benefits of a private sector player, that is freedom from rules developed to control the police as part of the state, while their regulation through markets is at least severely curtailed.

There is a second line of argument that shows why using TC providers for law enforcement purposes is likely to differ from previous attempts to co-opt ISPs. Referring again to the study by von der Meulen and Lodder, ISPs were particularly willing to cooperate with the police when they themselves were the direct target of criminal activity. This was mainly the case in botnet attacks. ISPs did not suffer, directly, from copyright violation, child pornography or online fraud, and were hence much less willing to cooperate in the control of these activities. TC, again, is different. Here we must remember our discussion of the

¹¹³ For a discussion, the reader is directed to Schoen, S. (2005). Compatibility, competition, and control in trusted computing environments. *Inf. Secur. Tech. Rep.*, 10(2), pp. 105-119. doi: <http://dx.doi.org/10.1016/j.istr.2005.05.005>. With a focus on the cryptography aspect of TC, see also Anderson, R. (2004). Cryptography and Competition Policy - Issues with 'Trusted Computing' *Economics of Information Security* (Vol. 12, pp. 35-52): Springer US. A sector specific analysis can be found in Yung, M. (2003). *Trusted Computing Platforms: The Good, the Bad, and the Ugly*. Paper presented at the 7th International Conference, FC 2003, Guadeloupe, French West Indies (pp. 250-254), Springer.

previous chapter, and the origins of TC as a Digital Rights Management system. SOPA and PIPA had pitted content owners against technology companies. The TC consortium straddles this divide, with several of its members relying on copyright, especially software copyright, as core part of their business.¹¹⁴ Even more worryingly, recent years have seen an increasing emphasis on criminal law as a tool of copyright enforcement.¹¹⁵ This trend in itself has raised a worrying spectre of “over-criminalisation” in substantive law.¹¹⁶ Here our concerns are the procedural and evidential issues more than the substantive law. TC providers become both police and victims of crime, policing actions of which they themselves were victims. In the offline world, such an obvious conflict of interests would result in grave concern – a police officer whose house has been burgled can’t use his warrant card to question, or let alone to detain suspects in his private time to find out who did it. This however is exactly the situation we might find with TC. As we saw in the previous chapter, TC technology is still carrying functional tools that are essentially DRM technology systems in disguise, or repurposes – sealed storage, remote attestation, secure I/O and curtained memory – implemented by code, give TC provider the important power to know when a copyright violation occurs. Even more than that, not only would the

¹¹⁴ See on this point e.g. Roemer, R. (2003). Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer. *UCLA JL & Tech.*, 2003, pp. 8. see also Cohen, J. E. (2006). Pervasively distributed copyright enforcement. *Georgetown Law Journal*, 95, pp. 1-48.

¹¹⁵ See already Green, S. P. (2002). Plagiarism, norms, and the limits of theft law: Some observations on the use of criminal sanctions in enforcing intellectual property rights. *Hastings Law Journal*, 54(1), pp. 167-242. which argued of the danger of an “increasing criminalization of intellectual property law and the widening gap between what the law is and what people think it should be”. See for a more recent analysis Manta, I. D. (2011). The Puzzle of Criminal Sanctions for Intellectual Property Infringement. *Harvard Journal of Law and Technology*, 24(2), pp. 2010-2030.

¹¹⁶ See e.g. Moohr, G. S. (2004). Defining Overcriminalization Through Cost-Benefit Analysis: The Example of Criminal Copyright Laws. *Am. UL Rev.*, 54, pp. 783.

information about a violation become visible, more actions are possible to occur according to the content owner rules – software that does not comply with these rules can be banned from using the specific file content through remote attestation, or even sealed storage that will prevent users from opening the file content from such an unauthorized software. Moreover, using curtailed memory and secure I/O, the TC technology prevents copying of a copyrighted file even from capturing it from sound peripherals in case of media files. All in all, TC will be impossible to be circumvented based on the approach they implemented,¹¹⁷ it will allow the content providers, and the software vendors to “exercise complete control over how and when their content is used” and point that the traditional relationship between the user and the content characterized by anonymity, copyright, privacy and other regimes, needs to be revisited in the digital age.¹¹⁸ Furthermore, as discussed earlier in Chapter 3, the control of the computer will be taken off the users and shift to the TC vendors allowing full control to the machine and the content.

Woodford, in an insightful paper back in 2004, described an example of how a legitimate music downloader using a Trusted Computing technology computer, can be deterred (by the changes in technology) from ripping or transferring the music bought on a storage medium or a device outside the computer tower (i.e. USB, CD, DVD etc.) thus indicating the change in the music ownership of the individual.¹¹⁹ Using the TC technology, illegitimate use as well as the *intention* to breach intellectual property found in digital form, can be trailed and controlled. This means the TC provider combines several key policing functions in this situation: He collects evidence and secures it, he deters, proactively, certain types

¹¹⁷ Carroll, A., Juarez, M., Polk, J., & Leininger, T. (2002). Microsoft Palladium: A Business Overview: Microsoft Press Release.

¹¹⁸ Woodford, C. (2004). Trusted Computing or Big Brother? Putting the Rights back to Digital Rights Management. *U. Colo. L. Rev.*, 75, pp. 253-300.

¹¹⁹ *ibid.* p.253ff

of behavior, and finally he even carries out something not too dissimilar from an arrest – when a suspect’s computer, using software in violation of copyright law, gets remotely “blocked”.

Going back to the fictional examples from the beginning of the chapter, the offline equivalent to law enforcement in a TC age might look closer like this: Every household has to hire a security guard or risks sanctions such as ostracism (inability to communicate with others) or inability to get insurance cover. All security guards are vetted and employed by a private company that also has a side business in theft insurance. While you pay for the security, the guards have a second income stream by checking your belongings for stolen goods, and will inform the police (or indeed change the locks on your door) when they find goods that belong to a client of the insurance arm of their company.

At the heart of this problem for us is the “dual nature” of TC: organized as a private sector company, but as a standard setting body premised on achieving eventually a monopoly, it takes on roles previously reserved to the state. This allows in the absence of clarifying legislation the potential of a very peculiar form of “forum shopping” – relying on private or criminal law depending on which regime maximizes their power, or conversely, risking penalties under either regime which could be a major disincentive to invest in the development of the technology.

For us, this is one more argument why it might be desirable to create a sui generis framework for TC (and similar security) providers that recognizes that or them, monitoring, analyzing and to a degree retaining data about suspicious activities is not the side effect of their activity, but their very reason for existence. Despite being a private sector actor, rules that normally apply to the police might be a much more appropriate avenue in the light of the discussion above.

We used above data retention duties as a case study, to which we can now return. In what follows, we will use data retention and forensically sound data storage as one example of how criminal evidence rules can be extended to TC,

with the double advantage that on the one hand, this creates particularly strong and convincing evidence, and on the other, it creates a new mechanism of control over the TC provider that can generate trust in them as a side effect.

Data retention duties of course are an intricate legal issue independently of the question of TC, and have created significant literature on their own.¹²⁰ We by contrast, will put the focus on an issue that is of particular relevance for TC – not if, but *how* data should be retained, assuming that legitimate law enforcement functions make some form of data storage necessary. We've argued above that TC takes on some post-crime policing function. We know from experience that the evidence of police officers, just as the evidence from expert witnesses, carries particular weight. This makes them potentially dangerous for us - a bend police officer or a negligent expert can condemn an innocent person to prison. Building again on our examples above, a corrupt police officer could use the authority of his office to gain access to our dwellings and plant a bloodied knife. A negligent expert may not have heard about the latest findings that invalidate his method. We trust police and expert witnesses for a similar mix of reasons that we discussed in the introductory chapter for social trust in general.¹²¹ Some of them, as we discussed in the previous chapter are emotive and organically grown in a

¹²⁰ See e.g. Bignami, F. (2007). Privacy and law enforcement in the european union: the data retention directive. *Chicago Journal of International Law, Spring*, pp. 233-255. , Blanchette, J.-F., & Johnson, D. G. (2002). Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness. *The Information Society*, 18(1), pp. 33-45. doi: 10.1080/01972240252818216, Cheung, A., & Weber, R. H. (2008). Internet governance and the responsibility of internet service providers. *Wis. Int'l LJ*, 26, pp. 403. For an analysis of the interaction between EU law and the law of a member state see DeSimmone, C. (2010). Pitting Karlsruhe against Luxembourg-German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German LJ*, 11, pp. 291.

¹²¹ The most comprehensive and influential study on trust in modern police forces is Tyler, T. R. (2002). *Trust in the law : encouraging public cooperation with the police and courts*. New York, [N.Y.]: New York, N.Y. : Russell Sage Foundation.

society, where they often rely on personal acquaintance and kinship bounds.¹²² Others are institutional: we trust the police because there are bodies such as the Police Complaints Commission, or the professional bodies for expert witnesses that can punish them if they violate the rules.¹²³ Others still are “rational” in the way Weber used the term, which is based on formal legal rules. The rules of evidence, especially the exclusionary rules, have this function: they tell us we can trust the police, for if they oversell their mark, their work will be for naught.¹²⁴

We discussed the problem of “emotive trust” and the TCI in the preceding chapter and concluded that the nature of the TC consortium mitigates against this basis for a trust relationship. Generating trust through institutions, the second aspect of trust, would see the TCI as a consortium getting integrated into a wider institutional structure, chains of responsibility and accountability, complaints procedures and sanctions. At present, there is no structure in Internet governance to provide for such an organization that in the past has been intimately linked with the concept of the modern nation state, as we saw in our brief discussion of Weber. There remains option three, using the rules of evidence

¹²² For an application to the police see e.g. MacDonald, J., & Stokes, R. J. (2006). Race, social capital, and trust in the police. *Urban Affairs Review*, 41(3), pp. 358-375. ; For expert witnesses see Brodsky, S. L., Griffin, M. P., & Cramer, R. J. (2010). The Witness Credibility Scale: An outcome measure for expert witness research. *Behavioral Sciences & the Law*, 28(6), pp. 892-907. doi: 10.1002/bsl.917.

¹²³ See for the police v Hough, M., Jackson, J., Bradford, B., Myhill, A., & Quinton, P. (2010). Procedural Justice, Trust, and Institutional Legitimacy. *Policing: A Journal of Policy and Practice*, 4(3), pp. 203-210. doi: 10.1093/police/paq027; For expert witnesses see Turner, J. A. (2005). Going after the Hired Guns: Is Improper Expert Witness Testimony Unprofessional Conduct or the Negligent Practice of Medicine. *Pepp. L. Rev.*, 33, pp. 275.

¹²⁴ See for the police Paulsen, M. G. (1961). The exclusionary rule and misconduct by the police. *The Journal of Criminal Law, Criminology, and Police Science*, pp. 255-265. See for expert witnesses Graham, M. H. (1986). Expert Witness Testimony and the Federal Rules of Evidence: Insuring Adequate Assurance of Trustworthiness. *U. Ill. L. Rev.*, pp. 43.

and similar procedural rules to generate trust. This is the option most in line with the general gist of this chapter's argument: since TC providers carry out de facto police functions, they need to be subject to the same procedural rules.

One particularly important procedural safeguard is the "chain of custody". More than most others, it carries on its face the role to control the police and thus create trust.¹²⁵ "Prove that at every step, only an authorized person handled the evidence, so that if something went wrong, or it got manipulated, we know whom to blame." More than any other it poses new and intricate problems for electronic evidence, even outside TC environments.¹²⁶

We will look now at this specific rule to see what specific issues TC in a post-crime scenario poses. Securing the data collected as evidence either from personal digital devices (e.g. computer, mobile phones, peripherals, PDAs, electronic devices etc.) or from networks (e.g. intranets, extranet, Internet) and maintaining a rigid chain of custody for the data has been a challenge. To maintain probative value, procedurally sensitive information retrieved from customer computers have to be kept safely and ensure that no data spoliation or alteration can take place.¹²⁷ From the beginning, courts were sensitive to the problem of

¹²⁵ See e.g. Stoughton, S. (2015). Evidentiary Rulings as Police Reform. *U. Miami L. Rev.*, 69, pp. 429-519. esp. p.437ff

¹²⁶ See e.g. Bratus, S., Lembree, A., & Shubina, A. (2010). Software on the witness stand: what should it take for us to trust it? *Trust and Trustworthy Computing* (pp. 396-416): Springer, Duranti, L., & Rogers, C. (2012). Trust in digital records: An increasingly cloudy legal area. *Computer Law & Security Review*, 28(5), pp. 522-531. , Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2014). Digital Evidence Cabinets: A Proposed Frameworks for Handling Digital Chain of Custody. *Int. J. Comput. Appl.*, 109(9), pp. 30-36.

¹²⁷ Article 7 of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108 C.F.R. (1985). "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination"; Research by Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer

tamper-proof chain of custody records in digital forensics. However, there are also significant risks and corresponding costs attached to data preservation, raising economic, long-term preservation and other hindrances¹²⁸ while avoiding it, has been described as the struck between “triumph and defeat in the courtroom”.¹²⁹ Digital integrity has been defined by Menezes et. al as “the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source”.¹³⁰ It is a real challenge for hardware and software manufacturers to achieve and self-prove integrity of digital evidence with time binding in order to achieve transparency for the threefold digital integrity marks of “who”, “when”, and “what”.¹³¹

forensics. *ACM Transactions on Information and System Security (TISSEC)*, 2(2), pp. 159-176. has been aimed to limit the ability of a successful attacker to corrupt log files storing sensitive information, by using encryption methods on the log files; Researchers Snodgrass, R. T., Yao, S. S., & Collberg, C. (2004). *Tamper detection in audit logs*. Paper presented at the Proceedings of the Thirtieth international conference on Very large data bases - Volume 30, Toronto, Canada. have also proposed mechanisms based on cryptographically strong one-way has functions aiming to prevent any possible corruption of the audit log produced by the system.

¹²⁸ Arora, J. (2009, January 29-30, 2009). *Digital Preservation, an Overview*. Paper presented at the National Seminar on Open Access to Textual and Multimedia Content: Bridging the Digital Divide, Hassell, J., & Steen, S. (2003). *Avoiding Spoliation of Electronic Discovery*. <http://www.experts.com/Articles/Avoiding-Spoliation-of-Electronic-Discovery-By-Johnette-Hassell-PhD-Susan-Steen>, Tibbo, H. R. (2003). *On the Nature and Importance of Archiving in the Digital Age* *Advances in Computers* (Vol. Volume 57, pp. 1-67): Elsevier, Waters, D., & Garrett, J. (1996). *Preserving Digital Information. Report of the Task Force on Archiving of Digital Information*: ERIC.

¹²⁹ Hassell, J., & Steen, S. (2005). *Preserving and Protecting Computer Evidence*. *Evidence Technology Magazine*, 3(4), pp. 16-18.

¹³⁰ Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of applied cryptography*. United States: CRC Press (Boca Raton).

¹³¹ Hosmer, C. (2002). *Proving the integrity of digital evidence with time*. *International Journal of Digital Evidence*, 1(1), pp. 1-7.

3.6.1 Chain of custody and Audit trails

“There is no single way to enforce chain of custody in digital forensics, but the use of techniques such as time-stamping and hashing algorithms are central to all methods”.¹³² As computers run, evidence of the user’s metadata are collected, revealing the date and time of creation, edition and last time of access for files. Traces are always left behind even if the user does not realize, making audit trails much easier to establish.¹³³ Preserving digital data is not enough on its own, as we need “proof that the preservation environment preserves authenticity and integrity while performing the communication constitutes a theory of digital preservation”.¹³⁴ It is this self-reflective move where TC comes into its strength. As we saw in the previous chapter, a key aspect of TC is that it permits a system to prove *about itself* that it wasn’t tampered with – issues we discussed there under the header of “unhindered operation”. In Trusted computing technology then, integrity is of paramount importance. The TPM manufacturer acting as an authoritative entity is used to create integrity data or values, which can then be used amongst others as chain of custody procedures, digitally sign and assign the date on files or components, in a way that later modification is impossible to occur. As the Trusted Platform consists of several components both hardware and software, it is important that these components (mutable or not) remain intact from any deviations from the original state, and in case of modifications the Trusted Platform will be in place to autonomously

¹³² Thorvaldsen, Ø. E. (2006). *Geographical Location of Internet Hosts using a Multi-Agent System*. Norwegian University of Science and Technology.

¹³³ U.S. DOJ. (2010). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*: Office of Legal Education Executive Office for United States Attorneys.

¹³⁴ Moore, R. (2008). Towards a theory of digital preservation. *International Journal of Digital Curation*, 3(1), pp. 63-75.

detect and report this to the owner/ user.¹³⁵ While the Trusted Platform desires integrity management, it has another objective: to manage the runtime integrity through proper management of its components during load-time and runtime although no promises are given that the components are implemented in a correct manner and are bug-free.¹³⁶

A second aspect of the traditional approach of chain of custody is that the entity that first collected (and in this sense “created”) the evidence needs to be clearly identified so that the integrity data source is clear. Again, in our discussion in the previous chapter, we saw how provable identities are created as part of the TCI attestation process. Thus in the TC case, the TPM manufacturer, or the TSS software manufacturer, or the BIOS manufacturer could all be considered as candidates for “co-creators” of the initial evidence data point, together with the target computer on which the evidence was found. The ultimate goal as described in the TCG Integrity Managements Architecture report is to provide all the necessary mechanisms to capture and represent integrity information and to verify the Integrity Report context using the reference measurements obtained during the runtime measurement procedure.¹³⁷ This process of integrity verification then becomes the natural correspondent of integrity verification measures in “real” evidence - the sealed plastic bag with the CSI’s signature.

Based on the Report,¹³⁸ recording the measurements (integrity measurements) performed by components constituting the trust chain and presenting them (integrity reporting) in a comprehensive way to the external world, is compelling. Thus, it is possible to preserve and conduct the information gathered by the trust chain of the platform with care while keeping in mind the

¹³⁵ TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.).

¹³⁶ *ibid.* p.13

¹³⁷ *ibid.* p.30

¹³⁸ *ibid.* p.42

timing of dissemination of the information to the external world. Briefly, the Integrity management collects actual integrity measurements from all the components comprising the Trusted Platform – the so called *snapshots*¹³⁹ – which on a running live platform, are the *runtime measurements*¹⁴⁰ making up the trust chain. It then compares these runtime measurements over pre-set reference integrity measurements of the same components which are called *reference measurements*¹⁴¹, which are determined by the components’ manufacturers or by other third parties and allow the Trusted Platform to measure the “level” of trust achieved.¹⁴² Being able to express trust numerically like this, chimes extremely well with recent developments in evidence law. In the US, in the landmark decision of *Daubert v. Merrell Dow Pharmaceuticals*,¹⁴³ the court established five

¹³⁹ Snapshots from the Integrity Report.

¹⁴⁰ Runtime measurements refer to the measurements taken from the components of the platform (specifically from the Root of Trust for Measurement (RTM)) during the actual boot and operation of the specified platform. It is therefore expected that these measurements will differ according to the computer and its components and will reveal the platform’s integrity state; for more information look TCG. (2011b). TCG Infrastructure Working Group Integrity Report Schema Specification v 2.0 (Revision 5 ed.). The actual measurements are acquired by the Platform Trust Services (PTS) process and is intended to be integrated within the Trusted OS components to ensure the trustworthiness that TCG claims TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.).

¹⁴¹ Pre-set static measurements are provided by the components’ manufacturers and are following the TCG Reference Manifest structure (RM) containing information that identify the manufacturer and are descriptive to the model TCG. (2011a). TCG Infrastructure Working Group Core Integrity Schema Specification v 2.0 (Revision 5 ed.).

¹⁴² TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.).

¹⁴³ *Daubert v. Merrell Dow Pharmaceuticals, Inc*, No. No. 92-102, 509 U.S. 579 (Supreme Court 1993).

criteria, the “Daubert Standard” that governs the admissibility of all forms of expert evidence.¹⁴⁴ The court established five criteria in particular:

1. Empirical testing: whether the theory or technique is falsifiable, refutable, and/or testable.
2. Whether it has been subjected to peer review and publication.
3. The known or potential error rate.
4. The existence and maintenance of standards and controls concerning its operation.
5. The degree to which the theory and technique is generally accepted by a relevant scientific community.

The “gold standard” for a Daubert-type analysis is DNA evidence or similar “laboratory based” disciplines, other newly emerging fields of forensic science should aspire to match them.¹⁴⁵ DNA and its concept of “match probability” explicates in particular the third criterion, the known or potential error rates, one of the most important aspects of Daubert.¹⁴⁶ Here we get the “there is a one-in-a-billion chance that the DNA could come from someone other than the suspect”.¹⁴⁷ No single piece of evidence needs to be perfect – but we need to know just “how

¹⁴⁴ on Daubert in general see Giannelli, P. C. (1993). Daubert: Interpreting the Federal Rules of Evidence. *Cardozo L. Rev.*, 15, pp. 1999. See also Dixon, L., & Gill, B. (2002). Changes in the standards for admitting expert evidence in federal civil cases since the Daubert decision. *Psychology, Public Policy, and Law*, 8(3), pp. 251.

¹⁴⁵ So e.g. Cheng, E. K. (2004). Reenvisioning Law Through the DNA Lens. *NYU Ann. Surv. Am. L.*, 60, pp. 649. or Mnookin, J. L. (2001). Fingerprint evidence in an age of DNA profiling. *Brook. L. Rev.*, 67, pp. 13.

¹⁴⁶ So e.g. Jabbar, M. (2010). Overcoming Daubert's shortcomings in criminal trials: making the error rate the primary factor in Daubert's validity inquiry. *NYUL Rev.*, 85, pp. 2034. or Christensen, A. M., Crowder, C. M., Ousley, S. D., & Houck, M. M. (2014). Error and its meaning in forensic science. *Journal of forensic sciences*, 59(1), pp. 123-126.

¹⁴⁷ See e.g. Scheck, B. C. (1993). DNA and Daubert. *Cardozo L. Rev.*, 15, pp. 1959. Koehler, J. J., Chia, A., & Lindsey, S. (1995). The random match probability (RMP) in DNA evidence: Irrelevant and prejudicial? *Jurimetrics Journal*, 35, pp. 201.

imperfect” it is, how strong its evidential weight is, even if it is in comparison to DNA very small.¹⁴⁸

Forensic computing is not a laboratory science like DNA, it is not normally based on large population data that provide us with background probabilities, and hence struggled for that reason alone to meet the Daubert standard.¹⁴⁹ TC’s “reference measurements” are one important way in which forensic computing can emulate DNA evidence and meet the Daubert criterion.¹⁵⁰ The ability to quantify the evidential strength, the trust that we can rationally place in a piece of evidence, is not restricted to the US legal system. In England and Wales, the Law Commission published in 2011 its final recommendations for reform of the law on expert evidence, with the emphasis on a new reliability-based admissibility test for expert opinion evidence based on the experience with

¹⁴⁸ A typical example is Gonzalez-Rodriguez, J., Rose, P., Ramos, D., Toledano, D. T., & Ortega-Garcia, J. (2007). Emulating DNA: Rigorous quantification of evidential weight in transparent and testable forensic speaker recognition. *Audio, Speech, and Language Processing, IEEE Transactions on*, 15(7), pp. 2104-2115. Forensic speaker identification will never reach the probative weight of DNA. But to have any value at all, we need to know, through rigorous methods, just how reliable it is.

¹⁴⁹ So in particular Marsico, C. V. (2005). Computer evidence v. daubert: The coming conflict *CERIAS Tech Report 2005-17* (pp. 1-21). Center for Education and Research in Information Assurance and Security Purdue University.; In a similar vein, but with greater emphasis on measuring the reliability of individual experts rather than the methods they use, Meyers, M., & Rogers, M. (2004). Computer forensics: the need for standardization and certification. *International Journal of Digital Evidence*, 3(2), pp. 1-11. Measuring error rates of individual experts rather than their methods has been one popular way to circumvent the spirit of Daubert. See e.g. Koehler, J. J. (2007). Fingerprint error rates and proficiency tests: What they are and why they matter. *Hastings LJ*, 59, pp. 1077.

¹⁵⁰ Not just addressing TC, but DRM in general for this purpose, see with more technical details Lee, W., & Hwang, C. (2007). *A forensic computing system using a digital right management technique*. Paper presented at the Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on (pp. 258-262),IEEE.

Daubert.¹⁵¹ This will also challenge computer forensic practices in the UK, with TC for the reasons given above, being a part of the answer.¹⁵²

Thereafter, the integrity data gathered need to be collected and assembled together to form a consistent set of integrity information about the Trusted Platform. The acceptable Reference Manifest will include only the formatted and normalized information that follow the ideal format.¹⁵³ The value of the collected integrity data should be highly estimated leading to trust affirmations concerning the platform altogether. Attached to the Reference Manifest a digital signature¹⁵⁴ from the issuer (either the manufacturer of the component or a trusted third party) provides source-authentication of the data. The security of the integrity data will be ensured in all stages of the collection process while an evaluator mechanism will be in place and adequately report on the presence and status of the component integrity information to the data source (e.g. the creator or manufacturer of the integrity data).¹⁵⁵

Following, the collection of integrity data, the verifier needs to authenticate them as well as all the components comprising the Trusted Platform. The data

¹⁵¹The recommendations are available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229043/0829.pdf for a discussion see Wheate, R. M., & Jamieson, A. (2009). A Tale of Two Approaches-The NAS Report and the Law Commission Consultation Paper on Forensic Science. *International Commentary on Evidence*, 7(2).

¹⁵² Sallavaci, O., & George, C. (2013). New admissibility regime for expert evidence: the likely impact on digital forensics. *International Journal of Electronic Security and Digital Forensics*, 5(1), pp. 67-79.

¹⁵³ TCG. (2011a). TCG Infrastructure Working Group Core Integrity Schema Specification v 2.0 (Revision 5 ed.).

¹⁵⁴ The digital signature can be confirmed by the Verifier by checking that the AIK private key previously used in the Integrity Report signature matches the one used to sign the quote information belonging in the attestation (Quote structure) as well as that the AIK certificate is attached to the EK-certificate of the TPM hardware. TCG. (2007). TCG Credential Profiles v 1.1 *For TPM Family 1.2; Level 2* (Revision 1.014 ed.).

¹⁵⁵ TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.).

can be passed to the verifier (user) in various methods; either by publishing the information in an Integrity Database (or Reference Manifest Database) solely available to the verifiers, or with the use of a storage component. It is up to the discretion of the manufacturer to decide whether to create a database including all its component products, or to publish the database to a third party service provider. The intention of this database is to maintain an accurate source of component integrity information and which can be accessible by the verifier.

During the collation stage which follows communication/publication, the integrity data gathered needs to align itself with the corresponding components for verification purposes. The verification of the correctness of the integrity data gathered, completes through the next and last phase of evaluation by the verifier entity when the components information is compared with those listed in the Reference Manifest Database.

The procedure of comparing snapshots to Reference Manifest Structures, is an automated one and compares the essential structural information of both records side by side. Furthermore, it facilitates the verifier to be aware of the status of integrity components creating the platform in addition to the component's source authenticity deriving from the manufacturer's signature obtained in the collection phase.¹⁵⁶ With the awareness of the verifier, an evaluation of the Requestor entity is executed under the term of Platform Authentication.¹⁵⁷ The Runtime/Loadtime measurements and Reference measurements processes are shown in the following figure taken from the TCG

¹⁵⁶ *ibid.* p.15

¹⁵⁷ TCG. (2005). TCG Infrastructure Working Group Reference Architecture for Interoperability (Part I) v1.0 (Revision 1.0 ed.).

report:

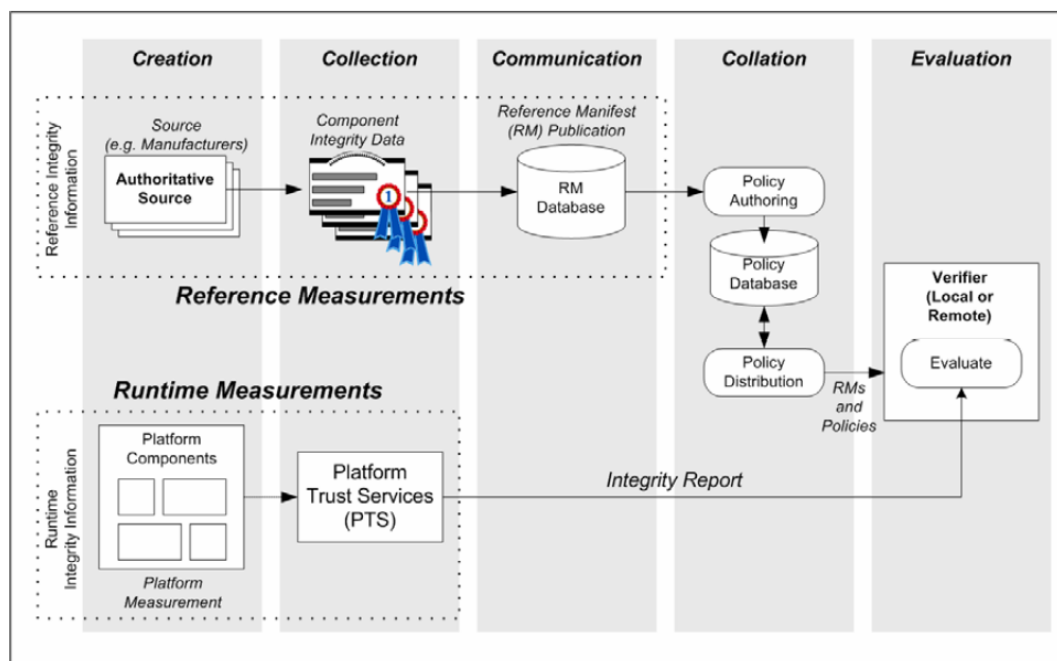


Figure 4: Runtime/Loadtime Measurements and Reference Measurement Processes ¹⁵⁸

Concerning protection of the Reference Manifest and Snapshot documents TCG has utilized an Integrity Wrapper that involves various attributes that are used by the verifier to establish the genuineness and the authenticity of the document (i.e. a confidence value, digital signature and date-time).¹⁵⁹ Here we note again the more than metaphorical similarity between the “digital wrapper” and the “evidence collection bag” of old.

As Chain of custody has been one of the options that TCG explored; expanding formally legal evidentiary rules on preservation of custody chains to them for forensic purposes seems an obvious option – though with the important “symbolic” effect that it “makes official” the quasi-police function of the TC providers by extending rules to them that in the past only applied to state actors.

¹⁵⁸ TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.). Figure in pg. 16.

¹⁵⁹ *ibid.* p.20

TCG is using a Core Integrity Manifest Schema which defines code and configuration integrity management primitives.¹⁶⁰ These primitives are commonly used in the Integrity Report produced and the Reference Manifest created by the component manufacturer. As stated earlier, for easier verification purposes, the Integrity Report and Reference Manifest follow common syntax and semantics enabling the Core schema to provide a unique interpretation of the measurements and their relation to the platform components.¹⁶¹ Amongst others, the Core schema consists of elements supporting collection and reporting of integrity values including the *Collector* element. This element may be included in the manifest as it holds the hash computation concerning the ComponentID. The *SigningComponent* element deals with the signature provided by the manufacturer on the component and it is optionally added to the manifest.

3.6.2 Collecting online evidence

Digital evidence handling from computers has been matured considerably in recent years. It includes collection of the data in a law-compliant way using specialized and standardized tools such as Encase®, AccessData’s Forensic Toolkit, Technology Pathways’ ProDiscover and others. One of the problems indicated above though, is that a TC system may well prove to be resistant to analysis by off-the-shelf forensic tools, as they tend to “force” the target computer into a behavior for which it was not designed. From the computer’s perspective, so to speak, there is no difference between the attack by an “untrustworthy” criminal hacker and a (socially) “trustworthy” police officer.¹⁶²

¹⁶⁰ TCG. (2011a). TCG Infrastructure Working Group Core Integrity Schema Specification v 2.0 (Revision 5 ed.).

¹⁶¹ TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.).

¹⁶² This should be a major source for concern. All the more worrying that apart from some lone academic voices such as Burmester, M., & Mulholland, J. (2006, April 23 - 27). *The advent of trusted computing: implications for digital forensics* Paper

While as we just saw, the authentication element makes TC superior to non-TC environments for evidential purposes, it poses serious difficulties to get the data from a non-cooperating target in the first place. That TC therefore also poses a problem for post-crime investigation, should hardly be surprising. After all, a key component of TC is also secure encryption, whose detrimental effects on law enforcement are otherwise widely discussed – to the point that recent suggestions by both the US and UK governments point towards prohibition of certain encryption tools, just after the “crypto wars” of the 1980’s seemed over.¹⁶³ Just how desperate these reactions to the threat of crime and terrorism are, becomes clear if one remembers that encryption is a key enabler for online banking and almost all other online transactions. If this proposal went to go ahead, TC would be a prime candidate for prohibition. To brute force even the

presented at the Proceedings of the 2006 ACM symposium on Applied computing, Dijon, France (pp. 283-287),ACM Press., the issue has been ignored by police, lawyers and technologists.

¹⁶³ It would go beyond the scope of this thesis to discuss the impediments that encryption can create for law enforcement. A comprehensive analysis from the early discussions, still in the shadow of the cold war, and present day crime-centric debates are in Koops, B.-J. (1999). *The crypto controversy: a key conflict in the information society* (Vol. 6): Kluwer Law International. The initial discussions centred around possible use by the Warsaw Pact, using export control laws as the chosen legal mechanism to (try to) prevent the spread of the technology. See e.g. Nguyen, T. (1996). Cryptography, Export Controls, and the First Amendment in *Bernstein v. United States Department of State*. *Harv. JL & Tech.*, 10, pp. 667. The question of access for law enforcement to encrypted data remains a persistent issue see e.g. Wolfe, D. (2000). Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption, *The Emory LJ*, 49, pp. 711. for a recent comparative overview see Saper, N. (2012). International Cryptography Regulation and the Global Information Economy. *Nw. J. Tech. & Intell. Prop.*, 11, pp. xv. An early socio-legal analysis similar to the one dominating this thesis, and also discussing the implications for online trust, can be found in Friedman, D. (1996). A World of Strong Privacy: Promises and Perils of Encryption. *Social Philosophy and Policy*, 13, pp. 212-228. doi: 10.1017/S0265052500003526 . Even more explicit on the link between encryption and trust is Akdeniz, Y., & Walker, C. (1998). UK Government policy on encryption: trust is the key. *JCL*, 3, pp. 110.

2048-bit public/private keys suggested in early versions of TC would mean, according to RSA, a task many times longer than the universe is likely to last. To brute force a 1640-bit key would require about a million computers (with 500 MHz processors) operating for about 100 billion years.¹⁶⁴ Even stronger and more comprehensive is the BitLocker tool that encrypts the entire hard disk based on the trusted computing techniques that we discussed briefly in the previous chapter. In our assessment this goes beyond the privacy measures Apple has announced recently for its iPhones, proposals that garnered condemnation from police and police-friendly legal academics.¹⁶⁵ Obviously, should the campaign to outlaw encryption gain against all odds momentum, this thesis will become moot and part of legal history.

Collecting digital evidence from the Internet however, belongs in a different unique discipline – Remote Internet forensics. The geographic location of the crime scene is what makes it distinct from digital forensics, as the data on computers can be accessed without being aware on the actual location of the data.¹⁶⁶ The Internet is a large pool of information for investigations used by almost everybody (i.e. military, government, attorneys, personnel etc.) as well as a large provider for tools used in investigations.

The Good Practice Guide for computer-based electronic evidence published by ACPO E-Crime Working Group & Metropolitan Police Service gives a clear

¹⁶⁴ Halboob, W., & Mahmood, R. (2012). State of the Art in Trusted Computing Forensics *Future Information Technology, Application, and Service* (pp. 249-258): Springer.

¹⁶⁵ See e.g. Timberg, C., & Miller, G. (2014). FBI blasts Apple, Google for locking police out of phones. *The Washington Post*, pp. 1-7. Critically also Orin Kerr in his contribution to the influential Volokh Conspiracy blog, Kerr, O. (2014). The Volokh Conspiracy - Apple's dangerous game. <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/>. A critical response to Kerr's analysis is here: Draughn, M. (2014, September 20, 2014). Orin Kerr's Dangerous Thinking, *Windypundit*. Retrieved from <https://windypundit.com/2014/09/orin-kerrs-dangerous-idea/>

¹⁶⁶ Shipley, T. G. (2007). Collecting Legally Defensible Online Evidence. pp. 1-25.

guidance on handling digital evidence from computers, yet the directions given on the collection of evidence from the Internet are much less clearer.¹⁶⁷ The main reason for this is that the data of interest may be temporary and should require live content capturing to be fetched along with the huge size of the Internet. A review on cases in the area of digital evidence from the Internet exposes the complications around the concepts of evidence collection and preservation and reveals that collection of evidence from computers has evolved to a standard process, something which is not the case for evidence collection from the Internet – still following invalidated methods for data collection.¹⁶⁸ Many commercial and freeware tools have been proved to capture Internet based data and some have been successful for law enforcement and therefore have been adopted for this purpose. However, it is worth noting that none of these tools have been originally designed for the purpose of collecting, preserving and presenting data to the court.

3.7 Conclusions

Internet security has finally gained the interest that it deserves from the governmental point of view.¹⁶⁹ Consumers also need to be confident in Internet security. TC proposes a technical solution, where security is neither entrusted to the user, nor enforced by the state, but is found in every unit of the Internet. This chapter has outlined that this amounts to a dramatic shift of power away from consumers and state regulatory bodies to the software providers, and such a

¹⁶⁷ ACPO E-Crime Working Group, & Metropolitan Police Service. (2007). Good Practice Guide for Computer-Based Electronic Evidence *Official release version*.

¹⁶⁸ Shipley, T. G. (2007). Collecting Legally Defensible Online Evidence. pp. 1-25.

¹⁶⁹ Cm7948. (2010). *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. London: The Stationery Office Limited, Downing, E. (2011). *Cyber Security – A new national programme*. (SN/SC/5832). House of Commons Library, Intellect. (2010). Intellect reacts to the National Security Strategy and Strategic Defence and Security Review. <http://www.intellectuk.org/media-releases/6378>

move will only be acceptable if it is accompanied by an equivalent shift in legal responsibility. While the House of Lords is right in its emphasis on the responsibility of software and hardware producers, it may have underestimated the amount of adjustments in the legal regime that this requires.¹⁷⁰ The author contends that TC is best understood as the outsourcing of state functions to the private sector, and with that arises the requirement to provide, on the one hand, adequate protection for citizens, and on the other, a rational framework that grants the necessary legal privileges while imposing certain responsibilities on TC providers, making them more like the 'special constables' they in fact will become.

In the preceding paragraph, we have seen how we can leverage the laws of evidence to rebalance rights and duties in a TC environment *if* we take the idea that TC providers are de-facto police service. Their greater rights to collect, evaluate and communicate data about their customers would be balanced by the same type of restrictions the police is under. TC, so we have argued, is not just another ISP that can more or less against its will be press ganged into supporting policing activity. Rather, TC changes for better or worse fundamentally the nature of digital evidence and computer forensic investigation. Its "dual nature" that oscillates between a traditional commercial entity, a quasi-public standard setting body, a de-facto monopoly and a law enforcement agency creates both risks and opportunities. The risk is that it falls between regulatory regimes, which could either see them amass power on behalf of the state, or conversely undermine even legitimate evidence gathering by law enforcement agencies. It could result in unchecked and unregulated powers concentrating in the hand of the TC consortium, but it could also result in a loss of the very trust that their

¹⁷⁰ House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm>.

systems try to create and with that ultimately the failure of this approach that relies after all on voluntary uptake by customers.

We have argued that with the great powers that the TC provider will yield, great responsibilities must come – and in a democratic society under the rule of law, these responsibilities need to be enshrined at law. Furthermore, law used in this way has been seen, ever since Max Weber, as a key element to generate societal trust – ultimately, being regulated in this way, and being seen to be regulated, is in the very best interest of the TC providers themselves, and can help to address the reluctant uptake that we traced back in the last chapter to the divergence between techno-trust and societal trust. In this chapter, we explored how such a legal rebalancing of rights and responsibilities can look like, focusing on public law and the law of criminal procedure. This chapter emphasized the “public service” role of TC as guarantor of the security of critical infrastructure. In the next chapter, we will focus on the other side of the coin, TC as a private sector actor whose relation with its customers is mediated by contract law. In this chapter, we argued that TC providers are not just another ISP, and while one can apply analogously some of the rules and regulations of e.g. EU data protection law or data retention duties that ISPs are subject to, it is more promising to treat them as a sui generis entity: A private sector actor in a monopoly position targeted by the state with maintaining the security of the critical infrastructure. This allows to exempt them from some restrictions on data collection that are appropriate for other ISPs, but that would unnecessarily impede their task of protecting the Internet against attacks, while at the same time making them subject to more stringent regulation that we would normally only find in the law regulating police activities.

However, TC providers remain a private sector entity, and their relation to their own customers is ultimately governed by contract law. In the next chapter, we will ask if a similar “rebalancing: of rights and duties, power and

accountability” that we discussed here for criminal procedural law is also possible and necessary for their “private sector” face.

CHAPTER 4 :

RELIANCE LIABILITY ISSUE IN ANALOGY TO TMS

4.1 Introduction

In the previous chapter, we approached the legal environment around TC from a public law (criminal law) perspective – what can the state or society legitimately demand from TC providers, what rights can they be given, what obligations should they be under? The premise for this analysis was that TC will either be successful (have significant uptake) and as a result inevitably shift power and control to the TC provider and their consortium. Or it will fail (have insufficient uptake to ensure herd immunity) because it won't be able to mobilize sufficient trust, and thus deprive us of a promising, and maybe the only, possible way to regulate and make more secure, dynamic, complex networks. We argued that criminal procedural laws are a type of law that is ideally placed to contribute to both goals: By extending demands previously only relevant for the police to TC providers, they acknowledge it tacitly, that the TC provider is now a de-facto police force. In their wake come potentially more rights (such some forms of data retention that would otherwise be impermissible, and generally a Data Protection regime that is made to fit their policing function rather than their commercial role), but also more duties. These duties in turn should foster societal trust – just as we allow the police under some conditions to search our dwellings, we protect ourselves against the abuse of this power by chain of custody requirements, we could, as we discussed, impose on TC a stringent chain of custody regime – as one worked-through example amongst many that are imaginable.

But as much as the TCI can be co-opted into policing, and as much as it looks as if it is taking on state function, it remains of course in law a private sector entity, and the direct relations with its customers are mediated through private law in general, and contract law in particular. Here, the same type of issue arise:

what type of private law is best suited to increase the acceptability of TC and the uptake of the technology, by creating rational trust. Second, what type of private law is best placed at responding to and rebalancing the power shifts and imbalances that TC creates? As with criminal procedural law, these two issues are intimately linked. If TC creates obvious power imbalances over its users, their trust will be limited and their willingness to buy into the technology will be limited. In this chapter, we therefore look at the private law side of the equation. Here too, we will argue that TC results in a shift in de-facto power that traditional law is not best placed in regulating. Liberal contract law in particular is still premised on the assumption of a “bargain between equals” where people freely decide to bind themselves in mutually advantageous relations. In his seminal analysis of the history of contract law, Horwitz writes:

“But where things have no “intrinsic value,” there can be no substantive measure of exploitation and the parties are, by definition, equal. Modern contract law was thus born staunchly proclaiming that all men are equal because all measures of in - equality are illusory“.¹

This classical liberal concept of contract with its emphasis on formal equality and freedom was of course always problematic, based on a fiction more than reality. Standard terms of contract, used by economically stronger parties to regulate the relationship with their customers, are the norm rather than the exception.² The typical response of the post-war, welfarist state was to use “good

¹ Horwitz, M. J. (1974). The historical foundations of modern contract law. *Harvard law review*, pp. 917-956. at pp 918-919.

² For a discussion see the early and still seminal work by Kessler, F. (1943). Contracts of Adhesion--Some Thoughts About Freedom of Contract. *Colum. L. Rev.*, 43, pp. 629. A more recent discussion can be found in Trebilcock, M. J. (1997). *The limits of freedom of contract*: Harvard University Press.

faith” provisions in contract law,³ or a notion of “unconscionability”⁴ as a road towards stricter scrutiny of the validity of individual contract clauses by courts, sometimes at the instigation of consumer groups or state-appointed ombudsmen or watchdogs.⁵ This opened up the development of a consumer protection law that allowed a degree of benign paternalism,⁶ protecting consumers if necessary from themselves. Modern technologies have brought these age-old questions into new and sharper relief. As automated contract formation is becoming more and more the norm, the notion of “free choice” and “meeting of the minds” looks increasingly outdated in an algorithmic society. When your fridge contracts with your supermarket the next beer delivery, limitations on the computational capacities alone, will mean that both sides cannot but utilize rigid, pre-

-
- ³ See for the US in particular. Summers, R. S. (1968). " Good Faith" in General Contract Law and the Sales Provisions of the Uniform Commercial Code. *Virginia Law Review*, pp. 195-267. For a comparative analysis of approaches within the EU, see Collins, H. (1994). Good faith in European contract law. *Oxford Journal of Legal Studies*, pp. 229-254. and also Zimmermann, R., & Whittaker, S. (2000). *Good faith in European contract law*: Cambridge University Press.
- ⁴ On this approach see the highly influential study by Leff, A. A. (1967). Unconscionability and the Code. The Emperor's New Clause. *University of Pennsylvania Law Review*, pp. 485-559. with an ultimately skeptical conclusion as to their efficiency in addressing inequality. Empirical data on the use of the concept by contemporary courts showing their limited role in the present day can be found in a very recent skeptical appraisal is in Fleming, A. (2014). The Rise and Fall of Unconscionability as the 'Law of the Poor'. *Georgetown Law Journal*, 102(5), pp. 1383-1441. For an economic analysis see Epstein, R. A. (1975). Unconscionability: A critical reappraisal. *Journal of Law and Economics*, pp. 293-315.
- ⁵ For a critical analysis of the different types of institutional arrangements that can «pre-approve» fair standard terms see in particular Becher, S. I. (2009). A'Fair Contracts' Approval Mechanism: Reconciling Consumer Contracts and Conventional Contract Law. *University of Michigan Journal of Law Reform*, 42, pp. 747-804.
- ⁶ See e.g Shiffrin, S. V. (2000). Paternalism, unconscionability doctrine, and accommodation. *Philosophy & Public Affairs*, 29(3), pp. 205-250.

determined protocols and standards.⁷ How “good faith” between machines should be understood remains an open problem.⁸

At the same time, the Information Society poses new dilemmas for the concept of “good faith” too. Unequal access to information was traditionally a “trigger condition” for good faith scrutiny: If an elderly widow enters into a commercial contract with a bank, then the bank’s vastly superior knowledge of the risks that come with this transaction trigger specific duties, such as a duty to follow accepted guidelines in informing the client about risks (even if this is to the detriment of the bank), or even the prohibition of some clauses that exploit this information asymmetry altogether. But in an information society, what does this “asymmetric access to information” even mean? The Internet also comes with a promise to democratize access to information, and undoubtedly, never before was so much information quickly, cheaply (for free) and ubiquitously available to so many. True, this revolution came with its own inequalities, and the “digital divide” creates a new underclass of the information poor.⁹ But in the context of TC contracts, this is by definition irrelevant – anyone considering buying TC protection by definition is online and connected. Exploitative terms and conditions then should be much less common in this new world, where customers

⁷ See on this problem in particular Allen, T., & Widdison, R. (1996). Can computers make contracts. *Harv. JL & Tech.*, 9, pp. 25. , Weitzenböck, E. M. (2001). Electronic agents and the formation of contracts. *International Journal of Law and Information Technology*, 9(3), pp. 204-234.

⁸ See e.g. Weitzenböck, E. M. (2004). Good faith and fair dealing in contracts formed and performed by electronic agents. *Artificial intelligence and law*, 12(1-2), pp. 83-110. For another approach that analyses “good faith” through the comparison of team playing, see Schafer, B. (2003). *It’s just not cricket-RoboCup and fair dealing in contract*. Paper presented at the Proceedings of the Law and Electronic Agents workshop (LEA’03) (pp. 33-46),

⁹ For a comprehensive introduction to this issue, that for the reasons stated goes beyond the scope of this thesis, see Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*: Cambridge University Press.

can much more easily compare notes and challenge abusive terms.¹⁰ This is a development that was hinted at by the Oxford philosopher Luciano Floridi, who predicted that in the Information Society, everybody will be deemed to know everything, and hence ignorance ceases being an excuse.¹¹ If this prediction is true, then “good faith” as a protective mechanism for those on the weaker side of information asymmetry will lose much of its bite, and that at a time when wider economic developments have left demonstrably to a greater and greater reluctance by courts to use this avenue.¹²

We will be taking a somewhat different approach in this thesis. Undoubtedly, consumer contract law and a paternalistic “good faith” based approach, also matters for the contracts that bind customers to their TC providers. However, we argue that issues created by TC go well beyond such a mere fix. TC is a game changer, with qualitative, not just quantitative new issues that require a more radical rethink of the regulatory environment. First, we argued that not only is the TCI as constituted a monopoly or cartel-like structure that has already proven quite apt at imposing their standards on smaller competitors, more importantly, TC itself, as a concept is based with necessity on a “monoculture” where herd

¹⁰ So optimistically Chari, N. V. (2010). Disciplining Standard Form Contract Terms Through Online Information Flows: An Empirical Study. *NYUL Rev.*, 85, pp. 1618. Similarly Peppet, S. R. (2011). Freedom of contract in an augmented reality: The case of consumer contracts. *UCLA L. Rev.*, 59, pp. 676-745. with a special focus on one specific technology, augmented reality.

¹¹ Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology*, 1(1), pp. 33-52. at p. 35

¹² on the decreasing importance of “good faith” and “Unconscionability” as legal mechanisms to reign in unfair contract terms, see e.g. Fleming, A. (2014). The Rise and Fall of Unconscionability as the 'Law of the Poor'. *Georgetown Law Journal*, 102(5), pp. 1383-1441. An empirical study of US courts shows a more mixed picture, though even in this study, “not as bad as it might be” is the overall result. See Landrum, S. (2014). Much Ado About Nothing?: What the Numbers Tell Us About How State Courts Apply the Unconscionability Doctrine to Arbitration Agreements. *Marquette Law Review*, 97(3), pp. 751-812.

immunity is gained by everybody being forced to participate. Market pressure and choice, the tools suggested by libertarian contract lawyers to ensure fairness, are therefore systematically disabled. Indeed, the “force” employed by TC goes beyond this, and prevents users from changing their own computer in ways they might prefer. Classical notions of consent become even more untenable in this environment. Affected by this power imbalance are not just individual citizens, the traditional subjects of consumer protection law, but also technology companies outside the TCI group, so that for this reason alone traditional contract law is insufficient. By the same token, this uniform, monopolistic approach is *necessary* to achieve the desired security effects, and thus fulfills a socially highly desirable goal. Using the blunt force of anti-competition law and breaking up the TCI to re-create a market, would be undermining the very purpose of the initiative, as would be duties to open up their standards and methods (as security relies partly on secrecy). Even greater power imbalances and information imbalances are therefore a necessary feature of the TC environment. This brings us to the second and more fundamental reason why an approach looks at individual clauses in a TCI contract through the lenses of good faith. Here we return briefly to Guadamuz’ analysis of the Internet as a complex dynamic network. Guadamuz juxtaposes in his analysis the early cyber-libertarianism with the more recent (apparent) successes “resurgence of the regulatory state”. Citing John Perry Barlow’s Declaration of Independence of Cyberspace, one of the early “regulation sceptics”:

“Governments of the Industrial World [...] Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.”¹³

he notes that in retrospect, such sentiment sounds naïve and unrealistic.¹⁴

¹³ Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace, . Retrieved 25/8/2015, from <http://homes.eff.org/~barlow/Declaration-Final.html>

¹⁴ Guadamuz op cit. p.84

He contrasts this with James Boyle's dictum that

"the idea that the technological changes of the digital revolution are always outside the control of the state seems unproven. In fact, the state is working very hard to design its commands into the very technologies that, collectively are supposed to spell its demise."¹⁵

and notes the considerable impact, at least in terms of laws that states enacted and enforced. However, when he then looks at the long term effects of this enforcement, his verdict becomes again more ambiguous: success seems to be at best temporary and not sustainable, crime, especially copyright violations, remain endemic. In his analysis, which this thesis embraces, the problem is not the international nature of the Internet. While it certainly complicates issues, it is not the root of the problem. Neither is it the difficulty of legislation, relatively slow, cumbersome and eternally reactive, to anticipate technology as such. Rather, the problem lies in the specific nature of complex networks. One quote from Strogatz that he gives is particularly relevant:

"scale-free networks are resistant to random failures because a few hubs dominate their topology. Any node that fails probably has small degree (like most nodes) and so is expendable."¹⁶

This feature protects the Internet from attack, but it also protects cyber-criminal networks that match its structure. TC in turn aims at a network of trust that is isomorphic to the Internet, does not even try to attack individual nodes of criminal activities in isolation, and thus circumvent the problem of their resilience. Security becomes an emergent property, not reducible to individual machines, friendly or unfriendly, or individual nodes.¹⁷ There is an extended debate on philosophy about the meaning of emergence, and to what extent it is a

¹⁵ Boyle, J. (1997). Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors. *U. Cin. L. Rev.*, 66, pp. 177.

¹⁶ Strogatz, S. H. (2001). Exploring complex networks. *Nature*, 410(6825), pp. 268-276.

¹⁷ Guadamuz op cit p. 39ff

legitimate concept. An overview of the discussion can be found in the recent treatise by Jochen Fromm.¹⁸ For the discussion here we only need to accept, for the sake of the argument, that complex dynamic systems have emergent properties, properties that cannot be reduced easily to properties of their constituent parts (in the way in which a mass of gas will have a mean temperature which cannot be predicted by looking at individual gas molecules). But the legal framework that it is using for this, classical contract law, is inherently reductive, reducing all legal relations to ultimately binary relations between two parties and two parties only.

The problem, then, is not just that TC providers are in a dominant bargaining position, which could be mitigated by a strong interventionist good faith jurisprudence that rewrites if necessary the contract for the parties. It is also not (just) an increasingly problematic concept of freely given consent that is undermined by increasingly automated contract performance, though this too is exacerbated by TC and its reliance on automated verification and authentication. Rather, it is the very nature of contract, not its substance but its form, that is the problem. Contractual relations, as we will see in more detail later, reduce a conflict to a dispute between two parties, and privacy of contract ensures that third party interests are bracketed out. But networks should be all about third parties – to have power laws requires transitive relations where everybody is connected to everybody, and everybody is affected by everybody, and be it by “six degrees of separation”.

It is this idea that the thesis tries to develop over the next section. We will first recast some of the problems from the last chapter in the language of private law and private law relations, using again some small case scenarios. We will then show how these issues are traditionally framed in contract law, backing up the theoretical study with some small scale empirical research conducted by the

¹⁸ Fromm, J. (2004). *The emergence of complexity*: Kassel university press Kassel.

author with TC developers. We will then introduce what we consider to be two independent building blocks of a better way to understand the role of private law in regulating and facilitating complex dynamic networks: On a theoretical level, we will suggest to understand the contract between TC vendor and seller not in the traditional, atomistic way as a one off exchange that affects two parties and two parties only, but through the lenses of “relational contract theory”. On the practical level, we suggest using the concept of “reliance liability” as a cornerstone of TC regulation through private law. Reliance liability, or third party liability, breaks open the atomistic binary relation of classical private law and “brings in” third parties into the emerging trust network.

4.2 Setting the scene

Even though individual use of computers today is becoming ever more widespread and we use computers increasingly in all fields of our daily lives, our knowledge about computers, and computer security in particular, has failed to match this development. We use e.g. smartphones for much more than making voice calls, they are for more and more citizens an essential tool to access government services, carry out essential financial transactions or access information that directly informs their decision making. Worryingly, this increased reliance on the ubiquitous availability of information resources also results in de-skilling of non-digital skills, making us more and more reliant on the proper performance of our information tools, and therefore even more vulnerable should they become under attack.¹⁹ Despite this, security awareness

¹⁹ A particularly drastic example is discussed in Aporta, C., & Higgs, E. (2005). Satellite culture: global positioning systems, Inuit wayfinding, and the need for a new account of technology. *Current Anthropology*, 46(5), pp. 729-753. which shows emerging reliance on the availability of ICT in some of the world’s most dangerous environments, and the loss of pre-technology skills. For navigation skills in western societies, see Leshed, G., Velden, T., Rieger, O., Kot, B., & Sengers, P. (2008). *In-car gps navigation: engagement with and disengagement from the environment*. Paper

remains low, we see the smartphone as not much more dangerous (or vulnerable to outside attacks) than the traditional telephone, where the greatest danger are fraudulent calls.²⁰ Even with high-education, high industrialization countries such as the EU, this leaves a bitter taste, with 50% confessing to little or no digital skills in 2012.²¹ This draws a picture where although ICT has become widely available during the last decade, computer skills and therefore computer literacy are far behind the expected standards.²² As a consequence, it is unsurprising to learn that too many users do not update their protection regularly, or use bogus anti-virus software²³ (aka scareware)²⁴, or decide not to protect themselves at all. Moreover, with the discovery of zero-day vulnerabilities and Flame – described as “the most complex malware ever found” –²⁵ MIT suggests that the Antivirus

presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1675-1684),ACM.

- ²⁰ So e.g. the study by Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, pp. 47-66. which suggested “security profiling” on the basis of their findings.
- ²¹ Koniotou, M. (2013, 14/10/2013). EU Commissioner stresses need for digital skills, *Cyprus News Agency*. Retrieved from <http://www.cna.org.cy/webnews.asp?a=6304a8e0a2fd4321ba4b9c697231faee>
- ²² European Commission. (2013b). "Information society statistics" - Statistics Explained Retrieved 15/10/2013 http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics#
- ²³ Graham, C. (2013, 21/1/2013). Fake anti-virus attack spread via bogus ADP anti-fraud update emails, *Naked Security*. Retrieved from <http://nakedsecurity.sophos.com/2013/01/15/bogus-adp-anti-fraud-update-emails/>
- ²⁴ See for an analysis of scareware Holtfreter, R. E. (2011). Scareware Fraud: All Trick and No Treat?(part 1). *Fraud Magazine*.
- ²⁵ sKyWIper Analysis Team. (2012). sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks (Vol. v1.05): Laboratory of Cryptography and System Security (CrySyS Lab)

era is over.²⁶ While this would be tolerable if negligent users only harmed themselves – we do not after all make security locks for our houses compulsory –²⁷ the nature of online threats means that such an individual poses not just a danger to himself, but also to others. Infected computers are the main element of a botnet²⁸, which in turn enables the type of large scale Denial of Service (DoS) attack that threatens the very existence of the net.²⁹ Additionally, botnets are a major source of spam, spyware, adware, click-fraud, access number replacements, and fast flux, mostly driven by the botmasters' financial interests and secondly used in political or military contexts.³⁰ Overall in 2011, botnets

²⁶ Simonite, T. (2012). The Antivirus Era Is Over, *MIT Technology Review*. Retrieved from <http://www.technologyreview.com/news/428166/the-antivirus-era-is-over/>

²⁷ this statement may need qualification in the light of what we discussed in chapter 2. While locks are not legally mandated, insurance companies can penalize you for being negligent.

²⁸ Botnets are networks formed by infected compromised machines which connect to a central server and compromise the host system. The European Network and Information Security Agency (ENISA) – the EU's cyber security agency, provided a comprehensive report on how to assess botnet threats including various types of best-practices to measure, detect and defend against botnets and recommendations on how to neutralise them, preventing new infections and minimising cybercrime profitability from botnets use. The document also examines the role of governments in the fight against botnets, and points out what legislation is needed and what investment is required Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, Measurement, Disinfection & Defence. In G. Hogben (Ed.), *ENISA's Emerging and Future Risk programme* (pp. 153): European Network and Information Security Agency (ENISA). Rajab *et. al* present challenges on botnet detection and tracking and an approach to infiltrate large numbers of botnets in Rajab, M. A., Zarfoss, J., Monroe, F., & Terzis, A. (2006). *A multifaceted approach to understanding the botnet phenomenon*. Paper presented at the Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, Rio de Janeiro, Brazil. .

²⁹ Bayer, U., Habibi, I., Balzarotti, D., Kirda, E., & Kruegel, C. (2009). *A view on current malware behaviors*. Paper presented at the LEET'09: Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more, Boston, MA, USA. http://www.eurecom.fr/people/vs_bayer.en.htm

³⁰ Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, Measurement, Disinfection & Defence. In G. Hogben (Ed.), *ENISA's Emerging and*

produced approximately 81.2% of all spam.³¹ Recent statistics presented by Eurostat, demonstrate that 31% of internet users in the EU27 caught a computer infection which resulted in loss of information in the last 12 months of 2011.³²

A key argument of this thesis is that while TC aims to eventually provide a more secure and trustworthy technological solution for the benefit of the user, the price is a massive shift of power to the software providers. Unless a computer is TC certified, its usability will be severely hampered. Customer choice of software, especially Open Source Software (OSS), will as a result be curtailed. As we indicated above, this alone is sufficient to call into question the adequacy of traditional contract law and its underlying rationale of free choice exercised by rational market actors. The TC provider will also have unprecedented access to user's hard drives, and the ability not only to extract information, but also to reconfigure the software. With such great powers, great responsibility should come, with a role for the law to address the arising ethical concerns and rebalance the interplay of power and responsibility. In short, governments (and citizens) should accept this power shift and its consequences only if a corresponding increase of responsibility occurs in the side of the TC provider.

Conceptually, we argued in the previous chapter that the TC approach has aspects of a part privatization of what is in the online world, a *core state function*. We also argued that as a result some public law concepts could be fruitfully extended to TC. Care must be taken however to not overextend this analogy. Ultimately, the way TC provider and TC user relate with each other is through contract. While we will talk in legal theory about the "social contract" that gives

Future Risk programme (pp. 153): European Network and Information Security Agency (ENISA), Wikipedia. (2011, 16/7/2011). Botnet. Retrieved 28/6/2011, 2011, from http://en.wikipedia.org/wiki/Botnet#Types_of_attacks

³¹ Symantec. (2012). Internet Security Threat Report. In P. Wood (Ed.), (2012 ed.): Symantec Corporation World Headquarters.

³² Eurostat. (2011). Nearly one third of internet users in the EU27 caught a computer virus 8 February 2011: *Safer Internet Day*. Luxembourg: Eurostat Press Office.

rise to society, we do not normally, in law, conceptualise the relation between a citizen and the police as contractual. If I'm burgled, I cannot normally sue the police for breach of contract, even if they fail to apprehend the guilty party – the “social contract” is not directly enforceable that way. Neither is a tort law action normally available, as courts in the UK have been historically averse to impose liability for “non performance” on public bodies.³³ Back in 1924, Edward Borchard summarises the position for the common law tradition as:

"obviously, the administration cannot be held to obligations of guaranteeing the citizen against all errors and defects, for life in an organised community requires a certain number of sacrifices and even risks".³⁴

This has remained due to this day. In the case of *Hill v Chief Constable of West Yorkshire*³⁵ the police succeeded to have the claim that they were negligent in investigating the Sutcliff murders struck out, since, the police owed no duty of care to individual citizens in the detection of crime. In a similar vein *Capital and Counties plc v Hampshire County Council* decided that a fire brigade only owed a duty of care if they inflicted damage on the property of an arson victim that would not have otherwise occurred (i.e. if they made things worse), but not for failing to prevent or effectively fight the fire.

The rationale behind these exemptions are policy driven – imposing liability on public bodies would be a strain on the public purse, the police getting tied down in litigation with individual citizens, resource allocation would be done not

³³ Hartshorne, J., Smith, N., & Everton, R. (2000). 'Caparo Under Fire': a Study into the Effects upon the Fire Service of Liability in Negligence. *The Modern Law Review*, 63(4), pp. 502-522. doi: 10.1111/1468-2230.00277

³⁴ Borchard, E. M. (1924). Government Liability in Tort. *Yale Law Journal*, pp. 1-45. at 1 for a more recent discussion see McMahon, M. (1992). Dangerousness, confidentiality, and the duty to protect. *Australian Psychologist*, 27(1), pp. 12-16. and Giliker, P. (2000). Osman and police immunity in the English law of torts. *Legal Studies*, 20(3), pp. 372-392.

³⁵ *Hill v. Chief Constable of Yorkshire*, 1988 238 (A.C. 53 1988).

to prevent or solve the most pressing crimes, but to prevent litigation etc. One question that then opens up is if we should extend such a general immunity to TC – under the assumption that our analysis in the preceding chapter was convincing, and that the monopoly position, together with the task to ensure the safety of a critical infrastructure, makes the TC provider sufficiently like a “public sector authority” to apply rules in analogy. In that case, the TC providers (and by implication, the entire IT industry that operates to TC compliant standards) would get blanket exemptions from liability when their products fail to deliver. Conversely, one could consider extending also some of the specific duty of the public sector, or the privatized utilities, to TC, such as some “non-discrimination” duties, duties to contract, or, most radically, even some upper limit on possible profits or price rises.³⁶

There might be some appeal in this approach. As we discussed, should TC become successful, then people whose computers are not TC certified will lose access to the Internet. As we increasingly consider access to the Internet a basic civil right,³⁷ a situation where excessive costs for TC protection could force people off the net (if you can’t afford the security, your computer will get access denied) together with the monopoly status of the TCI, would bring them very closely to a privatized water utility in terms of the power they yield and the social impact they have. This, however, is not the route we will go down in this thesis.

³⁶ For a discussion of the regulation of the privatized utilities in the UK, see e.g. Beesley, M. E., & Littlechild, S. C. (1989). The regulation of privatized monopolies in the United Kingdom. *The RAND Journal of Economics*, pp. 454-472. Even closer to our example, a discussion of privatised policing and the liability regime can be found in McBeth, A. (2004). Privatising Human Rights: What Happens to the State's Human Rights Duties When Services are Privatised. *Melb. J. Int'l L.*, 5, pp. 133.

³⁷ See e.g. Best, M. L. (2004). Can the internet be a human right. *Human Rights & Human Welfare*, 4(1), pp. 23-31. , Lim, Y. J., & Sexton, S. E. (2011). Internet as a human right: a practical legal framework to address the unique nature of the medium and to promote development. *Wash. JL Tech. & Arts*, 7, pp. 295. , Skepys, B. (2012). Is There a Human Right to the Internet. *J. Pol. & L.*, 5, pp. 15.

While as we will see there is some pressure emanating from Parliament to ensure the safety of the Internet through a combination of state investment on the one hand, increased liability for software developers on the other, there seems to be no appetite for state involvement that is either direct (“nationalizing Internet security”) or even indirect through creating a sui generis regulatory regime similar to the banking sector.

By contrast, there might be some scope to “nudge” TC companies even in a monopoly position to responsible behavior, by adjusting gradually and incrementally the civil liability regime. Contracts can be used as a regulatory tool, as a way to build societies.³⁸ This need does not result in a radical individualism, an approach called “Contractarianism” by Jean Braucher.³⁹ Braucher remains critical of the neo-liberal over-emphasize on contracts as regulatory tools to build societies, also because it fetishizes free choice in environments where little of it is to be found. As our discussion above shows, this is particularly pertinent in an environment with automated contract formation, systemic information asymmetries and monopoly power.

With TC, safety becomes a commodity, and its exchange is primarily governed by contract. This of course is not something entirely new – customers already “buy” safety offline and online, through private security firms or safety locks to their houses, and through products such as Intrusion detection systems, firewalls and anti-virus software online. For these traditional countermeasures, the operation of efficient free markets justified a cautious approach when imposing liability, letting alone other duties such as a duty to contract, giving the providers a large free reign to compete not just on issues of reliability and security, but also on the degree in which they offer guarantees and compensation.

³⁸ So e.g. in Schäfer, B., & Bankowski, Z. (2003). Emerging Legal Orders. Formalism and the Theory of Legal Integration. *Ratio Juris*, 16(4), pp. 486-505.

³⁹ Braucher, J. (1990). Contract Versus Contractarianism: The Regulatory Role of Contract Law. *Wash. & Lee L. Rev.*, 47, pp. 697.

At present, users can choose between a variety of competing products or none at all, if they conclude that the costs of protection outweigh the risks of an attack. Their computer could remain fully operational and capable of interacting with the Internet regardless of their choice. If they suffer harm from a cheap product, or by refusing any protection, the loss lies entirely with them. On the other side of the coin, most if not all antivirus software producers make it clear that their system merely *increases* safety, but cannot entirely prevent threats, both from a technical standpoint as well as from bad security policies and procedures that are in place.⁴⁰ Just as a doctor doesn't guarantee your health as a result, but only to provide means to make you healthier, so does TC promise only a means to make you safer, not safety as such. Clauses to that effect will typically be found in the Standard Terms and conditions, the "boilerplate" of the contract that we never read and always sign and agree with. By this, they minimize contractual liability, while potentially of course remaining liable in tort – e.g. when it can be proven that they have acted gross negligently, e.g. by infecting user's computers with a new virus that had been analyzed in their lab, but through careless handling found its way into their latest updates.

It is this convergence of issues that is behind our discussion here: If TC were to operate always faultlessly, offering total protection, issues of liability would, trivially, not arise. On the other hand, if TC was just a market competitor amongst many others, the traditional method of regulation through markets, backed up, as necessary with a robust consumer protection law to address information imbalance, would suffice. But TC cannot guarantee security – remember the discussions of different meanings of trust and security. But it requires, ultimately, a monoculture where the user, the main security risk, is heavily restricted in

⁴⁰ Arief, B., & Besnard, D. (2003). Technical and Human Issues in Computer-Based Systems Security. *TECHNICAL REPORT SERIES- UNIVERSITY OF NEWCASTLE UPON TYNE COMPUTING SCIENCE*(790), Symantec. (2012). Internet Security Thread Report. In P. Wood (Ed.), (2012 ed.): Symantec Corporation World Headquarters.

his/her choices. It is this combination of factors that requires revisiting the issue of civil liability in a TC context.

To recap the crucial concept discussed at length in chapter 2: In a TC world, my computer can “trust” other computers that identify themselves as “Trusted Computers”, and in turn is trusted by them. If the system fails, three possible scenarios occur:⁴¹

- A. My TC system does not operate as specified, for instance due to a bug preventing me from accessing my own files altogether. This is a classical contract law issue, and while the discussion on software liability is complex and complicated, with “liability exclusion clauses” of often dubious enforceability in abundance, it raises no new *conceptual* questions.
- B. My TC system behaves as specified, but is outwitted by an attacker. I in turn have behaved with (even less) safety awareness than before TC was introduced, relied totally on the TC protection, and suffer as a result a loss (by downloading e.g. malware). This remains at first sight a contractual issue between me and the TC provider, but under current law, my position is weak. However, as we argued, the *need* to use TC and the *inability* to make my own security arrangements mean that there is a social trade off involved that the law, possibly, should recognize.
- C. Someone else, relying on my computer’s malfunctioning certificate, downloads harmful software from me. Does this third party have any claims against *my* TC provider, given that he acted in reasonable reliance on the TC

⁴¹ We will touch on the issue of software liability again below, but only in passing. A more comprehensive discussion can be found in an early paper by Voas, J., McGraw, G., Kassab, L., & Voas, L. (1997). A ‘crystal ball’ for software liability. *Computer*, 30(6), pp. 29-36. An interesting new dimension to this discussion is in Reutiman, J. L. (2012). Defective Information: Should Information Be a Product Subject to Products Liability Claims. *Cornell JL & Pub. Pol’y*, 22, pp. 181. , which expands the scope of the discussion beyond software to information in general.

certificate? This is the most radical conceptual issue that TC raises: do TC providers incur liability outside the contractual nexus? This is also the question that links this chapter to the previous one: For *if* we accept that TC owes a duty of care not just to its own customers, but also to third parties that rely on their certification, the similarity to a public sector agency such as the police becomes clearer. Furthermore, we will argue that this method of “breaking out of” the contractual atomism is a way to create network structures of legal liability that come closer in matching the trust network that TC tries to build up, and thus in turn the Internet.

We will visit each one of these scenarios in the next sections and we will try to examine the contractual relation found in scenario B and from the proposed scenario of reliance liability for scenario C.

4.2.1 Contractual relation between buyer and seller

Liability for faulty software is an area of considerable legal controversy, not least because it remains unclear in UK law whether software is to be treated as a good, a service, or something else. The distinction is, seemingly, important because it determines the nature and scope of liability that can be derived from a contract, and also to some extent what can be legitimately excluded by contract. Trusted Computing further complicates the issue because a failure in such a system may be hardware or software related. As we saw in chapter 1, it is a crucial novelty of the TC approach to security that as Epstein noted “security software is not enough for software security solutions”,⁴² and thus hardware and software have to work in unison.

⁴² Epstein, J., Matsumoto, S., & McGraw, G. (2006). Software security and SOA: danger, Will Robinson! *IEEE Security & Privacy*(1), pp. 80-83.

Hardware is clearly a good⁴³ - if software is deemed to be a service or *sui generis* in nature, this suggests that different components of the TC concept might be held to different standards. This would be problematic enough if faults in hardware and software could be neatly separated analytically. For TC, this is highly doubtful. As the discussion in the first chapter showed, the various TC components rely on each other and are essentially intertwined. This raises the very real possibility that each component works correct on its own terms, but still, once combined, fall short of what is expected from them. We suggest that potentially, a much better way is a “gestalt switch” that sees TC as neither “just” software nor “just” hardware and moves away from the mere *tools* that TC utilizes to a goal-oriented characterization. The “business” of the TCI, so to speak, is security. Security is what they sell, and the methods they use for this are merely coincidental. When hiring a security company for physical protection, we do not need to worry who build their guns or who provides the network service for their communication equipment. They promise my safety, I trust and can rely that they use the right tools for the job. In the field of IT security, this notion of “security as a service” has recently gained traction in the field of cloud computing.⁴⁴ Trusted computing has indeed been characterized as one such “security of service provision” in cloud environments.⁴⁵ The legal implications of this conceptualization have not yet been fully explored, but it is maybe not surprising that the idea of TC as a “security as a service” (SECaas) solution should emanate from cloud environments. Unlike the traditional customer buying a physical PC

⁴³ Bradgate, R. (1999). Beyond the Millennium - The Legal Issues: Sale of Goods Issues and the Millennium Bug. *The Journal of Information, Law and Technology (JILT)*, 2. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_1992/bradgate/.

⁴⁴ See e.g. Hussain, M., & Abdulsalam, H. (2011). *SECaas: security as a service for cloud-based applications*. Paper presented at the Proceedings of the Second Kuwait Conference on e-Services and e-Systems (pp. 8), ACM.

⁴⁵ Kaufman, L. M. (2010). Can a trusted environment provide security? *Security & Privacy, IEEE*, 8(1), pp. 50-52.

and installing software on it – “real” activities that make us think immediately of “buying software” or “buying hardware”, the virtual environment of the cloud strips us off these preconceptions and allows us to see things as they really work. We will return to this idea of TC as “security as a service” bundle below.

It has been suggested in the past that a more rigid liability regime would provide the right type of pressure to software vendors to improve software security and to ensure that the software provides the security it should provide.⁴⁶ Commissioners Viviane Reding and Meglena Kuneva proposed that “Licensing should guarantee consumers the same basic rights as when they purchase a good: the right to get a product that works with fair commercial conditions”.⁴⁷ The rights of a purchaser of a physical product - which are familiar to us - along with the implied terms, are significant and are found in sections 12 to 15 of the Sale of Goods Act.⁴⁸ These state, among others, that the goods supplied should correspond with their description and are of satisfactory quality and reasonably fit the buyer’s purpose. Contracts of sale such as those we just described are legislated under the Sale of Goods Act, and legislation has extended the scope of application to apply to all forms of contract arrangement by which goods are supplied.

These rights are probably the ones best understood by both parties of a contract (consumers and retailers) and are arming the consumer in possible

⁴⁶ EC. (2009). Consumer Rights: Commission wants consumers to surf the web without borders. (IP/09/702). http://europa.eu/rapid/press-release_IP-09-702_en.htm#PR_metaPressRelease_bottom, Espiner, T. (2009). EC wants software makers held liable for code, *ZDNet UK*. Retrieved from <http://www.zdnet.co.uk/news/it-strategy/2009/05/08/ec-wants-software-makers-held-liable-for-code-39649689/>. For a comparative, academic analysis see August, T., & Tunca, T. I. (2011). Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science*, 57(5), pp. 934-959.

⁴⁷ EC. (2009). Consumer Rights: Commission wants consumers to surf the web without borders. (IP/09/702). http://europa.eu/rapid/press-release_IP-09-702_en.htm#PR_metaPressRelease_bottom

⁴⁸ Sale of Goods Act § c.54 (1979).

breach of the contract by the retailer. Our courts too seem to remain in a pre-information age, at least conceptually – we understand physical objects much better than abstract information objects such as software. Even in cases where undoubtedly, the issue was a software fault, empirical studies also indicate that courts are much more likely to hold a software vendor liable for harm if the software was part of a physical machine had caused physical harm, and are less likely to apply the same rules to software flaws that remain “unseen and virtual”, such as ID theft due to weak security.⁴⁹ Despite the increasing significance and explosive growth of the economic importance of the digital products and digital technology, the application of these legal requirements over this type of products still remains ambiguous. This “selective” application of the law which distinguishes digital products from the existing legislation creates a risk that the consumer of such products may be exploited by suppliers to deny consumers’ rights, or may be denied any protection of the law and that way may deprive the rights that consumers enjoy.

In its White paper the UK government committed itself to take actions “which will enhance and protect consumer rights in a changing world” in relation to digital products (including computer software) and that will take the appropriate actions so that all principles applying to (physical) sales will also apply to digital products.⁵⁰

In an influential study, Chandler analyses two approaches where the law can be used to intervene in the software development process to provide the standards that the end-user demands. The first approach is the use of regulations or laws to overcome market failures (i.e. where the market fails to put pressure on manufacturers to produce more secure software, such as in a monopoly

⁴⁹ A typical example is the reasoning in *Petry v. Cosmopolitan Spa Intern., Inc*, 641 S.W.2d 202 (Tenn: Court of Appeals, Eastern Section 1982).

⁵⁰ Cm7669. (2009). *A Better Deal for Consumers - Delivering Real Help Now and Change for the Future*. (ID 6192113 07/09). London: The Stationery Office.

situation) by mandating minimum security standards. This has a number of disadvantages not least that a law may be too broad in its reach if applied uniformly across the software marketplace, because there are different levels of risk in different types of programs and it would be unrealistic to expect them to meet the same design standards.

The second approach is “to impose liability for negligently-designed software”. This approach has some advantages like that the care needed from software developers can vary according to the context and therefore “software intended for use in conditions where design flaws may lead to substantial losses may be treated differently from software that does not present high risks”.⁵¹

Chandler notes that applying a negligence standard to software security might be a way forward, but specifically warns that taking that path might cause the software industry to take measures that while improving security could have other, less desirable implications. Here she specifically refers to TC and the types of concerns noted above - the loss of consumer freedom and the implications for competition. She also notes (in the context of DDoS attacks) that, currently, purchasers may find it difficult to sue vendors for liability for damage caused by their product's failure. Firstly, license terms disclaiming or limiting liability may affect possible lawsuits. Secondly, users may face counterclaims of contributory negligence if they did not maintain properly their security by patches or virus scanning.

The liability question that TC creates can therefore be turned into four separate issues:

- is software a good, a service or *sui generis*?

⁵¹ Chandler, A. J. (2003). Security in Cyberspace: Combatting Distributed Denial of Service Attacks. *University of Ottawa Law and Technology Journal*, 1(1-2), pp. 231-261.

- what are the implications for TC if the hardware and software components carry different liabilities, and should we think of TC better as “security as a service”, independent from tools used?
- is the current level of liability exposure for producers in the event of hardware and software failure, appropriate for TC?
- what are the implications for TC of a higher level of liability?

4.2.1.1 Software as Good

The Sale of Goods Act implies terms into contracts for the sale of goods in (ss.12-15).⁵² These implied terms aim to express the intention of the parties and can be helpful in the case where a user purchases defective software if such software is categorized as goods. For us, they are the door through which the consumer perception of “trust” and “security” that we discussed in the second chapter can be given legal voice. We noted there, the systematically diverging perceptions of “trust” and “security” between lay people and computer professionals. In an environment where contracts will be typically boilerplate and written from the perspective of the better informed party, this type of purposive reading can unearth again the meaning that the weaker, less informed party gave to the meaning of the transaction. Normally, software is not explicitly categorized as a good, unless it is part of a system which involves the use of software and hardware.⁵³ While this seems to apply, *prima facie*, to TC, the typical examples of “embedded software” have a somewhat different form, e.g. the software in a digital radio that makes it work. The relation between hardware and software components of TC, as we saw in the second chapter, is rather different. They are at the same time more complex in their possible interaction (one generating proof about the other) and more loosely connected, as a battery

⁵² Sale of Goods Act § c.54 (1979).

⁵³ Rowland, D., & Macdonald, E. (2005). *Information Technology Law* (Third ed.). London, UK: Cavendish Publishing.

of independent security measures. It is less the case of software “making the hardware doing things” as in the radio, but more a question of mutual dependencies.

In case of a breach of a condition the injured party has the right to reject the goods and claim damages. However, the Sale and Supply of Goods Act modifies the normal remedy in the case of breaches of ss.13-15 “conditions” and states that:

- 1) Where in the case of a contract of sale –
 - a. The buyer would, apart from this subsection, have the right to reject goods by reason of a breach on the part of the seller of a term implied by section 13, 14, or 15 above; but
 - b. The breach is so slight that it would be unreasonable for him to reject them, then, if the buyer does not deal as consumer, the breach is not to be treated as a breach of condition but may be treated as a breach of warranty.
- 2) This section applies unless a contrary intention appears in, or is to be implied from, the contract.
- 3) It is for the seller to show that a breach fell within subsection (1) b above.⁵⁴

The implied term dealing with fitness for the buyer’s purpose was originally dealt by section 14(1) of the SGA 1893. Nowadays, an amendment is contained in SGA 1979 and in there it is stated that:

Where the seller sells goods in the course of a business and the buyer, expressly or by implication, makes known –

- a. to the seller; or
- b. where the purchase price or part of it is payable by instalments and the goods were previously sold by a credit broker to the seller, to that credit broker,

⁵⁴ Sale and Supply of Goods Act § c.35 (1994).

any particular purpose for which the goods are being bought, there is an implied obligation that the goods supplied under the contract are reasonably fit for that purpose, whether or not that is a purpose for which such goods are commonly supplied, except where the circumstances show that the buyer does not rely, or that it is unreasonable for him to rely, on the skill or judgment of the seller or credit-broker.

In this statement we will analyze two terms that are crucial for the discussion. The first term is the one of “satisfactory quality”. By this term a standard quality is set for goods. Section 14(3) may result in the seller guaranteeing that goods will meet the needs of the buyer, whilst the above does not relate to the buyer’s intended use of goods.⁵⁵ The second reference to the “particular purpose” of the buyer mainly refers to the “specified purpose” for which the user buys the product.

Implied terms are quite significant as they arise automatically, they are easy to prove and they are classified as conditions which mean that in case of breach the consumer is entitled to a range of legal remedies including rejection of goods, demand a price refund, have the price reduced and return goods for repair or replacement. Yet, it is very rare for a consumer to take professional advice on a claim even for relative expensive items.⁵⁶ “In most cases, consumers do not complain because the financial loss is limited (42%), they do not expect to get a satisfactory solution to their problem (35%) and they consider it too time-

⁵⁵ Rowland, D., & Macdonald, E. (2005). *Information Technology Law* (Third ed.). London, UK: Cavendish Publishing.

⁵⁶ As recent statistics by Eurostat pp.104-105 Eurostat - European Commission. (2009). *Consumers in Europe* (2009 ed.). Luxembourg: Office for Official Publications of the European Communities. reveals that out of the consumers interviewed for the consumer satisfaction and complaints on the prices of products they purchased, only 16% of consumers in EU-27 made a formal complaint in form of writing, by telephone or in person during 2009. The most surprising though is that 51% of unsatisfied customers chose not to take any further action (e.g. in courts) and seeking advice by a solicitor appeared on the extremely low proportion of 9%.

consuming to complain (27%)”.⁵⁷ However, in the present context the essentiality lays in these last two implied terms points: the exclusion or limitation of liability for any condition breach is prohibited by civil and criminal law; and consumers and retailers who hold reasonable expectations, are all familiar with the implied terms included in the contract.

In order for a term to be implied, the buyer must rely upon the seller to provide goods which reasonably fit for the buyer’s particular purpose and furthermore it must be reasonable for the buyer to do so. There are two kinds of reliance: partial and non existence or non reasonable. The first one relates to the aspect of the goods’ fitness, which is relevant to the buyer’s claim, and the second one is valid if the buyer has the greater expertise or is in the best position to make an assessment for the goods’ suitability.

It appears from the above, that where there is a combination of hardware and software being sold together, the courts may treat the combination as a sale of goods. This may fit the TC scenario, depending upon the nature of the customer (business or consumer), the nature of the sale (once-off or continuing upgrades), and the purpose to which the equipment is put. Although software is the most obvious example of digital product, the boundaries are still blurred as software can be a wide category on its own.⁵⁸ Nevertheless, given the uncertainty surrounding software, it is appropriate to also consider other options.

4.2.1.2 Software as a Service

⁵⁷ Eurostat - European Commission. (2012). *Consumer Conditions Scoreboard – Consumers at home in the single market* (7th ed.). Luxembourg: Office for Official Publications of the European Communities.

⁵⁸ Bradgate, R. (2010). *Consumer Rights in Digital Products* (I. a. S. Department for Business, Trans.) *A research report prepared for the UK Department for Business, Innovation and Skills* (pp. 76). Sheffield: Institute for Commercial Law Studies, University of Sheffield.

It is possible that software could be regarded as a provision of services - this has been suggested in cases where a vendor has written software specifically for a client thus a “bespoke” product - the writing of the software being the service. This was the approach taken by the court in *The Salvage Association v CAP Financial Services Ltd*.⁵⁹ However in *St Albans City & District Council v International Computers Ltd*⁶⁰ the court held that where a computer program was delivered on a disk it might be both a good and a service.⁶¹

In terms of TC, it is clear that there are a number of issues to consider when considering the goods/services question:

- is the software a “bespoke” product written/adapted for a particular client or is it mass market software?
- if written for a particular client is it delivered as part of a purchase of hardware, or separately?
- does some other element, such as a continuing provision of automatic upgrades and other software changes suggest an ongoing service?

The answers to these questions can essentially change the way that the issue is approached as a “bespoke” product has more in common with the contract for professional services, yet a mass market software is “closer” to a physical product. To demonstrate the difference along with the means that the product is delivered, for example, Australian authorities in *Toby Constructions v. Computer Bar Sales* consider the hardware and software that is supplied as a package for sale, under one universal price, to be treated a single contract and it is classified as a sale of goods.⁶²

⁵⁹ *Salvage Association v. CAP Financial Services Ltd*, 1995 654 (1995).

⁶⁰ *St Albans City and District Council v. International Computers Ltd*, No. 1997-98, 1996 481, 1995 F.S.R. 1686 (All E.R.4 1996).

⁶¹ Bainbridge, D. (2005). The Nature of Software Contracts. *IP & IT Law*, 10.6(3), Singleton, S. (2003). Sale and Supply. *ITLT*, 11.2(11).

⁶² *Toby Constructions Products Pty Ltd. v. Computer Bar Sales Pty. Ltd* [case]. (1983). 2 NSWLR 48 (pp. 288).

Bainbridge suggests that the differences between goods and service where software is concerned are not so great, even after the passage of the Sale and Supply of Goods Act 1994. In essence, where the sale of goods legislation is concerned with quality and fitness for purpose, the provision of services legislation is concerned with the provision of a service using reasonable care and skill where reasonableness is generally regarded as at a relatively low standard of a "reasonably competent provider of the relevant services". In computer software terms, that does not require software to be entirely free from bugs or minor faults as held by the court in *Saphena Computing v Allied Collection Agencies*.⁶³

However, both commentators and the courts have suggested that computer software does not fit the existing legislation well due to the intangibility of the product, and the fact that it is usually licensed rather than sold outright. The Court in the *St Albans* case eventually decided the case by creating a new rule for software written specifically for a client of "fitness for purpose" even in the absence of a sale of goods, and Bainbridge argues that while that was a mistake (he feels it was a service), he makes the case for mass market software being considered a *sui generis* item.⁶⁴

4.2.1.3 Software as a Sui Generis Item

From time to time, when the courts or the legislature are faced with a new development to which existing legal concepts do not adequately fit, they will create a new concept, for example the protection of rights in databases did not fit well in existing copyright law - the existing rights were inappropriate. Thus the legislature created a new or *sui generis* right to protect databases - the right to control extraction.

⁶³ *Saphena Computing Ltd v. Allied Collection Agencies Ltd*, 1995 616 (F.S.R. 1995).

⁶⁴ Bainbridge, D. (2005). The Nature of Software Contracts. *IP & IT Law*, 10.6(3).

Equally, as matters stand, the existing law on the sale of goods and services does not fit well to the purposes of determining contractual liability for software failure - it may be therefore that the appropriate way forward would be a *sui generis* form of contractual liability for software. This would perhaps not be without precedent, as Lord Penrose said in *Beta Computers (Europe) v Adobe Systems (Europe) Ltd* "... In my opinion the only acceptable view is that the supply of proprietary software for a price is a contract sui generis".⁶⁵ This leaves open two questions relating to the project, what such a *sui generis* right should consist of for software now, and whether the advent of TC might mean a stronger level of protection should be given to users in the light of the promises made by vendors about the security qualities of TC systems.

4.2.1.4 Implications for TC if the hardware and software components carry different liabilities

As we have seen, TC comprises both hardware and software components. This also corresponds to the organizational structure of the TCG which is partly composed by both kinds of industries. We can here go back briefly to the different scenarios we described above. If we are dealing with a TC system malfunctioning, that is a system that is not even delivering what according to the state of the art would have been expected and possible, then it may just be possible to identify exactly which component is to blame. For type 2 failures, failure of the system due to better attack capabilities, this might be impossible in principle. In theory,

⁶⁵ *Beta Computers (Europe) Ltd v. Adobe Systems (Europe) Ltd*, 1996 367, 1996 S.L.T. 1604 (1996), Bradgate, R. (1999). Beyond the Millennium - The Legal Issues: Sale of Goods Issues and the Millennium Bug. *The Journal of Information, Law and Technology* (JILT), 2, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_1992/bradgate/.

legal options available are to treat it as a matter of joint liability for a “security service”, hardware or software liability only.

At this point, we step back a bit from a purely formal legal analysis, and ask how the TC industry itself perceives the issue, what their conceptual understanding is. In order to assess the viability of a large scale project to examine the liability hypothesis, a small-scale set of semi-structured interviews was conducted – the sample contained Hewlett Packard research staff members and Computer Science academic staff at the University of Bristol. The interviews uncovered a number of interesting issues, but also led to the conclusion that the issue was going to be more complex to research than was originally expected.

“It’s common understanding” that it is more likely to be a software problem rather than hardware says Plaquin at HP Labs, although he does not provide much justification for this position, clearly basing his argument on his own experience. It is a truism that software is never ‘bug free’, and therefore it is expected that it may not always work exactly as intended. Prof. Smart notes that it is possible to use processes that can make the software as bug-free as possible but that is mainly used in safety critical systems, as it is extremely costly.

Prof. Smart went on to say that:

“... if you are ... producing hardware you are prepared to tolerate errors ... one, you can detect errors quickly, two, if there are errors you just replace the component. The problem with software is that actually detecting errors is much harder, it’s deployed and then in the field you have to re-change the software without actually having the physical mechanism go back to the manufacturers ... there has to be some sort of remote update facility, so it’s actually much harder ... the hardware is actually a relatively easy thing to get right...”.

It seems therefore that imposing liability on hardware manufacturers might be a more realistic solution, as hardware industries are in better place to deal with failures. Dr. Page, on the other hand, suggested that the joint liability question was difficult to answer, noting that actually proving whether it was a

software or hardware problem which caused the failure of a trusted system would be very difficult:

“... it’s difficult to actually replicate these things, so proving that they even happened in the first place is slightly contentious.”

Adding to that, he views the issue in some respects as a matter of trade-off between reliability and performance suggesting that

“... the best thing to say ... about the reliability of software is ... it’s not a solved problem, but the reason you’ve got unreliable software, at least partly, is because people have ... made a trade-off between reliability and performance, or reliability and other things ... if you are willing to pay the price for reliability you can get a lot more reliable systems that you’ve got now.”

Yet, Pearson at HP Labs sees things as perhaps more complex than that.

“Because of the way the whole mechanism works ... there are multiple parties involved. ... you’ve got, for example, the specification itself which is produced by the TCG and describes ... what you have to do to produce a trusted platform ... it’s possible someone might discover there was a problem with that, but I doubt it ... then if someone actually makes a trusted platform they need to produce a design and someone else needs to certify that the design is conformant with the specification. There are different bodies performing different roles, and then ... there are the people that actually produce the different components that go into the platform and they’ll actually certify what the values of the hash functions and the metrics are going to be ... then there’s going to be the components that actually do the checks, the agents that do the checks in the system, and then there’s the software that has to reside on a person’s platform that’s checking that it’s engaged with the protocols and actually getting the information and doing the analysis on that and deciding, is it going to recommend to go ahead or not to go ahead. So there’s all sorts of people who are involved, it’s not just the manufacturers of the platform, the people who make the chips, ... there are probably 10 different groups involved in putting things together, some of whom are certifying that things conform to a design and things like that...”

In essence, it appears that she is saying that it may never be clear enough which party involved in the provision of a TC based system will be liable in case

of failure. Interesting though the answer by Pearson, alerts us to the fact that the TCG as a group is performing a different function from its constituent parts. The TCG, as an entity, merely certifies the type of system their members are actually developing and building. This brings in a potential new dimension: If the system fails, in any of the three ways described above, is there in addition to the contractual relation with the software vendor also a (quasi-contractual) relation with the TCG as certifying body? We will return to this issue below.

Another issue raised was the issue of shifting liability. In case of failure of TC technology, will the vendor companies take responsibility, or will they blame users, either individuals or enterprises, for the failure? As regards this concern Plaquin at HP Labs answered by saying that at the end of the day it is human nature to shift liability, but not the role of the technology. The technology can help to establish relevant evidence, independently from the parties. Here, our discussion about “chain of custody” from the previous chapter comes back into play. To ensure that the evidence isn’t tampered with, the TC system needs to be able to reason about its own status, and prove that it was not interfered with. For the civil liability issue, this feature becomes obviously relevant to identify where, if anywhere, a Type 1 malfunction happened. When the same question was put to Prof. Smart, he responded by suggesting that the liability in circumstances where there is a failure in TC systems, should, in the enterprise arena at least, be covered by contract terms with the liability clearly on the manufacturer i.e. the corporation or person selling the kit, and not to the customer who simply buys the technology. “A lack of software liability is effectively a vast government subsidy of the computer industry. It allows them to produce more products faster, with less concern about safety, security, and quality”.⁶⁶ In our case of TC, we argue that the user relies on the TC vendors that the system they are offering

⁶⁶ Schneier, B. (2008). Software makers should take responsibility, *The Guardian*. Retrieved from <http://www.guardian.co.uk/technology/2008/jul/17/internet.security>

(and the user is buying) is actually operating as it was supposed to. In our opinion this leads to the definition of reliance liability that we believe that is the most appropriate way to ensure the trust of the users in TC.

4.2.1.5 Current level of liability exposure for producers, in the event of hardware and software failure appropriate for TC?

One of the lessons we learn from even these short interviews, is that the industry thinks that any exposure to liability can be managed contractually. There might be disagreement where the risk is best located - with the university based developers accepting that a shift to consumers may have detrimental effect, while the commercial developers are more willing to exclude liability “as long as we do everything possible”.

The legal contract concerning software which binds the user with the software vendor is called End-User Licence Agreement (EULA). This agreement contains the terms and conditions that the user must obey, in order to use the software legitimately. The agreement may also contain various terms and conditions such as to install the software in only one computer, or to use it for personal purposes only.

There are many ways this contract can be presented to the user, in order for him to accept and then install and use the software. The EULAs can restrict the usage of the software; they may “force” agreement on certain conditions while using the system; and lastly they seriously limit the ability of the user to sue the vendor for damages or vulnerabilities presented to the software.⁶⁷ The latter, is perhaps the most crucial reason why software developers tend to use EULAs as an “insurance” against the users. These kinds of agreements take away the user’s

⁶⁷ Desautels, E. (2005). *Software license agreements: Ignore at your own risk*. End-User License Agreements: Security and Privacy Implications.

right to customize or even repair their own devices.⁶⁸ Moreover, the software vendors can trust that the software has not been reverse engineered or disabled, in any possible way, so that any activities that waive any term or condition contained in the EULA are prevented.

From the manufacturer's perspective, the disclaimer of liability for software faults is probably the most important function contained in an EULA. With the user's agreement, he can no longer sue, or file class-action lawsuits against the vendor for faulty products, or for products that do not fulfill the user's requirements. Due to the limited uptake of TC so far, it proved difficult to find good examples of TC specific EULAs. But one of the main features of the TCG technology, as discussed, is the remote attestation. Principles underlying this feature enforce certain aspects of EULAs as it brings third parties into the user - computer vendor relation. We note here that EULAs therefore potentially "go beyond" the relation between the two contracting parties, and obligate the user to a certain behavior towards a party that is not party to the contract.

As we noted above, it has been suggested in the past that it would be useful to apply pressure to software vendors to improve software security and to ensure that the software provides the security it should provide, and that in any other case, the purchasers should be able to sue the software vendors for any kind of harm caused by the use of their products.⁶⁹ Experts in the fields of IT remain divided in two camps on whether software product-liability rules could cause more problems rather than they are supposed to solve. Schneier one of the most influential IT experts called by the House of Lords Science and Technology

⁶⁸ Newitz, A. (2005). *Dangerous Terms - A User's Guide to EULAs*. *Electronic Frontier Foundation (EFF) - Defending Freedom in the Digital World*. from <http://www.eff.org/wp/eula.php>

⁶⁹ Chandler, A. J. (2003). *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*. *University of Ottawa Law and Technology Journal*, 1(1-2), pp. 231-261.

Committee to give testimony on the report they issued on "Personal Internet Security", states that "there's no other industry where shoddy products are sold to a public that expects regular problems, and where consumers are the ones who have to learn how to fix them".⁷⁰ He also thinks that the key to solve this problem is by applying software liabilities as computers are the only mass-market consumer item in which the vendors are not liable for any faults.⁷¹

Advocates for more burdensome liability rules have made unfavourable comparisons to the rules that apply to toasters, automobiles, tablesaws, airplanes, and other products.⁷² In each of these cases, the vendors would be held liable if they sell a defective product, and product liability laws compel them to issue recalls, or provide warranty repairs or compensation to possibly injured buyers or damages caused.

Expressing a commonly thought question McKenzie asks: "Can you imagine a world where the words "software" and "warranty" actually appear on the same page?".⁷³ Rolling on to the next logical question: "What will be the responsibility of the software vendors that sell flawed software?".

⁷⁰ Schneier, B. (2008). Software makers should take responsibility, *The Guardian*. Retrieved from <http://www.guardian.co.uk/technology/2008/jul/17/internet.security>

⁷¹ Schneier, B. (2007). Schneier on Security. Retrieved from http://www.schneier.com/blog/archives/2007/01/information_sec_1.html

⁷² For TC comparison with toasters see McKenzie, M. (2009). Software Liability Laws: Thinking The Unthinkable. Retrieved from <http://www.informationweek.com/news/smb/ebusiness/229206517>, automobiles see Schneier, B. (2008). Software makers should take responsibility, *The Guardian*. Retrieved from <http://www.guardian.co.uk/technology/2008/jul/17/internet.security>, and tablesaws see Ganssle, J. (2011). Software liability laws – Part 2. Retrieved from <http://www.eetimes.com/electronics-blogs/other/4233623/Software-liability-laws---Part-2>,

⁷³ McKenzie, M. (2009). Software Liability Laws: Thinking The Unthinkable. Retrieved from <http://www.informationweek.com/news/smb/ebusiness/229206517>

4.2.2 An alternative view: Security as service and the relational contract theory.

Let us recap briefly: In the past, liability regimes for software were far from burdensome on software developers and vendors. This has been at least in part blamed for the security flaws that they generate.⁷⁴ Under normal conditions, market competition should mitigate this, but even in traditional fields of software, monopolies or near monopolies have been the norm rather than the exception, on contribution to the high level of software vulnerabilities.⁷⁵ As we argued, TC is premised, to an extent, on the absence of diversity and competition, making this an even more pressing issue. At the same time, shifting the burden entirely to the industry might not only deter necessary investment in security, it can encourage reckless behavior by users. TC is already a potential contributor to this “moral hazard”, where people relying on the technology could be induced to take excessive risks, as we discussed in chapter 2. Additionally granting users with wide ranging legal protection could increase this danger even more.⁷⁶ Industry seems willing to treat TC just like any other product, and use EULAs to manage their exposure to liability, by regimenting use and hiding the limitations of the approach in the small print. This brings us back to the first chapter where we discussed the disappointingly limited uptake of TC by consumers. We argued there that TC is a compromise between costs and safety - ideally not too costly, but as a result not as safe as it could possibly be. From a liability perspective

⁷⁴ See also Edwards, B., Locasto, M., & Epstein, J. (2014). *Panel Summary: The Future of Software Regulation*. Paper presented at the Proceedings of the 2014 workshop on New Security Paradigms Workshop (pp. 117-126), ACM, Kamp, P.-H. (2011). The software industry is the problem. *Queue*, 9(9), pp. 10.

⁷⁵ See in particular Kim, B. C., Chen, P. Y., & Mukhopadhyay, T. (2011). The effect of liability and patch release on software security: The monopoly case. *Production and Operations Management*, 20(4), pp. 603-617.

⁷⁶ August, T., August, R., & Shin, H. (2014). Designing user incentives for cybersecurity. *Communications of the ACM*, 57(11), pp. 43-46.

though, this compromise could become an issue in the context of litigation – after all, there were foreseeable risks, and known countermeasures, which were however not taken due to costs – and all that documented in the technical literature. Unsurprisingly, manufacturers will want to emphasize and legitimize this in the EULAs, making the buyer a willing accomplice in the corner cutting. At the same time, TC adds costs, and the best way to ensure take up is to emphasize the security benefits, or at least tacitly rely on the different understanding laypersons have of terms such as “trusted” and “secure”. Due to the monopoly position of the TCI, a possible option therefore seems to be on balance to increase liability (possibly by using “good faith” reading of the EULAs aggressively), while allowing some risk management on the side of the TC providers, and if for no other reason than to remind users to remain vigilant.

However, we think that any mere tinkering with software liability rules, or EULAs, falls short of what is needed here, for both industry and users. Any such attempt would at best address Type 1 failure, failure of the technology to function as specified. In the constant arms race between hackers and security solutions, Type 2 failures are just as important, and they fall outside even the most aggressive use of “good faith” review of liability rules. Here harm is caused by an ingenious third party that finds way to circumvent security mechanisms that at the time they were developed were state of the art. The fault of the supplier, if any, was that it raised unrealistic expectations and caused the buyer to engage in risky behavior, preventing out of distrust of users in general that the client used other protective measures not TC certified (because in a TC environment, at least potentially, some effective but open source and uncertified tools will not work), and potentially rather than helping with damage limitation making things worse by disabling the affected party from taking remedial steps of their own.

One part of our solution is relatively simple. “Buying TC” should in law be classified as what the consumer will perceive it to be – that is certified security service as a package. This sidesteps the debate on whether software is a good, a

service or sui generis, and how hybrid hardware/software systems are to be considered. It should support “social trust” on the side of the customer, as expectations and what is promised match closer, the ability to shift liability is at least reduced, and the consumer need not to worry which part of the system failed to deliver. To conceptualize TC as a certified security service contract however also has another advantage. Service contracts are closer to the paradigmatic example of a different way to think about contracts altogether, the relational contract theory. While mainly motivated historically by employment relations, we can think of “security services” not as a one off service, but a long lasting relation. This, we will argue, allows an understanding of the contract relation that is much better suited to create “networks of trust”, with a long term convergence of interests between the parties, that would match the technology based “trust networks” that TC tries to build.

To understand this argument, we need first to look a bit at one of the conceptual shortcomings of classical contract theory for this purpose. In one of the most influential papers in legal theory, Wesley Hohfeld’s *Fundamental legal conceptions as applied in judicial reasoning*, the author explicates the meaning of core legal concepts such as right, duty and privilege, by constructing an interlocking system that maps the relations between the “atoms” so to speak of a legal system.⁷⁷ “Duty” and “Right” are two of these atoms or basic concepts, they stand in a relation of judicial correlative to another: that is to say if I have a right against you, you have a corresponding or correlative duty towards me. “Duty” and “privilege” by contrast are legal opposites: If I have a duty towards you to do X, then I don’t have a privilege not to do X.⁷⁸ Crucially for our purpose, his analysis

⁷⁷ Hohfeld, W. N. (1917). *Fundamental legal conceptions as applied in judicial reasoning*. *Yale Law Journal*, pp. 710-770.

⁷⁸ *ibid.* p.719ff. This is one of the most frequently cited papers in legal theory. We will only focus on some core ideas, for a fuller academic discussion, the reader is referred to the early appraisal here Cook, W. W. (1919). *Hohfeld’s Contributions to the Science*

is premised on two assumptions: The first can be called a commitment to bi-polar atomism. That is, the legal status of a person, or indeed any complex legal problem, can ultimately be broken down in simple relations between two people and two people only, each in turn characterized by the basic legal concepts that he proposes. For many of his contemporaries (and indeed subsequent critics), this seemed problematic. How can we understand “ownership” or right in rem as it is traditionally called? If I have an “absolute” right of ownership, say in my computer, then this is a right against everybody, not just an individual person. For Hohfeld, this is a misconception. Where lawyers often saw a relation that involved infinitely many parties, he argued that this can always be reduced in principle to a multitude of bi-polar relations between just two people, and nothing else but the substance of this relation determines their rights and duties. Connected to this view is a “litigation centric” approach to law. In Hohfeld’s view, we only understand the meaning of a legal concept when it is litigated in court. And in a court room setting, we obviously always have just two parties – plaintiff and defendant, fighting it out. So the meaning of “ownership” in my computer is not best understood as a complex relation involving everybody, but a relation that crystallizes only when you take my computer away, and I sue you in court.

We can already see here the problem that this conception of law can create for TC. In the second chapter, we argued that in modern societies, interpersonal, emotive trust between acquaintances had to be replaced by impersonal trust in institutions. Weber, so we argued, had given the law an important role in creating

of Law. Ibid., pp. 721-738. and to the more recent comprehensive study here Halpin, A. (2007). Rights, Duties, Liabilities, and Hohfeld. *Legal Theory*, 13(01), pp. 23-39. Hohfeld’s analysis has recently received renewed interest in the context of law and computers, especially automated legal reasoning and agent technology. Its simplicity lends itself to automated, computational characterisations. See e.g. Krogh, C., & Herrestad, H. (1999). Hohfeld in cyberspace and other applications of normative reasoning in agent technology. *Artificial intelligence and law*, 7(1), pp. 81-96. doi: 10.1023/A:1008367514393

this trust. I can trust you to fulfill your obligation, because you are under a legal obligation to do so. But for Weber, this was arguably not meant simply as “compliance by threats”. In his conception of the modern economy, I can trust you, and to a degree expose myself to risks, because I know the law, and you know the law, and I know that you know the law – a situation which is known under the technical term of “common knowledge” in game theory and the theory of distributed computer agents.⁷⁹ In such a situation, my thoughts are not primarily that something will go wrong, but that I will be protected. Rather, it is an assumption that everything will be as promised, for we all agree that following the law is the right thing to do, and only if there should be a problem, exceptionally, there is redress. This leads to a concept of more substantive trust, as opposed to a society where we think when engaging with others: I do not really trust you, you probably will default, but the law will save me. It is however that latter attitude that the litigation centric view of law promotes, and which finds its expression in reality in the abusive or unfair use of general terms and EULA’s discussed above. Their content becomes intelligible if we assume that the issuer thinks from the beginning the worst of his customers, and from the outset pursues a defensive strategy.

Just as problematic as the litigation centric view is the emphasis of bi-polar relations only. In Hohfeld’s analysis, the law is only concerned with a situation where things went wrong, and you have an issue with your TC provider. Nobody else is involved. But as we discussed in our analysis of what TC is trying to achieve, this breaks up the very essence of a TC mediated relation. I trust the TC provider to verify the trustworthiness of everybody that I encounter, and in return trust my TC provider enough to provide them with enough information about me so that they in turn can assure third parties of my trustworthiness. The

⁷⁹ See e.g. Halpern, J. Y., & Moses, Y. (1990). Knowledge and common knowledge in a distributed environment. *Journal of the ACM (JACM)*, 37(3), pp. 549-587.

result is an intricate network where everybody is related to everybody else – and where, as Guadamuz noted, power laws and network effects can be efficient. By breaking up this network analytically, and disassemble it into bi-polar relations between just two parties, the law fails to map the reality of what it tries to regulate.

Building on Hohfeld’s work which was a general characterization of all of the law, formalist theories of contract characterize the contract relation in particular as an atomistic, bi-polar relation that is not receptive to third party interests or wider societal concerns at all. The most influential, and most concise, account for formalist contract doctrine can be found in Ernest Weinrib’s “The Idea of Private law”.⁸⁰ Contract law in this view can be fully understood as a bipolar relation whose content is entirely dependent on the parties’ stated intention at contract formation, and whose sole aim is to ensure “corrective justice”, that is if one party’s rights are interfered with, it is entitled to have the balance restored. Wider social or political concerns are irrelevant for this view – this is what Weinrib calls “the autonomy of private law”, and as a formalist theory, issues such as unequal access to information or unequal bargaining power of the parties are also of no concern.⁸¹ Here we face the problem of trust creation through law even closer at home – contracts, the main mode of regulating the relation between TC provider and customer, are particularly prone to an interpretation that focuses on the “magic moment in time” when offer and acceptance are matched, and is irresponsive to any third party interests – the concept of privity of contract that we alluded to before. This again breaks up the trust network that TC tries to build

⁸⁰ Weinrib, E. J. (1995). *The idea of private law*. Cambridge, Mass.: Cambridge, Mass. : Harvard University Press. For a critical discussion see e.g. Marshall, J. (2009). On the Idea of Understanding Weinrib: Weinrib and Keating on Bipolarity, Duty, and the Nature of Negligence. *S. Cal. Interdisc. LJ*, 19, pp. 385.

⁸¹ So in particular in Weinrib, E. J. (1993). Jurisprudence of Legal Formalism, *The. Harv. JL & Pub. Pol’y*, 16, pp. 583.

into small bipolar atoms, and is thus incapable of matching the reality that TC creates.

While formalism in the Weinribian tradition is a highly influential way to think about contracts, some of the similarly influential competitors are even worse. Economic analysis of contract law in particular shares with the above theories its atomism – contracts remain essentially an issue between two parties only – but limits the relevant interests to “rational maximization of economic interests”.⁸² One way in which this conception of contract law is expressed in practice is the attitude to “efficient breach” of a contract relation: According to this theory, if I find myself in a contractual relation, but my economic interests would be better served by defaulting and accepting “some” penalty, then the rational thing is to walk away from my promise. Contract law, in this view, should permit this if the damages in turn are market optimal. In a typical example, if I promise to sell my car to you for £300, and I get immediately afterwards an offer for £3000, then a rational contract law should allow me to walk away from the contract with you, provided I give you your money back plus an adequate remuneration for the additional expenses you incurred while waiting in vain for your car to be delivered (say £20 for taxi costs, and £5 to make up for inflation which means cars are now more expensive). This leaves me better off, and you not worse off, in financial terms, as if we had never met.⁸³ We can immediately see why this is not an ideal foundation for a contract in security services. Imagine you hire a security service in the offline world: you have to trust them with access to

⁸² For a comprehensive discussion see Goldberg, V. P. (1976). Toward an expanded economic theory of contract. *Journal of Economic Issues*, pp. 45-61. For a balanced but friendly appraisal, see Posner, E. A. (2003). Economic analysis of contract law after three decades: Success or failure? *Yale Law Journal*, pp. 829-880.

⁸³ See for a full discussion Craswell, R. (1987). Contract remedies, renegotiation, and the theory of efficient breach. *S. Cal. L. Rev.*, 61, pp. 629. For a rational calculation of damages under these conditions see Birmingham, R. L. (1969). Breach of contract, damage measures, and economic efficiency. *Rutgers L. Rev.*, 24, pp. 273.

your house, they will know where your valuable property is, where your protection is the weakest, and if they offer personal protection as well, where your children go to school. This requires considerable trust. A contract that essentially says that as soon as a local criminal offers more for the service, they can terminate the contracts on return of last month' wages seems incapable of creating this type of trust. In the real world, some or all of the trust will have to come from something else instead – and we discussed some of the mechanisms in the second chapter: public law regulation of the security industry, or self-regulation of the industry, with a code of practice and an institutionalized complaints procedure e.g.. But as we discussed there, this type of framework does not exist (yet) for online security: the bouncer who keeps suspicious people out of the nightclub is much more heavily regulated than the “firewall bouncer” that keeps suspicious packets out of your computer.

As we discussed above, this is not just a theoretical problem. The way in which the industry uses EULAs, and the way in which in our interview “insiders” conceptualized the role of contract law, fits this “calculating” approach to use contract terms strategically: The customer buys a good in a one off transaction (buying say a computer that says “TC in it”) and this marks effectively both the beginning and the end of the relation, which is not deeper than say buying a toaster. The problem with modern contract theory as a creator of trust has however been recognized as a more general problem of modern economies, and is sometimes discussed under the concept of “calculativeness of trust” in societies governed by classical contract law. It finds a clear expression in this summary by Diego Gambetta.

“There is a degree of convergence in the definition of trust which can be summarized as follows: trust is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action [...] When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least

not detrimental to us is high enough for us to consider engaging in some form of cooperation with him”.⁸⁴

We can immediately see the close similarity to the “inductive” concept of techno-trust discussed in chapter 2 that underpins TC: trust is an extrapolation from past behavior about the probability of future positive behavior. Economic theory of contract law recognized that problem, it tried to develop more sophisticated models of rationality to minimize its predicted impact. Machiavelli may have advised the Prince that he could and indeed should breach contracts with impunity, just as classical economic theory of contract law predicts. More recent and more sophisticated approaches to economic contract theory such as transaction cost economics advises us that “investment in trust” can pay off in the long term, and that therefore the wise Prince will give more credible commitments.⁸⁵ However, while there are therefore variations of economic theory of contract available that offer a “fix” to the most obvious trust-destroying aspects of economic contract theory, there are strong doubts that “calculative trust” is ultimately a possibility.

Writing with general support for an economic analysis of law and from the perspective of an economist, Oliver Williamson concludes in an article that had substantial impact on the debate on the relation between contracts, economic analysis and trust, that:

“If functional separability does not imply attitudinal separability, then piecemeal calculativeness can easily be dysfunctional. The risk is that pushing metering at the margin every where to the limit will have spillover effects from easy-to-meter onto hard-to-meter activities. If cooperative attitudes are impaired, then transactions that can be metered only with difficulty, but for which consummate cooperation is important, will be discharged in a more perfunctory manner. The

⁸⁴ Gambetta, D. (2000). Can we trust trust. *Trust: Making and breaking cooperative relations, 2000*, pp. 213-237. at IX.

⁸⁵ Machiavelli, N. (1952). *The prince* (L. Ricci, Trans.). New York: New York American Library.(Original work published 1513), pp. 92-93.

neglect of such interaction effects is encouraged by piecemeal calculativeness, which is to say by an insensitivity to atmosphere.”⁸⁶

In our analysis above, we identified all the elements for the TC setting that trigger the problems Williamson describes: TC, or computer security in general, does indeed require “consummate cooperation” – technological fixes alone can lead to moral hazards, only if consumer and TC provider cooperate will true benefits be realized. TC can be metered only with difficulty – that was expressed by our interviewees when they pointed out the difficulties of modeling and predicting flaws and the potential for malfunctioning in a hostile environment in advance. This makes it difficult to “meter” what either party needs to do, resulting in a “grab for control” by the economically stronger party – the use of Terms and Conditions and EULAs to shift risk to the consumer and prescribe in detail what they must not do or risk voiding the contract. This converges with other studies that have shown the tension between security provisions and an economic understanding of contractual relations.⁸⁷

Williamson reaches a skeptical conclusion:

“Trust, I submit, should be concentrated on those personal relations in which it really matters, which will be facilitated by the use of “political, social, and economic institutions” to govern calculative relations. If calculativeness is inimical to personal trust, in that a deep and abiding trust relation cannot be created in the face of calculativeness, and if pre-existing personal trust is devalued by calculativeness, then the question is how to segregate and preserve relations of personal trust”.⁸⁸

⁸⁶ Williamson, O. E. (1993). Calculativeness, trust, and economic organization. *Journal of Law and Economics*, pp. 453-486. at 480; for a critical discussion see Craswell, R. (1993). On the Uses of “Trust”: Comment on Williamson, “Calculativeness, Trust, and Economic Organization”. *Journal of Law and Economics*, pp. 487-500.

⁸⁷ See e.g. Langheinrich, M. (2003). *When trust does not compute-the role of trust in ubiquitous computing*. Paper presented at the Workshop on Privacy at UBICOMP (pp. 1-8),

⁸⁸ Williamson op cit p. 483

If we followed this conclusion, we should abandon the talk about trust in TC altogether, and also abandon the idea that the contractual relation between TC provider and customer can sustain the necessary trust between the parties. But as we saw, all the alternatives – personal trust, kinship loyalty or institutional trust are also not available to us in a global, disembodied medium like the Internet. This could explain the low uptake of TC: customer and TC provider need a substantial degree of trust to be willing to accept the risks that come for both, with that relationship, it requires a degree of cooperation, yet not only is there little social capital to sustain that trust, the chosen method of interaction, contract law, is based on calculativeness and thus destroying rather than fostering trust.

We will argue however that this needs not be the end of the story. Ultimately, Williamson, and with him the many economic, political science and contract law theorists that shared his concern, are still within the conceptual framework of the classical, formalist notion of law and legal relation as a one of, bipolar relation that we described above in description of Hohfeld and Weinrib. While modern society relies essentially on contracts and contracting (again as per Weber), they need to be understood differently to fulfill this task. This was particularly obvious on long term economic relations such as employment law, where the idea of a “one off” meeting of the minds is the least plausible model, and parties tie themselves to each other for a long and unpredictable future.⁸⁹ This gave rise to a very different understanding of contracts, the “relational theory of contracts”, developed in particular by Ian Roderick Macneil and Stewart Macaulay.⁹⁰

⁸⁹ Seminal: Macneil, I. R. (1977). Contracts: adjustment of long-term economic relations under classical, neoclassical, and relational contract law. *Nw. UL Rev.*, 72, pp. 854.

⁹⁰ See for an exposition of the theory in full e.g. Macaulay, S. (1985). Empirical View of Contract, *An. Wis. L. Rev.*, pp. 465. , Macneil, I. R. *Ibid.* Relational contract: What we do and do not know. pp. 483. ; See also Gudel, P. J. (1998). Relational Contract Theory and the Concept of Exchange [comments] (pp. 763).

This understanding of contract law also leads away from the “litigation focused” understanding of law that we encountered above in our discussion of Hohfeld, to a view of regulation through contract that is less adversarial and more geared towards “community creation”.⁹¹ In essence, he argues that contracts are never just discrete commodity exchanges, but are situated in complex webs of exchange relations.⁹² This is in marked contrast to both Weinribian legal formalism and economic analysis of the law, which both ignore in varying degree contextual matters surrounding the contract and concentrate only on the expressed terms together with a strictly limited and *a priori* known range of implied terms. They fleetingly connect “total strangers brought together by chance rather than any common social structure”.⁹³ Or, as we put it above, parties in discrete exchanges are atomised individuals. For this to work, they “would have to be completely sure of never again seeing or having anything else to do with the other”.⁹⁴ They are also transient, as a necessary condition of their discreteness: “everything must happen quickly lest the parties should develop some kind of a relation impacting on the transaction so as to deprive it of discreteness”.⁹⁵

The paradigmatic exchange for them is the contract of sale of a perishable good, such as shopping in a supermarket. By contrast, Macneil takes employment contracts as paradigmatic and argues that all contract relations are on a spectrum from the highly relational contract to those that look “as if they are discrete”, and

⁹¹ Skeptical on this diminishing role of litigation to explicate legal concepts is Komesar, N. K. (1985). *Lawyering versus Continuing Relations in the Administrative Setting*. *Wis. L. Rev.*, pp. 751. , which nonetheless gives a good disucssion of the meaning of this shift in focus.

⁹² MacNeil, I., & Campbell, I. D. (2001). *The relational theory of contract : selected works of Ian MacNeil*. London: Sweet & Maxwell. pp. 365–386 at p. 379

⁹³ MacNeil, (1978) p. 856

⁹⁴ *ibid* p. 856

⁹⁵ *ibid* p. 856

transactionalised relations such as one-off commodity purchase. On closer inspection though, all relations are connected with and situated within a social context. The only successful relations are those that are harmonized with this context and do not interrupt them. This by Macneil can be achieved through a number of "norms in a positivist sense". Amongst these, he lists:⁹⁶

1. role integrity;
2. reciprocity (or 'mutuality');
3. implementation of planning;
4. effectuation of consent;
5. flexibility;
6. contractual solidarity;
7. the 'linking norms' such as restitution, reliance and expectation interests;
8. the power norms that create and restraint power;
9. propriety of means;
10. harmonisation with the social matrix.

By "norms in a positivist sense", what he means is that these are the conditions that we see observed when humans interact successfully through contracts, as opposed to the predictions that the "homo economicus", the rational self-maximiser, of positive economics predicts them to be. So even when we just buy a computer, the social context is important. At first, this looks like a simple one – off transaction that does not affect the two parties beyond handing over goods for money. But once we look closer and keep an eye on the context, a much more complex system emerges. McNeil in his examples mentions e.g. brand loyalty that this sale can generate well beyond the individual transaction.⁹⁷ We

⁹⁶ Macneil, I. R. (2000). Contracting worlds and essential contract theory. *Social & Legal Studies*, 9(3), pp. 431-438. p. 432

⁹⁷ Macneil, I. R. (1973). Many Futures of Contracts, *The. S. Cal. L. Rev.*, 47, pp. 691-816. p. 701; See on this issue also Ivens, B. S., & Blois, K. J. (2004). Relational exchange

can add in the modern IT driven economy many more. The customer data that now allows the seller to improve services or advertising – her data will reside forever in some form in the data sets of the vendor, and thus you could poetically say, a small part of her will influence the strategy of the vendor’s business for a long time. Then there is the issue of “commensurability”. The choice of software system will make this computer compatible with some, and less compatible with other computers – the core of a network of users who find it easier to exchange files amongst themselves. Indeed, they may soon find that they need voluntary Internet discussion boards where owners of this system exchange tips, help and advice. Furthermore, there can be contractual software updates or service contracts involved.

So even in situations that look like simple one-off commodity transactions, in reality lasting networks are created and facilitated. This works best, so Macneil, as a contingent, empirical matter if the above norms are observed in addition to what contract law demands as a minimum. Interesting here, and used as an example, is mutuality. In the Weinribian concept of contract, I want a computer, and the seller wants my money. I grudgingly give him the money (I would rather keep it and the computer, and where the law allows, will do so), and he grudgingly gives me the computer (he would rather keep it and the money and where the law allows, will do so). This “thin” notion of reciprocity and balance is contrasted by Macneil’s concept of mutuality. Now, I not only want the computer, I also want the company to have the money and make wise use of it – as this enables better after-care, or better products in the future which strengthen the brand and thus the peer reputation I get from my purchase. The seller in turn wants me to have the computer and be happy with it – the compatibility issue can then entice my friends to also buy that model, or prepares me for buying updates, upgrades or

norms in marketing: A critical review of Macneil’s contribution. *Marketing theory*, 4(3), pp. 239-263.

follow up models. If in that scenario, power is too unequally distributed, these network benefits will not incur, and hence the power norms need to be carefully balanced – taken up the recurrent theme of this thesis that great power demands great responsibility. As TC contracts inherently and with necessity contain strong power norms (since the technology alone will prevent the user from many activities) they need to be balanced and adjusted in the contract, not made worse by aggressive use of EULAs.

This, again, is not an appeal at the better self of the parties. Rather, the extent, to which a particular exchange relation is in accordance with the norms will influence the success of the relation for both sides, resulting in greater longevity (where desired) and the ability for both parties to gain the full range of benefits that the exchange can potentially offer. We therefore submit that the contractual relation that regulates the sale of TC products should be particularly attuned to these norms, since longevity is intended (the process of remote attestation and assurance extend beyond the sale of the TC verified equipment), the power differentials are particularly strong, and the aim for both sides, a more secure Internet, can only be realised if networks of trust are build. Contract law in this view almost becomes a form of sociology, a way to understand the complex networks, alliances and interdependencies that make up society, rather than (merely) regulating and by doing so even disrupting, the way classical contract theory does.⁹⁸

In a recent study, Chen Wei Zhu has shown convincingly how relational contract theory is particularly suited for software licensing contracts, both on historical grounds as the form of contract most closely relate to the original

⁹⁸ On this understanding of relational contract theory as sociology see Macneil, I. R. (1987). Relational Contract Theory as Sociology: A Reply to Professors Lindenberg and de Vos. *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft*(2), pp. 272-290.

hacker spirit, but also in modern settings.⁹⁹ While his focus is on open source licensing, many of his insights can also be transferred to some types of proprietary software. Software, especially software like the one used in TC that enables computers to communicate safely, is in his words best understood as “relation-ware”.¹⁰⁰ This is particularly the case if, as in the open source community that he focuses on, developers and users are ultimately the same and everybody contributes in the long term. This is less obvious in proprietary software, but for security software like TC, the success of the system as we saw in the second chapter is also based on continued learning – the users, so we discussed, had to give up some information about themselves and their past to allow the system to predict their future trustworthiness. In this way, there is a continued bi-lateral exchange, a contribution by both parties beyond the moment of sale.

In an even more radical study, Bankowski and Schafer further pushed this idea by analyzing relational contracts as constitutive for international legal order – which is for obvious reasons of particular relevance for an analysis of Internet law and governance.¹⁰¹ They take their inspiration from ‘The Player of Games’ by the Scottish novelist Ian M. Banks. In it, the Culture, a profoundly peaceful and libertarian human/machine symbiotic society takes on the cruel and aggressive Empire of Azad. Azad is unique in its election procedure for its government and administration. It is centred on a game, also called Azad. Whoever wins this highly complex game becomes Emperor. The final takes place between the Culture representative and the Emperor. Both recreate on the board pictures of their

⁹⁹ Zhu, C. W. (2013). ‘Copyleft’ Reconsidered Why Software Licensing Jurisprudence Needs Insights from Relational Contract Theory. *Social & Legal Studies*, 22(3), pp. 289-308.

¹⁰⁰ Zhu op.cit at p. 305

¹⁰¹ Schäfer, B., & Bankowski, Z. (2000). Mistaken identities: The integrative force of private law. *The Harmonisation of European Private Law*, pp. 21-47.

respective societies. The Empire creates a “centralised hierarchical power structure in which influence is restricted to an economically privileged class retaining its influence through a judicious use of oppression and skilled manipulation of the society’s information system. In short, it is all about dominance”.¹⁰²

The player of the Culture on the other hand, constructs:

“a grid of forces and relationships, without any obvious hierarchy or entrenched leadership, and initially quite profoundly peaceful”.

The difference in attitude permeates the whole game.

Bankowski and Schafer suggest that one way to understand this novel as two different ways “to see” present society. The first they equate with “public law thinking”. Focused on an Austinian notion of the absolute sovereign, it looks for “well defined power structure” and “centralised hierarchies”. The use of force to guarantee adherence to this one set of rules. There are no networks, just a strict line of command. This comes in contrast with the view of a (relational) contract lawyer, the player for the Culture, who sees a “grid of forces and relationships without entrenched leadership”. They argue that while classical contract law is insufficient to explain the formation of societies, a relational understanding of contract leads to an understanding of society that is both contractual and network centric – thus a legal arrangement that now really matches Guadamuz’ characterization of the Internet as complex dynamic system.

To recap: The relation between TC provider and customer is shaped by contract. Part of the function of this contract, so we argued, is to create trust in a liberal society where people do not have prior social or familial bounds. We argued that classical contract law is however unable to fulfill this function. It is based on distrust, and thus disrupts rather than enhances the network of techno trust that TC tries to build. EULAs are seen as epitomizing this approach to legal

¹⁰² Chapter 1 pg.48 Banks, I. M. (1988). The Player of Games. pp. 1-320.

formation of relations, by further entrenching power differentials and enhancing the disempowerment of the user that is already inherent in TC (the user as problem, who needs to be prevented from interfering with what is good of his security) through further legal disempowerment – shifting liability away from the vendor and in addition imposing even more restrictions on the buyer what they can do without losing; what little protection remains. The inability to create the necessary trust, by violating the 10 principles, is ultimately harmful for all concerned. This is evidenced by the relative lack of success of TC and the minimal uptake – it requires more trust than the system can generate. By contrast, if we analyze the contractual relation through the lenses of relational contract theory, we see the potential of a TC contract to be the core for an emerging complex and sustainable network of the type it needs to create to guarantee Internet security. But is this just a different way to look at the same legal reality, a purely philosophical speculation which furthermore looks suspiciously idealistic, or do real legal consequences follow from it? This is an issue we will discuss in the next section.

4.2.3 Third party liability – no contractual relations – the reliance liability case

Above, we encountered 10 norms that Macneil identified as necessary so that contract relations can maximize the mutual interest of all parties, and create sustainable networks. From this it is a small step to argue that the degree to which actual doctrinal law “fits” these norms determines the usefulness of legal concepts methods and interventions in exchange relations. But can we make the transition from legal theory to legal practice, apart maybe from admonishing TC providers not to leverage their bargaining position too much in drafting liability exclusion clauses, or courts to use good faith aggressively in striking out such clauses? Is it a purely theoretical or jurisprudential issue, or one that can guide us in designing alternative legal rules? It has indeed been argued that legal

formalism, on closer inspection, is compatible with relational contract theory,¹⁰³ and that for this or similar reasons, changes to contract law doctrine are not necessary.¹⁰⁴ On the opposite end of the spectrum, it has been argued that a relational contract law is impossible in principle.¹⁰⁵ We will not engage with this discussion, which admittedly was for the author as a computer scientist... difficult to follow. Instead, we will demonstrate and argue for two specific and related proposals of how we should doctrinally understand TC that does take some inspiration from Macneil. We will focus for this on conditions 7 and 8 from the above list, (7) the 'linking norms' such as restitution, reliance and expectation interests; (8) the power norms that create and restraint power.

We mentioned the importance of power several times, and it was a recurrent theme in this thesis. To ensure internet safety, we permit a monopoly being formed in whose hand considerable power is concentrated. To a degree, they will determine who can communicate with whom. This, almost inevitably, can bring third parties into the equation. We mentioned this briefly above as our “scenario 3” of things that can go wrong. Malfunctioning TC can harm me, the owner, if my computer communicates with an untrustworthy source. Here a contractual nexus exists between me and the TC provider who caused the harm. But what if my TC system “overlooks” that my computer was compromised, signals this to the machine of a third party who, relying on this information, communicates with me and as a result also acquires a virus? OR what happens if my computer mistakenly does not recognize the remote attestation of the other computer’s safety, block it

¹⁰³ See in particular Scott, R. E. (1999). Case for Formalism in Relational Contract, *The Nw. UL Rev.*, 94, pp. 847.

¹⁰⁴ So Austen-Baker, R. A Relational Law of Contract?,(2004). *Journal of Contract Law*, 20, pp. 125.

¹⁰⁵ So Eisenberg, M. A. (1999). Why there is no law of relational contracts. *Nw. UL Rev.*, 94, pp. 805. For a response see Macaulay, S. (2003). The real and the paper deal: empirical pictures of relationships, complexity and the urge for transparent simple rules. *The Modern Law Review*, 66(1), pp. 44-79.

as a result and a loss for the owner of that computer ensues? Here, the party that suffered the harm is not in a contractual relation with my TC provider, nor with me. As we will discuss, I may be liable in the first scenario, a third party infected with my virus, in tort for the harm - not something the present legal system normally imposes on me, but a possibility. Alternatively, we could argue that the third party reasonably relied on the signals it received from my TC provider, who therefore should shoulder the loss.

Here relational contract theory comes to its strength, by recognizing the extra-legal, social norms that regulate this type of expectation. Through condition 7, it links the contractual issue to other legal concepts, including as we learned “linking norms” to reliance. Reliance or third party liability is indeed the legal doctrine that can extend the reach of a contract beyond the parties, and thus enable us to move beyond the bipolar, atomistic relation. Here a rough outline of the basic idea: I, when contracting with my TC provider, am not just an isolated, self-interest maximising actor of neo-liberal economics. I’m a social being with pre-existing networks and connections, and I care for others, at least those within my network. My TC provider’s role is to guarantee safety not just by checking if those who contact me can be trusted, but he also vouches for me. In such a situation, what I will need, to trust my TC provider, is not just that he covers through damages harm that happens to me. I also want him to cover harm that his actions cause my friends, or everyone who relied on him mistakenly certifying my trustworthiness, even if they don’t have a contract with him. On the other hand, if I trust someone else’s TC provider, I want ideally to know that if things go wrong, not just the owner of the computer that I contacted is obligated to compensate or help me – as he may lack the resources of the former and the knowledge for the latter. What I would like to know is that if something goes wrong because I relied on someone else’ TC attestation, is that in case of a problem, they (TC provider) will feel obligated to me to help sorting out the problem.

The legal concept that encapsulates this type of liability outside the contractual nexus is known variously as “quasi-contractual”, “third party” or reliance liability. We will use this latter term, as it encapsulates what our issue is about: compensation for the damage of third parties who trusted mistakenly my TC provider’s attestation.

To do this, we will first discuss the above scenario in a bit more detail, and also discuss briefly possible alternatives. We will then split up the problem into two configurations which reflect the TC process. In the TC set-up, we can distinguish two different forms of “signaling”. When I buy a TC computer, its components are certified as we discussed as TC by the TCG as a legal entity, who is responsible for developing appropriate standards and tests. So the first type of reliance is on this TCI “seal of approval”. Secondly, when actually working, my computer self-certifies its correct working, which is then, as we discussed, remotely attested by my specific TC provider (who will be a member in some form or other of the Trusted Computing Group). Here too, the third party will rely on this attestation. For the first scenario, there is a relatively straightforward analogy that can be made: The TCG acts like a Trust Mark certifier. We will use the discussion on the legal liability of Trust Marks to argue that a) a case has successfully been made already to impose reliance liability on them and b) that TC is an even clearer candidate for reliance, so that *a fortiori* this argument can be expanded to TC. For the second scenario, our argument is more complicated and will look initially more as if the discussion went on a strange tangent.

To argue that my TC provider should be liable under reliance liability for third parties that trusted its remote attestation of my computer, we will compare remote attestation with “writing a reference letter” and “certifying as an expert the airworthiness of an aircraft”. We will argue that the way TC works combines aspects of both types of social activity. This will then allow us to argue that since some legal systems successfully use reliance liability in these cases to protect

third parties who hired on the basis of a flawed reference, or who boarded an airplane on the basis of a flawed certification, so should TC.

To recap briefly the type of setting that concerns us here: My computer was compromised and now can infect other computers that communicate with it. Due to a failure in my TC system, this is not spotted, my computer remains “trusted” and mistakenly signals its “clean bill of health” to the world. Other computers get infected as a result and taken over for a denial of service attack. Who, if anybody, is liable for the harm to those computers who trusted me?

From a legal perspective, one possibility would be to impose on me liability for the harm that ensues. If I leave my computer vulnerable and insufficiently protected, and it is later used in a crime, I too have to accept some of the blame and the liability, just as people might find themselves liable when they leave a gun in easy reach of children who then injure someone with it.¹⁰⁶ Our computers are dangerous for others, if we do not look after them properly, we should bear some responsibility even if a nefarious third party, a criminal, intervenes in the causal chain and exploits our negligence by harming others. However, for practical, conceptual and procedural reasons, this is not really an option. Ordinary users lack the know how to properly protect their computers – this we discussed in the beginning of the chapter. It would also expose them to potentially massive losses which can’t be quantified in advance. If I disable my firewall (because I ignorantly thought that it slowed down my video clips streaming) and my computer becomes compromised as a result, it could then be used on a Denial Of Service attack against the Bank of Scotland. The damage to which I contributed could reach the billions. If I’m held liable for this, then computer use would become impossible for ordinary citizens.

¹⁰⁶ For a discussion of the idea and a comparative analysis of some jurisdictions that impose liability, see McClurg, A. J. (2000). Armed and Dangerous: Tort Liability for the Negligent Storage of Firearms. *CONNECTICUT LAW REVIEW*, 32, pp. 1189-1246.

The affected user whose computer is zombified (taken over by an attacker)¹⁰⁷ will regularly lack the relevant intent, and also lacks the means to avoid such an attack. As the House of Lords notices, protecting yourself against the latest threats requires skills simply not available to many.¹⁰⁸ Also, each individual computer taken in isolation will have played only a marginal role in the attack, making it difficult to prove causality, and he also won't have the financial means to compensate for a large scale attack. As we discussed, TC is based on a recognition that the user is the weakest chain in the security link. The TC philosophy therefore takes the responsibility away from him entirely and passes it on to the software and hardware producers. However, in this new reality, *not* buying the product stops being an option, if not for legal, then for practical reasons: unless seen as trustworthy by other machines, the computer will not any longer be able to communicate with them, or communicate fully. It is at this point possible to return to the "virus" analogy from Chapter 2. TC is similar to a mandatory vaccination program, where "herd immunity" is achieved at the expense of individual choice. Many jurisdictions have rules that permit exactly this type of tradeoff in situations of great societal risk,¹⁰⁹ and it is not by coincidence that the UK, groups large scale DoS attacks together with the danger of a pandemic, as a tier one security risk.¹¹⁰

¹⁰⁷ on the term "zombie" and its role in DOS attacks, see Elliott, J. (2000). Distributed denial of service attacks and the zombie ant effect. *IT professional*(2), pp. 55-57.

¹⁰⁸ House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm>.

¹⁰⁹ Colgrove, J., & Bayer, R. (2005). Manifold restraints: liberty, public health, and the legacy of Jacobson v Massachusetts. *Am J Public Health*, 95 (4), pp. 571-576.

¹¹⁰ Cm7953. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: The Stationery Office Limited Retrieved from http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/d

4.2.4 Reliance liability

If holding the owner of an infected computer liable is not an option, and while if TC was established as a solution to the security problem, another option presents itself. As stated in the previous point, there is a contractual relationship between TC providers and the client (the user) which becomes relevant when the client relies on the TC certificate. However, can we also impose a tortious relationship between TC vendor and a third party relying on the TC certificate? In this case the third party could seek redress directly from the TC provider who issued the certificate to the client. If liability is expressed purely in monetary terms, this too may be a problem. Even though the TC provider is in a better position to insure himself, the risk would be open ended. This could deter investment in security. But the TC provider also has access to considerable computing expertise. What we suggest therefore is an obligation to make this expertise available to third parties who suffered a harm as a result of relying on an inappropriately issued attestation. This, again taking up the ideas of relational contract theory, would also match our extra-legal sense of responsibility. If I give a neighbor advice, based on my advanced computer knowledge, then I would not necessarily feel responsible for every economic harm that he incurs when acting on my advice, but I would feel the need to inform him as soon as I realize that I made a mistake, and to do my best to use my skills to mitigate the problem.

This type of delictual “reliance liability” has for instance been discussed in the context of engineers certifying an aircraft as airworthy, employers writing overly generous references for an employee who subsequently gains a position for which he is ill qualified,¹¹¹ or even publishers for publishing bee-keeping

ocuments/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritys
strategy.

¹¹¹ Allen, T. (1995). Liability for References: The House of Lords and *Spring v Guardian Assurance*. *The Modern Law Review*, 58(4), pp. 553-560. doi: 10.1111/j.1468-2230.1995.tb02031.x, Honsell, H. (1999). Die Haftung für Gutachten und Auskunft

manuals that contained erroneous information.¹¹² What all these cases have in common is that one party has superior knowledge and expertise, is seen as a trustworthy source of information by the wider community (and builds its business on this reputation) and relying on them for advice is therefore a rational decision to make. This bears clear similarities to both TC settings that we discussed. The TCG, as a consortium of the major soft- and hardware developers, has unique expertise on security issues, and also an insider view on computer vulnerabilities – after all, it is more often than not, their own software that is vulnerable, and knowledge about the defects is hidden by them behind trade secrets and copyright law.¹¹³ Indeed, the frequent refusal by companies to share security information and information of vulnerabilities could itself be constructed as a liability trigger, were it not for the fact that it remains unclear and disputed if openness or secrecy is the better policy to ensure security.¹¹⁴

4.2.5 Relying on the TCG

In this first scenario, we will analyse reliance liability with regards to the TCG as a group that certifies certain products as TC compliant. We do this by building an analogy to the better known and established Digital Trust Marks (TMs).

As more and more of our activities are carried out online, it has become increasingly clear over the past decades that the Internet, which was never intended for this type and scale of commercial activity, is vulnerable to attacks

unter besonderer Berücksichtigung von Drittinteressen *Festschrift für Dieter Medicus* (pp. 211-233). Heymann: Köln.

¹¹² Lane Jr, D. M. (1988). Publisher Liability for Material That Invites Reliance. *Tex. L. Rev.*, 66, pp. 1155-1629.

¹¹³ For a discussion of this problem see Swire, P. P. (2001). What should be hidden and open in computer security: lessons from deception, the art of war, law, and economic theory. *arXiv preprint cs/0109089*, pp. 1-54.

¹¹⁴ see e.g. Nowey, T., & Federrath, H. (2007). *Collection of Quantitative Data on Security Incidents*. Paper presented at the Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on (pp. 325-334),IEEE.

and criminal activities. Given the widespread acceptance of the commercialization of the Internet, e-commerce has experienced astonishing growth since its development in the 1990's. Security and privacy – amongst other issues – seem to be at the top of consumer's concerns while conducting online transactions.¹¹⁵ As recent statistics show, e-consumers do not feel secure at all in the online environment and this has an impact on their willingness to provide personal or payment details over the Internet.¹¹⁶

Not long time ago, powerful organized crime gangs target as victims uninformed and unprepared consumers and exploit weaknesses in their computer systems. Attempts to deal with the growing number of reported cybercrime incidents include legislation, user training, public awareness, and other technical security measures.¹¹⁷ The UK government recognizes the detrimental impact that a cyber attack can have on the economy and the social well being of the country and the effect of how nations deal with internet freedom and security.¹¹⁸

¹¹⁵ Cheng-Hao, C., & Saeedi, M. (2006). Building a Trust Model in the Online Market Place. *Journal of Internet Commerce*, 5(1), pp. 101. doi: 10.1300/J179v05n01•06, Endeshaw, A. (2001). The Legal Significance of Trustmarks. *Information & Communications Technology Law*, 10(2), pp. 203-230. doi: 10.1080/13600830120074690

¹¹⁶ Organisation for Economic Co-operation and Development. (2005). Scoping Study for the Measurement of Trust in the Online Environment *Working Party on Indicators for the Information Society*: Organisation for Economic Co-operation and Development, Organisation for Economic Co-operation and Development. (2008). Measuring Security and Trust in the Online Environment: A View Using Official Data. In t. a. i. c. f. i. Directorate for science, computer and communications policy (Ed.), *Working Party on Indicators for the Information Society*: Organisation for Economic Co-operation and Development.

¹¹⁷ Cm7642. (2009). Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space. London: The Stationery Office Limited.

¹¹⁸ Cm7234. (2007). The Government reply to the fifth report from the House of Lords Science and Technology committee. London: The Stationery Office Limited, Cm7948.

To reap the benefits of the ICT revolution, users must be able to trust their system. When asked to pay for goods bought online, to make a bank transfer from an online account, or to apply for a passport at a government run website, it is essential that the user can trust the communication to be secure, and that the party he is communicating to, is the party it claims it is. These are issues that go well beyond the remit of TC, whose sole function is protection against viruses or Trojans. It does not protect people from handing their bank details to “businesses” that have impressive websites and little else, using the stolen data for ID theft or online fraud. This type of “computer enabled crime” is for most people a greater concern than the fear that their own machine is hacked (the TC focus), discouraging potentially the economically beneficial uptake of e-services. In an effort to attract and maintain consumers, e-businesses seek ways to enhance consumers’ trust to the Internet and to e-commerce as such, to allow this “new way of transferring ownership or right to use good or services through a computer mediated network”¹¹⁹ to flourish and economy to raise.

4.3 TMs - Promoting the feeling of security and trust

Trustmarks (TMs) have been developed in the late 1990s as an attempt to develop and gain consumer trust through web signals and thus answer this problem.¹²⁰ The Trustmark Organisations (TMOs) which are also defined as

(2010). Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review. London: The Stationery Office Limited.

¹¹⁹ Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350

¹²⁰ See e.g. Aiken, K. D., Liu, B. S., Mackoy, R. D., & Osland, G. E. (2004). Building internet trust: signalling through trustmarks. *International Journal of Internet Marketing and Advertising*, 1(3), pp. 251-267. or De Bruin, R., Keuleers, E., Lazaro, C., Pouillet, Y., & Viersma, M. (2005). Analysis and Definition of Common Characteristics of Trustmarks and Web Seals in the European Union: Recuperado de http://ec.europa.eu/consumers/cons_int/e-commerce/e-commerce_final_report_annexe_en.pdf; For

Trusted Third Parties (TTPs), are independent parties that provide TMs to online merchants (e-merchants), as a way to label that a product, process or service - that the e-merchant offers - conforms to specific quality characteristics concerning legitimacy, security of transactions, privacy and integrity.

TMs are said to promote the feeling of security and trust to e-consumers¹²¹ thus influencing them to engage in e-commerce¹²² so when the e-merchant displays the TM on its website, the e-consumers will minimize their questioning of the integrity of that e-merchant in relation to security, privacy and business practice. In economic terms, this equates to a reduction in transaction costs.¹²³ This is mostly because e-consumers rely on the reputation of TMOs¹²⁴ and on the perception that “a third party gives a written assurance that a product, process,

the role in a particularly sensitive area, medical products and information, see Adams, S. A., & de Bont, A. A. (2007). More than just a mouse click: research into work practices behind the assignment of medical trust marks on the World Wide Web. *international journal of medical informatics*, 76, pp. S14-S20.

- ¹²¹ Houston, R. W., & Taylor, G. K. (1999). Consumer Perceptions of CPA WebTrustSM Assurances: Evidence of an Expectation Gap. *International Journal of Auditing*, 3(2), pp. 89-105. , Palmer, J. W., Bailey, J. P., & Faraj, S. (2000). The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements. *Journal of Computer-Mediated Communication*, 5(3), doi: 10.1111/j.1083-6101.2000.tb00342.x
- ¹²² Kovar, S. E., Burke, K. G., & Kovar, B. R. (2000). Consumer Responses to the CPA WEBTRUST Assurance. *Journal of Information Systems*, 14(1), pp. 17-35. , Mauldin, E., & Arunachalam, V. (2002). An Experimental Examination of Alternative Forms of Web Assurance for Business-to-Consumer e-Commerce. *Ibid.*, 16, pp. 33-54.
- ¹²³ See generally Barney, J. B., & Hansen, M. H. (1994). Trustworthiness as a source of competitive advantage. *Strategic management journal*, 15(S1), pp. 175-190. For an application to online environments, see Bunduchi, R. (2005). Business relationships in internet-based electronic markets: the role of goodwill trust and transaction costs. *Information Systems Journal*, 15(4), pp. 321-341.
- ¹²⁴ Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350

or service conforms to specific characteristics".¹²⁵ This is considered a form of guarantee,¹²⁶ though we have to be careful that it is the right type of guarantee. Warranties for instance, even though they too are guarantees and should perform a similar function, are often not increasing trust – probably because they remind the customer too much of all the things that can go wrong.¹²⁷ This matches to a degree our argument above about the “litigation centeredness” of classical contract law: if contracts are perceived as long lists of things that will go wrong, as EULAs frequently do, they are not trust enhancing. If they are read as a manual for a fruitful cooperation, they might. The procedure of giving a TM to an e-merchant goes like this: the e-merchant cooperates with the TMOs and asks for a TM, which he gains when he submits a satisfactory self-assessment report referring to the business’s security, privacy and practices.¹²⁸ However, it is significant to note that a large gap is identified between the online consumers’ actual needs for assurance and the assurance that seals are supposed to offer.¹²⁹

¹²⁵ Rae, A., Robert, P., & Hausen, H.-L. (1994). *Software Evaluation for Certification*. New York, NY: McGraw-Hill, Inc. .

¹²⁶ Dean, D. H., & Biswas, A. (2001). Third-Party Organization Endorsement of Products: An Advertising Cue Affecting Consumer Prepurchase Evaluation of Goods and Services. *Journal of Advertising*, 30(4), pp. 41-57. , Pacini, C., & Sinason, D. (1999). Auditor Liability for Electronic Commerce Transaction Assurance: The CPA/CA Webtrust. *American Business Law Journal*, 36(3), pp. 479.

¹²⁷ So e.g. Boulding, W., & Kirmani, A. (1993). A consumer-side experimental examination of signaling theory: do consumers perceive warranties as signals of quality? *Journal of Consumer Research*, pp. 111-123.

¹²⁸ Endeshaw, A. (2001). The Legal Significance of Trustmarks. *Information & Communications Technology Law*, 10(2), pp. 203-230. doi: 10.1080/13600830120074690

¹²⁹ Hu, X. R., Wu, G. H., Wu, Y. H., & Zhang, H. (2010). The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *DECISION SUPPORT SYSTEMS*, 48(2), pp. 407-418. , Odom, M. D., Kumar, A., & Saunders, L. (2002). Web Assurance Seals: How and Why They Influence Consumers' Decisions. *Journal of Information Systems*, 16(2), pp. 231-250.

4.4 The analogy between TMs and TC

While the legal system struggles to keep up with technology developments and their enforcement and prosecution, the regulation through technology took increasingly center stage.¹³⁰ Rather than prosecuting crime, the focus shifted on communicating architectures that make it impossible to commit crimes in the first place. One such architecture is the Trusted Computing (TC), Trustmarks are another. But while TC is like all law compliance by design “strongly paternalistic” in the sense that it prevents the user from doing certain things harmful to him, TM is closer to what Turilli Mateo and Luciano Floridi described as “pro-ethical design”: it provides assured information only, but leaves the ultimate decision to the user.¹³¹ To use a maybe slightly frivolous analogy: as a parent, you use TC with your infants, TM with your teenagers, whose autonomy and potential to reasonableness you have to respect despite all evidence to the contrary.

“TMs are seen as information on somebody or something to be relied upon by others”.¹³² In fact, the e-consumer is “nudged” from the mark (TM) on the e-merchant’s website to trust that e-merchant and engage in business with him. In the case that the collaboration between the e-merchant and the TMOs breaks down however, ends or was never properly enforced, the TM system has been proved to be potentially weak: cases have been reported that e.g. e-consumers’

¹³⁰ Lessig, L. (1996). The Zones of Cyberspace. *Stanford Law Review*, 48(5), pp. 1403-1411.

¹³¹ For the distinction between pro-ethical design and paternalistic design see Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology*, 11(2), pp. 105-112.

¹³² Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350

personal identifying data were kept, shared or sold by e-merchants without the data subject's consent and without the TMO's knowing.¹³³

In these cases the TMO issued the TM to such e-merchants - who kept the TM on their website at the time the malpractice occurred and remained there after the violation was discovered¹³⁴ – causing damages¹³⁵ to e-consumers.¹³⁶ Thus, it is obvious that the reliance to the trust provided by TMs is potentially treacherous and TMOs services can be unreliable and generally lacking in accountability.¹³⁷

In our present study, we aim to provide a comparison between TMOs, and TC in order for both technologies to profit from each other. We argue that both fulfil analogous roles, (see Figure 5) in the sense that TC can provide information (assurances) that a platform is to be trusted, so that a third-party (i.e. another user's machine) can rely upon and proceed with successful communication and exchange of information. The user of the platform communicates with a verifier who wants to assure that the user uses the platform containing the specified TPM.

¹³³ Froomkin, A. M. (2000). The Death of Privacy? *Stanford Law Review*, 52(5), pp. 1461-1543. , Kornblum, J. (1998). FTC, GeoCities Settle on Privacy, *CNET News.com*. Retrieved from <http://news.cnet.com/news/0-1005-200-332199.html>, McCarthy, J. (1999). TRUSTe Decides Its Own Fate Today, *Slashdot*. Retrieved from <http://slashdot.org/yro/99/11/05/1021214.shtml>

¹³⁴ McCarthy, J. (1999). TRUSTe Decides Its Own Fate Today, *Slashdot*. Retrieved from <http://slashdot.org/yro/99/11/05/1021214.shtml>

¹³⁵ Damages include violation of e-consumer's privacy and data protection right to pure economic loss.

¹³⁶ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995).

¹³⁷ Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350

In the same way TMs are seen as information that somebody or someone can rely upon by third-parties (e-consumers).

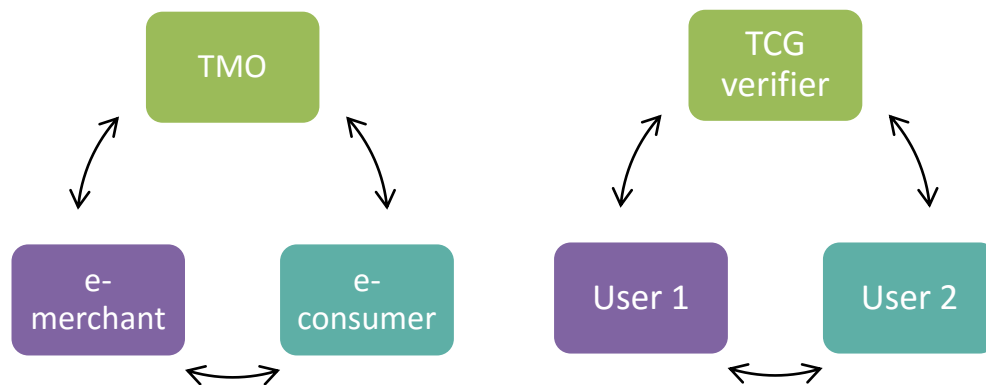


Figure 5: Analogy between TMOs (left) and TC (right)

As we saw, the whole TC procedure is automated using one out of the four main features of TC technology, the *remote attestation*. This aims to allow “unauthorized” changes to software to be detected. It remotely traces any changes made to any application and allows a third party to decide whether the platform is considered trustworthy.¹³⁸ This feature helps to prevent the sending of data to or from a compromised or untrustworthy computer and certifies that no unauthorised program installs, updates or modifications are made in the hardware or software on the user’s machine. Moreover, “this allows an entity to authenticate the software configuration of a platform that is not under its control”.¹³⁹ Here we can see one main difference between TC and TM: *If* TC is functioning correctly, it is nearly impossible to fool the trusted third party that attests the correct working of a platform. This security comes at a “cost”: the

¹³⁸ Reid, J., Gonzalez Nieto, J., Dawson, E., Okamoto, E. (2003). *Privacy and Trusted Computing*. Paper presented at the Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA’03) (2003), Washington (pp. 383-388),IEEE.

¹³⁹ *ibid.* p.3

assurance provider has real time access to the computer whose safe functioning it attests, raising concerns about privacy in particular.

We can see more clearly the differences if we compare this approach with SysTrust, a TM approach initiated by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). SysTrust, is a service which aims to independently assure business and customers that an organisation's systems are reliable.¹⁴⁰ SysTrust procedures, in conformity with attestation standards of the AICPA, determine the effectiveness of controls that make a system operate reliably. Reliability is determined through four criteria: security (from physical or electronic unauthorized access), availability (operational readiness and access as agreed), integrity (the system should be complete, accurate, prompt, and authorized in processing of information) and confidentiality in terms of information that are kept.¹⁴¹

It has been argued however by critics that such TM systems are more marketing based than quality based, which leads to questions on the credibility of the TM system in the long run.¹⁴² The TM provider has no incentives to probe too deeply the credentials of the company it certifies – who might desert him for a less stringent TM provider. Nor will it be always feasible to check the submitted data for its correctness – as seen above, the type of features that TM attests are much less demanding, but also more woolly and imprecise than the very formal properties assured and certified by TC. Therefore, the danger of opportunistic

¹⁴⁰ American Institute of Certified Public Accountants Inc., & Canadian Institute of Chartered Accountants. (2006). Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (Including WebTrust® and SysTrust®) *Trust Services Principles, Criteria, and Illustrations* (pp. 155).

¹⁴¹ Endeshaw, A. (2001). The Legal Significance of Trustmarks. *Information & Communications Technology Law*, 10(2), pp. 203-230. doi: 10.1080/13600830120074690

¹⁴² Riegelsberger, J., & Sasse, M. A. (2000). Trust me, I'm a .com. The Problem of Reassuring Shoppers in Electronic Retail Environments. *Intermedia*, 28(4).

behaviour by e-traders, along with unregulated market forces, are forcing TMOs to a more untrustworthy practice that needs to be altered.¹⁴³

4.5 Legal environments for digital trust

In analogy to the case scenarios for TC that we introduced above, we can now ask:

1. what e-consumers can do in order to recover the damage from their reliance on the TM and
2. the fundamental liability question is whether the TMOs are to be held liable to e-consumers, for their damages.

The legal relationship between the two parties (i.e. the TMOs and the e-merchants) of the TM procedure is contractual; however, an implied tortious relationship between the TMOs and e-consumers can be argued as the e-consumers relied on the certificates that the TMO's issued (see Figure 5). This quasi-contractual relationship cannot at least be excluded *a priori*.

Even though TM is a more mature and tested approach than TC, the issue of liability of TMOs hasn't been given much attention from courts or governments, but unlike with TC, where this thesis tries to start a discussion, there is at least beginning of an academic debate on that issue.

As stated earlier, in cases where the e-consumer suffers damages due to his reliance on the TM that has been issued on the e-merchant's website, the consumer could sue the e-merchant for breach of contract or in tort for wilful act or breach of their duty of care (negligence liability). However, the easiness with which anyone can set up a commercial website selling products or services

¹⁴³ Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350

through the Internet,¹⁴⁴ decreases the chance for an e-consumer to seek vindication against negligent or malicious e-merchants. Therefore, it is easier for the e-consumer to locate and sue the TMO for the provision of inaccurate information (TMs) on the e-merchants website and also request for compensation. There are TMs that use a redress mechanism that “may also have character as a third-party guarantee, where the consumer may seek redress”.¹⁴⁵ The redress is not necessarily monetary, but it provides at least access to mediation and with that room for a highly flexible system of assigning duties to the TMO that issues an unmerited certificate. We agree moreover with Balboni that the TMO third-party legal liability systems are inadequate when we compare them with Certification Service providers (CSPs) (i.e. auditors/ accountants and surveyors) which are considered TMO’s equivalents, in terms of liability rules.¹⁴⁶ Article 6 of the EU’s Electronic Signatures Directive¹⁴⁷ describes third-party liability of CSPs and in England this is incorporated into the Electronic Signatures Directive in Section 4.¹⁴⁸ The issue of TMOs third-party liability has been at least

¹⁴⁴ For an analysis on the barriers for spotting an e-merchant who has set up a commercial website see *ibid.* p.28

¹⁴⁵ Trzaskowski, J. (2010). *Chapter 3 Legislation and requirements concerning Trustmarks*. In E. C. C. Denmark (Series Ed.) *E-Commerce Trustmarks in Europe* Retrieved from <http://dokumenter.forbrug.dk/forbrugereuropa/e-commerce-trustmarks-in-europe/helepubl.htm>

¹⁴⁶ Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350

¹⁴⁷ Balboni, P. (2004). Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication. *Information & Communications Technology Law*, 13(3), pp. 211-242. doi: 10.1080/1360083042000219074, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 43 C.F.R. (2000).

¹⁴⁸ The Electronic Signatures Regulations 2002 (2002).

discussed by Balboni¹⁴⁹ and others¹⁵⁰ who have analysed liability more closely and made proposal for a model of adequate TMO liability.¹⁵¹ Their outcomes are described in the following section.

While there is no case law and almost no literature on the liability of TMOs that offers direct protection against damages caused by reliance on information,¹⁵² as pointed out by Balboni there is a strong case to be made for TMOs third-party liability legal issue towards e-consumers.¹⁵³ As he shows, if we analyse this problem from a first principle basis, then the general principles of civil liability, tort and contract law alone should be sufficient to make a case for reliance liability for TMO – at least in the absence of explicit “do not trust this TM” notices.

¹⁴⁹ Balboni, P. (2004). Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication. *Information & Communications Technology Law*, 13(3), pp. 211-242. doi: 10.1080/1360083042000219074

¹⁵⁰ Endeshaw, A. (2001). The Legal Significance of Trustmarks. *Ibid.*, 10(2), pp. 203-230. doi: 10.1080/13600830120074690, Terry, N. P. (2000). Rating the "Raters": Legal Exposure of Trustmark Authorities in the Context of Consumer Health Informatics. *Journal of Medical Internet Research*, 2(3), doi: 10.2196/jmir.2.3.e18, Wendel, P. T. (2004-2005). The Evolution of the Law of Trustee's Powers and Third Party Liability for Participating in a Breach of Trust: An Economic Analysis. *Seton Hall L. Rev.*, 35, pp. 971 - 1028.

¹⁵¹ Balboni, P. (2008a). Model for an adequate liability system for Trustmark Organisations. *INTERNATIONAL JOURNAL OF LIABILITY AND SCIENTIFIC ENQUIRY*, 1(1/2), pp. 151-163.

¹⁵² Schellekens, M., & Prins, C. (2006). Unreliable information on the internet: a challenging dilemma for the law. *Journal of Information, Communication and Ethics in Society*, 4(1), pp. 49 - 59.

¹⁵³ Balboni, P. (2008a). Model for an adequate liability system for Trustmark Organisations. *INTERNATIONAL JOURNAL OF LIABILITY AND SCIENTIFIC ENQUIRY*, 1(1/2), pp. 151-163.

The issue that arises now is that TMOs usually tend to include specific clauses¹⁵⁴ on their contracts in order to limit or exclude in some cases, the liability towards e-merchants and e-consumers. And this is where we see a paradox: “TMOs are seen as professionals who provide information on their clients, or their clients’ practice, to be relied upon by third parties”¹⁵⁵ and therefore enhance e-consumer’s trust. It is then highly unlikely that an e-consumer will trust e-merchant’s security, privacy and business practices if the TMO - that certifies the aforementioned - refuses (through those disclaimers) any kind of liability in relation to the certificates.

E-consumers will have to invoke either the general principles of tort and contract law or on statutory provisions and case law that may be applied in analogy to TMOs. Based on an extensive analysis done by Balboni on US and European legal systems concerning third-party liability, most commonly e-consumers will have to provide evidence

- for the damages they incurred,
- against the decision of the TMO to issue the TM (i.e. prove that the TMO owes a duty of care towards the consumer and that the TMO acted in a way that breached the duty of care) and
- for the causal link between the TMO’s professional fault and the plaintiff’s occurred damage.

¹⁵⁴ Clauses limiting or excluding the liability of TMOs to e-consumers can be found on the TMO’s website. For a selection of the most commonly used clauses that TMOs are using to limit their liability see Ibid. p.153

¹⁵⁵ Balboni, P. (2008a). Model for an adequate liability system for Trustmark Organisations. *INTERNATIONAL JOURNAL OF LIABILITY AND SCIENTIFIC ENQUIRY*, 1(1/2), pp. 151-163.

For the last point, it is a prerequisite to prove both 'foreseeability'¹⁵⁶ and 'proximity'¹⁵⁷. However in the absence of specific provisions, third-party TMO liability will be based on policy arguments.¹⁵⁸ It worth to be noted that under the 2005 Directive on Unfair Commercial Practices,¹⁵⁹ TMs can be considered as unfair commercial practice if they are not provisional on setting higher standards of consumer protection compared to the protection offered by legislation. In fact, it will be a requirement to consider advertising and using a TM with equal levels of consumer protection and legislative requirements, as unfair commercial practice, under national or community law.¹⁶⁰ In particular Annex I of the Directive comprises a list of commercial practices which are considered unfair.

From this we can conclude that a good case can be made for a degree of reliance liability of TM providers under the general principles of tort law. TC providers as we saw are in a better position to assure the integrity of their products than TM providers, they are less likely to be impacted by imprudent consumer choices (as TC is fully automatic) and the direct damage is more

¹⁵⁶ 'Foreseeability' determines if the harm caused to the plaintiff, resulting from an action by the defendant was reasonably able to be predicted. Epstein, R. A. (1989). Beyond Foreseeability: Consequential Damages in the Law of Contract. *The Journal of Legal Studies*, 18(1), pp. 105-138. , Keeton, W. P. (1984). *Prosser and Keeton on Torts* (5 Sub edition ed.). St. Paul MN: West Group, Leon, G. (1961). Foreseeability in Negligence Law. *Columbia Law Review*, 61(8), pp. 1401-1424.

¹⁵⁷ The function of proximity is concerned with how one party is placed in regard to the other party. Mendelson, D. (1994). The law of torts *Deakin Law Review*, pp. 255 - 260.

¹⁵⁸ Balboni, P. (2008a). Model for an adequate liability system for Trustmark Organisations. *INTERNATIONAL JOURNAL OF LIABILITY AND SCIENTIFIC ENQUIRY*, 1(1/2), pp. 151-163.

¹⁵⁹ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (2005).

¹⁶⁰ Trzaskowski, J. (2010). *Chapter 3 Legislation and requirements concerning Trustmarks*. In E. C. C. Denmark (Series Ed.) *E-Commerce Trustmarks in Europe* Retrieved from <http://dokumenter.forbrug.dk/forbrugereuropa/e-commerce-trustmarks-in-europe/helepubl.htm>

foreseeable: opening the computer for an attack. This means the absence of the policy objections could be used, as per Balboni's analysis, to deny reliance liability even though general tort principles allow it. TC in this sense is closer still to Certification Service Providers, even if it lacks at present their tight regulatory framework. For them, Certification Service Providers (CSPs) (surveyors, accountants, auditors and crucially in an online context, e-signature verifiers) reliance liability is often explicitly regulated by statute. As Balboni pointed out in his research on the liability issue, by applying the set of rules set by Article 6 of the Electronic Signatures Directive, which map out fault-based third party liability for CSPs, and postulate CSP's liability towards third-parties who suffer from damages as a result of their reasonable reliance on CSP certificates.¹⁶¹ In the same way, TMOs can be held liable to e-consumers who reasonably rely on the TM and then suffer loss from such reliance, for the information included in the TM at the time of issue, even though the TMO has not provided evidence of negligence.

Our literature survey suggests that while computer scientists seem primarily concerned with the technical feasibility of implementing TC, legal academics have tended to concentrate on content control and privacy issues.¹⁶² Neither group

¹⁶¹ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 43 C.F.R. (2000), The Electronic Signatures Regulations 2002 (2002).

¹⁶² Anderson, R. (2003a). Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA - Version 1.1. (2003). <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>, Anderson, R. (2004). Cryptography and Competition Policy - Issues with 'Trusted Computing' *Economics of Information Security* (Vol. 12, pp. 35-52): Springer US, Bradgate, R. (1999). Beyond the Millennium - The Legal Issues: Sale of Goods Issues and the Millennium Bug. *The Journal of Information, Law and Technology (JILT)*, 2, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_1992/bradgate/, Chandler, A. J. (2003). Security in Cyberspace: Combatting Distributed Denial of Service Attacks. *University of Ottawa Law and Technology Journal*, 1(1-2), pp. 231-261. , Charlesworth, A. (2005). DRM: the Straw to Break of Procrustean Approaches

appears to be overly concerned with an analysis of the implications of the imposition of legal liability for failure within such a system, or potential responsibility for wider social and legal concerns to which they may give rise. If greater legal responsibility is placed upon hardware/software providers, this may have a significant impact upon the speed and scope of system roll-out, and may leave the system vulnerable to threats from market pressures.

A model of adequate third-party liability for TMOs is elaborated based on the principles of CSPs liability developing the concept of 'adequacy'.¹⁶³ Through this concept, liability rules need to protect the e-consumer's expectations when trusting the TMOs, while at the same time, the difficulties that TMOs face because of their operation online can be considered.¹⁶⁴ This is the type of "contextual" analysis that follows the spirit of relational contract theory: do not focus on the

to Copyright? In F. Grosheide & J. J. Brinkhof (Eds.), *Intellectual Property 2004: Articles on Crossing Borders between traditional and actual (Molengrafica Series)* (pp. 405-422): Intersentia, Erickson, J. S. (2003). Fair use, DRM, and Trusted Computing. *Communications of the ACM*, 46(4), pp. 34-39. , Hilley, S. (2004). Trusted computing - path to security or road to servitude? *Network Security*, 2004(8), pp. 12-15. , Pearson, S. (2005, 23-26 May 2006). *Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy*. Paper presented at the Proceedings of the Trust Management: Third International Conference, iTrust 2005, Paris, France (pp. 305-320), Springer-Verlag GmbH, Reid, J., Gonzalez Nieto, J., Dawson, E., Okamoto, E. (2003). *Privacy and Trusted Computing*. Paper presented at the Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03) (2003), Washington (pp. 383-388), IEEE, Samuelson, P. (2003). DRM {and, or vs.} the Law. *Communications of the ACM*, 46(4), pp. 41-45. , Turner, M., Budgen, D., Brereton, P. (2003). Turning software into a service. *Computer -- IEEE Computer Society*, 36(10), pp. 38- 44. , Woodford, C. (2004). Trusted Computing or Big Brother? Putting the Rights back to Digital Rights Management. *U. Colo. L. Rev.*, 75, pp. 253-300.

¹⁶³ Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350

¹⁶⁴ Balboni, P. (2008a). Model for an adequate liability system for Trustmark Organisations. *INTERNATIONAL JOURNAL OF LIABILITY AND SCIENTIFIC ENQUIRY*, 1(1/2), pp. 151-163.

magic moment where a customer enters a contract with a TM certified merchant, consider the entire transactional environment, and what signals were sent by the parties. Such a liability system should also improve TMOs practice quality level in order to give TMs the ability to extend their potentials and benefits in social, economic and political levels.¹⁶⁵ Balboni evokes the ethical theory of Warranted Trust to protect both TMOs and e-consumers and develops the context in which their trust relationship is constructed,¹⁶⁶ an approach equivalent to the relational contract theory described above, but with less direct connection to doctrinal legal issues.

Similarly, we argue that based on the TMOs third-party liability, the TC reliance liability should be structured as statutory regulations that can be potentially applicable by analogy. The same concept of 'adequacy' which is defined by relating the trust relationship between TMOs and e-consumers should be applied in the trust relationship between TC and TC consumers.

Indeed, in many ways TC is the more obvious target of the reliance liability that Balboni discusses, than TM. The TC philosophy takes the responsibility away from the user entirely and passes it on to the software and hardware producers. Imagine if the user wants to verify that a legitimate TMO is behind that TM. The user then clicks on a TM, and for his surprise is transferred to a spoofed website, and he realizes that the TMO is not the one that claimed to be. An automated system, just like a TC, ought to be able to prevent this from happening, and damages for the user to incur. Where in the non-automatic TMO environment, it is ultimately a decision by the customer whether to trust a TM, or to engage with a site without one, in TC that choice will be more and more limited by design.

¹⁶⁵ *ibid.* p.155

¹⁶⁶ Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350

With that, legal issues of intervening causality that could be seen as an obstacle to reliance liability are removed.

4.6 Wrap-up

TMOs, unlike TC, rely ultimately on human judgment, and unless backed up by a strong regulatory regime could lead to a perception where TMOs are untrustworthy, in contrast with their initial aim, and non accountable. At the moment, Europe, as well as US, are arguably inefficient in specific statutory provisions and case law on TMO third-party liability which makes things harder – if not impossible – for e-consumers to enforce TMO third-party liability in cases they suffer damages from their reasonable reliance on TMs. Therefore, the TM system will be questioned and e-consumer's trust will be lost once more.

More generally, due to the unreliability of some TMOs practices, all players could ultimately be damaged: the reputation of the TM program damaged by a run to the bottom, e-merchants will run the risk of housing an untrustworthy TM which other e-merchants used and violated, and e-consumer's trust in e-commerce will decrease. Consequently, e-business and e-economies will be hurt and governments which remain reluctant to regulate in this matter will allow untrustworthy TMOs spreading out.

In fact, the absence of specific rules on TMO liability creates a legal 'immunity' for TMOs, which is unacceptable. As Balboni proposed,¹⁶⁷ floodgates arguments which are widely used to limit third-party parties that can rely on the TM, should be taken into consideration. As a solution, he proposed that TMOs could reasonably limit their liability as it happens, following the example of the CSP's liability provision set in Article 6 of the Electronic signatures directive¹⁶⁸

¹⁶⁷ *ibid.* p.131

¹⁶⁸ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 43 C.F.R. (2000).

and European governments should sooner or later act on this issue before it is too late.

4.7 Regulating reliance

The previous section made the case for reliance liability for the TCG when it acts in a function similar to a Certification Authority and certifies individual TC products “in abstracto”. This, we argued, is similar to a TMO or a Certifying Service Provider Authority: They all base their certification on a methodological self-assessment of the certified party which submits evidence in form of data, protocols, accounts of internal procedures, or in the case of a TC program, specifications. These are then more (CSP) or less (TMO) rigorously tested for their truthfulness. TC, as our interviews show, can test to a rather great extent, though not completely, what exactly every proposed component or product submitted for certification is doing.

We now turn to the second setting, the application of TC in specific interactions. In this scenario, my computer calculates its own trustworthiness, has it remotely attested by the TC provider, and communicates this to a third party. What is the status of this communication, and if it is misleading, is there an avenue for recourse to the TC attestator?

Our argument will use an analogy to similar certification in offline settings which have been around for a long time in both cases – some jurisdictions do impose reliance liability.

We will examine two different concrete cases starting with an employers’ reference letter writing. When an employee seeks a new job, prospective employers are asking for reference letters retained by previous employers in order to evaluate employees’ job performance, productivity, adaptability, reliability, efficiency and character to make a job assignment decision. Pre-employment screening of the applicant is the most important aim of a reference

letter which helps prospective employers¹⁶⁹ avoid hiring staff which are unsuitable, especially in high-risk situations, like school teachers, truck, bus or train drivers, pilots and others. Some of these will work in environments that impose specific legal duties for background checks of their employees.¹⁷⁰ A high profile case in point is that of Ariel Castro a former school bus driver for 22 years, who was sentenced to life plus 1000 years of imprisonment “after pleading guilty to 937 charges including aggravated murder, kidnapping, rape and assault that allowed him to avoid the death penalty”.¹⁷¹ During his employment as a school bus driver, he had been divorced by his wife while he was accused of attacking her and violently abusing his wife and their children. Work colleagues in a previous job had reported hating working with him, as he was not treating school children well, which was documented in support of the school’s decision to fire him after a sequence of incidents with school students. Nonetheless, this history had been omitted in the reference letter to the next employer – possibly hoping that the problem, and an unfair dismissal charge, might go away.¹⁷²

In the case where a job reference given is not accurate either in full or partially (selectively omitting crucial information for the employee),¹⁷³ problems may arise when the prospective employer, reasonably relying on the job reference given by a previous employer hires the employee, which at the end is proved to be unsuitable of the job and results in a foreseeable personal injury, tragic social

¹⁶⁹ Gatewood, R., & Hubert, F. (1998). *Human resource selection*. Fort Worth, Tex.: Dryden Press.

¹⁷⁰ See e.g. Connerley, M. L., Arvey, R. D., & Bernardy, C. J. (2001). Criminal background checks for prospective and current employees: Current practices among municipal agencies. *Public Personnel Management*, 30(2), pp. 173-183.

¹⁷¹ News, B. (2013). Profile: Cleveland abductor Ariel Castro, *BBC News*. Retrieved from <http://www.bbc.com/news/world-us-canada-22444882>

¹⁷² Sperber, A. J. (1997-1998). When Nondisclosure Becomes Misrepresentation: Shaping Employer Liability for Incomplete Job References. *University of San Francisco Law Review*, 32(405), pp. 28.

¹⁷³ *ibid.* p.407

losses as well as hamper the employer's business reputation. Injuries can occur, either within the business environment, or by an employee outside of the environment of the business during working hours or not.

Should an employer be held liable, for the negligent misrepresentation of the employee's qualifications or for inadequately supplying information for him to subsequent employers? In fact should liability be imposed on the referring employer for recommending an employee that was proved to be unsuitable for the job by selectively omitting important information?

Different problems are arising in this case if courts do impose liability for selective omissions – in this case referring employers in their effort to guard themselves against negligent misrepresentation liability can possibly disclose all the employee's negative qualities, which in turn can cause privacy concerns. Should e.g. an employer mention in a reference that the candidate had an affair with a co-workers wife, badly affecting work morale?¹⁷⁴ On the other end, former employers could possibly minimise the amount of information given for an employee down to the strictly essential, thus significantly reducing the value of a job reference letter. Or even worse they can refuse a reference letter to a former employee and disseminate information about their employees following a “no comment” policy, to avoid defamation liability¹⁷⁵ or negligent misrepresentation

¹⁷⁴ *ibid.* p.408

¹⁷⁵ The thread for defamation liability can deter a former employer from giving a reference letter, including either totally true or totally false references. Statistics over a pilot study prove this fear for legal repercussions by employers, although they admit the need for reference letters when they are recruiting themselves Adler, R. S., & Peirce, E. R. (1996). Encouraging Employers to Abandon Their No Comment Policies Regarding Job References: A Reform Proposal [article] (pp. 1381), Harshman, E., & Chachere, D. (2000). Employee References: Between the Legal Devil and the Ethical Deep Blue Sea. *Journal of Business Ethics*, 23(1), pp. 29-39. doi: 10.1023/a:1006218926970. Still, an employer's refusal for a reference letter can be conceived as defamation Skopic, K. E. (1986-1987). Potential Employer Liability for Employee References. *University of Richmond Law Review*, 21, pp. 28.

liability affecting both the quality and quantity of information given to a prospective employer.¹⁷⁶ “No comment” policies have been excessively extended through years, and are definitely not working in favour either of the prospective employer nor the candidate employee leading to detrimental effects also being socially undesirable¹⁷⁷ plus exposes others to harm that could have been avoided.¹⁷⁸ There have been various proposals on how employers can deal with these issues and avoid these significant legal issues,¹⁷⁹ which outweigh the benefits of providing a reference, as well as to encourage employers to provide reference letters,¹⁸⁰ restoring the social balance.¹⁸¹ Ethics and social responsibility have also been discussed.¹⁸²

In the light of these issues, there has been discussion on reforming defamation law or compel disclosure obligations on employers¹⁸³ which are not

¹⁷⁶ Sperber, A. J. (1997-1998). When Nondisclosure Becomes Misrepresentation: Shaping Employer Liability for Incomplete Job References. *University of San Francisco Law Review*, 32(405), pp. 28.

¹⁷⁷ Saxton, B. (1995). Flaws in the Laws Governing Employment References: Problems of Overdeterrence and Proposal for Reform. *Yale L. & Pol'y Rev.*, 13.

¹⁷⁸ *Randi v. Muroc Joint Unified School Dist.* 1066, 1929 P.1062d 1582, 1060 Cal. Rptr. 1062d 1263 (14 Cal. 4th 1997).

¹⁷⁹ Saltzman, A. (1997). Suppose they sue? *U.S. News & World Report*, 123(11), pp. 68. , Swerdlow, J. (1990-1991). Negligent Referral: A Potential Theory for Employer Liability. *Southern California Law Review*, 64, pp. 30.

¹⁸⁰ Saxton, B. (1995). Flaws in the Laws Governing Employment References: Problems of Overdeterrence and Proposal for Reform. *Yale L. & Pol'y Rev.*, 13.

¹⁸¹ Adler, R. S., & Peirce, E. R. (1996). Encouraging Employers to Abandon Their No Comment Policies Regarding Job References: A Reform Proposal [article] (pp. 1381).

¹⁸² Harshman, E., & Chachere, D. (2000). Employee References: Between the Legal Devil and the Ethical Deep Blue Sea. *Journal of Business Ethics*, 23(1), pp. 29-39. doi: 10.1023/a:1006218926970

¹⁸³ In the start of the previous century Missouri state first Wages, Hours and Dismissal Rights § 290.140, 3020 Stat. (1909). and a number of other states later on IND. CODE ANN., Information Maintained by the Office of Code Revision Indiana Legislative Services Agency § 22-6-3-1 (1994)., enacted a legislation that for every employee of any corporation that is fired or voluntarily quits a service, the former employer's

as effective as expected.¹⁸⁴ However many cases¹⁸⁵ suggest that former employers should be held liable for negligent or fraudulent referral towards third parties that suffer substantial risk of physical harm, for selective omissions¹⁸⁶ in the recommendation letter provided. Sections 311¹⁸⁷ and 323¹⁸⁸ of the Restatement (Second) of Agency which are extensively applied to the employment reference situation, clearly state the subject of reliance liability:

§ 311

(1) One who negligently gives false information to another is subject to liability for physical harm caused by action taken by the other in reasonable reliance upon such information, where such harm results

- a) to the other, or
- b) to such third persons as the actor should expect to be put in peril by the action taken.

(2) Such negligence may consist of failure to exercise reasonable care

- a) in ascertaining the accuracy of the information, or
- b) in the manner in which it is communicated.

§ 323

One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the

manager is responsible to issue a reference letter known as “service-letter” stating between other information the true reason for the employees discharge or cause for the employee to quit such service.

¹⁸⁴ Verkerke, J. H. (1998). Legal Regulation of Employment Reference Practices. *The University of Chicago Law Review*, 65(1).

¹⁸⁵ Such as *Akins v. Estes*, 888 35 (S.W.2d 1994), *Gutzan v. Altair Airlines, Inc.*, 766 F.2d 135 (United States Court of Appeals 1985), *Randi v. Muroc Joint Unified School Dist.* 1066, 1929 P.1062d 1582, 1060 Cal. Rptr. 1062d 1263 (14 Cal. 4th 1997).

¹⁸⁶ Either because the former employee fails to provide or affirmatively misrepresents information about a former employee

¹⁸⁷ Restatement (Second) of Agency, §311, NEGLIGENCE MISREPRESENTATION INVOLVING RISK OF PHYSICAL HARM (1977a).

¹⁸⁸ Restatement (Second) of Agency, §323, NEGLIGENCE PERFORMANCE OF UNDERTAKING TO RENDER SERVICES (1977b).

protection of the other's person or things, is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking, if

- a) his failure to exercise such care increases the risk of such harm, or
- b) the harm is suffered because of the other's reliance upon the undertaking.

Although there have been debates whether and how to regulate employment reference letters, in such cases the court suggested that every former employer should give a complete recommendation letter without omitting facts or negative information for the prospective employee, thus leading to a deceptively incomplete recommendation. These courts thus recognise the tort of negligent misrepresentation of information regarding job reference letters.¹⁸⁹ Here we can identify a *special relationship* between the former employer and the potential employer as they depend upon one another. The latter *relies* and depends on the first, that the reference letter he acquires about a candidate will be accurate, truth, honest and comprehensive in all aspects concerning the employee's suitability for the job and will not omit any negative elements or be overly generous. The reliance lies to the fact that only the former employer of the candidate is in the best position to know the truth about the candidate's suitability for the job and it is reasonable to believe that a prospective employer will rely on any information acquired in order to take the hiring decision. Former employers would be logical to expect suits over faulty references or misrepresentation by third parties when a misleading reference that they have given, leads to a negligent hiring.

On the other hand this can create fear to any prospective employer under the light of negligent hiring, and furthermore create a situation where the

¹⁸⁹ Sperber, A. J. (1997-1998). When Nondisclosure Becomes Misrepresentation: Shaping Employer Liability for Incomplete Job References. *University of San Francisco Law Review*, 32(405), pp. 28.

prospective employer could claim¹⁹⁰ and would need to explore whether the former employer had a duty to warn that the candidate could foreseeably pose danger to the prospective employer's business, or to the general public.¹⁹¹ Under this theory the defamation fear seems to emerge, as a fired candidate can sue the former employer in case that the reason for the loss of a job opportunity amounted to defamation.¹⁹²

Courts have also recognised the tort of negligent hiring of an employee obliging every prospective employer to reasonably investigate a candidate's background before employment and make sure that he will not pose any threat of injury for any member of the public.¹⁹³ This may be interpreted as "a social mandate that employers must exercise reasonable care to hire workers who will work safely with co-workers and members of the public".¹⁹⁴ Under this tort "employers may be liable to employees or members of the public who are injured by an employee whom the employer hired without a reasonable investigation".¹⁹⁵

The issue still remaining, is how to judge whether the prospective employer's investigation on a candidate's background has been sufficient.¹⁹⁶ In case that a personal injury occurs, the plaintiff can sue the current employer and that would solve the problem as liability is posed by this theory. It is important to note that plaintiff successes in case of lawsuits outweigh defences in negligent hiring actions.

¹⁹⁰ Cohen v. Wales, 133 A.D.2d 94, 518 N.Y.S.512d 633 (Supreme Court of the State of New York 1987).

¹⁹¹ Swerdlow, J. (1990-1991). Negligent Referral: A Potential Theory for Employer Liability. *Southern California Law Review*, 64, pp. 30.

¹⁹² *ibid.* p.1645

¹⁹³ Restatement (Second) of Agency, § 213(b) (1958).

¹⁹⁴ Saxton, B. (1995). Flaws in the Laws Governing Employment References: Problems of Overdeterrence and Proposal for Reform. *Yale L. & Pol'y Rev.*, 13.

¹⁹⁵ *ibid.* p.76

¹⁹⁶ Swerdlow, J. (1990-1991). Negligent Referral: A Potential Theory for Employer Liability. *Southern California Law Review*, 64, pp. 30.

How can we relate this back to TC? In our discussion in Chapter 2, we encountered several ways in which “trust” can be build. One way we encountered was “inductive, experience based trust”: if you observe over an extended period of time that someone behaved trustworthy, you conclude that he is going to be trustworthy in the future until proven otherwise. This is not a perfect proof, but the best evidence that will often be available. TC incorporates this idea directly – the TC components monitor the behaviour of “their” computer, and if there is no evidence for tampering in the past, signal that it is trustworthy. Sitting on the certified customer’s computer they are in an ideal position to monitor the behaviour. In both the employment situation and the TC situation, I have to accept that my activities are monitored to some degree. Moreover, in the employment situation, I *want* and *need* my employer to write a reference for me, and thus have to enable this by sharing information with him, and allowing him in turn to share it with third parties. This corresponds to the necessary disclosure of private information that comes with TC that we discussed in the second chapter, and may also shed a new perspective on the more widely discussed issue of privacy and TC. If my employer blocks me from finding a new job by giving untrue information about me, I can have in some cases a defamation remedy. We are not going as far as suggesting that a mistakenly refused trustworthiness attestation is actionable under defamation law (as interesting as this proposition sounds). We treat it more in the spirit of relational contract theory again – I have a protected expectation that what my computer tells about me is correct, which forms part of the secondary network of obligations that comes with every transaction. The hiring employer in turn has an actionable interest in the correctness of the reference, and we have seen how difficult it can be to balance candour, privacy defamation and information content in references.

TC faces a similar issue: how much information do I need to disclose about myself to prove trustworthiness on the one hand, how much can I blindly trust the reference on the other. As we saw, courts are willing (in some jurisdictions)

to make this trust actionable, and we suggest that analogous reasoning applies to TC. This leaves still much room to form policy based arguments on just how negligent the mistake must have been to trigger liability, for us the important part is to establish the principle. Just as in the reference cases, the legal network is now extended from employer-employee to the hiring parties, or anyone reading the reference, so would an application to TC extend the trust network beyond vendor and customer to the reliant party.

Trust, based on the observation of past performance was, as we saw in Chapter 2, one way to form rational trust. A very different approach is to predict trustworthiness on the basis of general principles or expertise. I can trust a bridge for instance even if I never saw it being used, if I can use general laws of physics to calculate what weight it should be able to bear. I don't need to know much about this specific bridge, but a lot about bridges, or physics, in general. I need with other words, abstract expert knowledge.

This is the second type of scenario where the issue of reliance liability can arise: trusting an expert because of his abstract knowledge, not (just) observation of the past of a specific object. In the offline world, this type of expertise can be found in many professions, accountants, engineers and medical experts being the most obvious.

A case in point is here *Candler v Crane, Christmas & Co*¹⁹⁷ where the plaintiff who wanted to invest into a specific company asked the company's accountants to verify the reliability and viability of the company and therefore make sure his investment would be a good deal. With the guidance of the accounts presented to him, he decided to move forward with his expenditure as all looked perfectly fine. The company collapsed and he sued the people on whose expertise he had relied – the company's accountants and auditors. In the courts, the judge found that the accounts have been indeed "defective and deficient" and that the accountants

¹⁹⁷ *Candler v. Crane Christmas & Co.*, 1 164 (K.B.2 1951). 2 KB 164

were negligent when preparing the accounts that led to the plaintiff's damage. In court the defendants stated that based on the contractual relation of their clients to the company, they only owed duty to them and nobody else. While the court of first instance and the court of appeal accepted this reasoning, it gave rise to an important and eventually successful dissent by Lord Denning.

Denning L.J, in the court appeal argued in his speech that there were two errors that affected the verdict; "The first error was (. . .) that no one who is not a party to a contract can sue on it or on anything arising out of it" and the second one "that no action ever lies for a negligent statement even though it is intended to be acted on by the plaintiff and is, in fact, acted on by him to his loss".¹⁹⁸ This led to the conclusion that a third person injured by the negligence of one of the two involved parties in the contract, could not sue for damages.

Contradicting the court's decision, Denning L.J. stated that persons whose professional knowledge and skills are to review books, accounts etc. and generate reports on which third parties can rely upon to make their business decisions, are having a duty of care towards those parties. Their duty is actually twofold: to carefully create their reports, and also to use care in their work resulting in these reports,¹⁹⁹ as they are possibly influencing third parties into investing into the business. Although his opinion has been rejected by the court of appeal, it has been adopted and relied upon by the House of Lords.²⁰⁰

In analogy with TC, we argue that the same rationale of Denning L.J.'s reasoning can be applied and therefore extend the duty of care of TC vendors not only to their clients, but also to any third party relying to the certification issued by them – as certification will be given only to those pc's who are following the standard that their professional knowledge and skills will depict. The main

¹⁹⁸ *ibid.* 2 KB 164

¹⁹⁹ *ibid.* 2 KB 164

²⁰⁰ *Caparo Industries Plc v. Dickman*, A.C.2 605 (House of Lords 1990), *Hedley Byrne & Co Ltd v. Heller & Partners Ltd*, A.C. 465 (House of Lords 1964).

questions discussed in *Candler v. Crane Christmas & Co* court appeal by Denning L.J. were basically the following:

1. "What persons are under such duty?"
2. "To whom do these professional people owe this duty?"
3. "To what transactions does the duty of care extend?"

Considering each one of the questions and discussion followed, we will try to show how it applies in the TC reliance liability case.

4.7.1 "What persons are under such duty?"

We argue that TC attestator should be considered as the equivalent to professionals that should owe a duty of care to any third party relying on the certification issued, that suffers harm. That process is done automatically and remotely and does raise the issue of liability for autonomous systems in distributed networks.²⁰¹ Given the deterministic nature of the attestation, which avoids the common objection against holding the owners of an autonomous system liable for mistakes by its agent, this should not be an obstacle. The TC attestator computes according to predefined rules (which in turn are certified by the TCG – the first setting above), it uses therefore knowledge and skills typical for a human expert. Indeed accountancy is one field where computer systems do

²⁰¹ see e.g. Karnow, C. E. (1996). Liability for distributed artificial intelligences. *Berkely Tech. LJ*, 11, pp. 147. See also Chopra, S., & White, L. F. (2011). *A legal theory for autonomous artificial agents*: University of Michigan Press, Koops, B.-J., Hildebrandt, M., & Jaquet-Chiffelle, D.-O. (2010). Bridging the accountability gap: Rights for new entities in the information society? *Minnesota Journal of Law, Science & Technology*, 11(2), pp. 497-561.

replace increasingly the human operator, bringing this example even closer to the facts of *Chandler v Crane*.²⁰²

4.7.2 "To whom do these professional people owe this duty?"

In his reasoning Denning L.J. discussed the extent to which the duty can be applied and stated that it should be limited to the extent to which it is reasonable for a third party to rely on the information provided by the professionals. If the relying party had information at its disposal that casts doubt on the judgment of the professionals, or could easily get hold of this information, the rational reliance would disappear and the tort claim would be extinguished. In the case of TC, this restriction might be moot. Decisions to communicate between computer systems have to be made instantaneously, one reason to automatize them, so we could never expect from the reliant party to carry out further investigations, or to use other information in their decision. Their computer recognizes the TC certification, and therefore trust the other computer, in all cases. Even more problematic is the indeterminate number of potentially relying parties. Denning in *Chandler v Crane* tried to develop a proximity test to prevent the problematic floodgate liability.²⁰³ In *Chandler*, the accountants communicated with one specific party, they knew who that party was and why it needed the information. That created a degree of proximity that went beyond e.g. writing a generally accessible article about their company, or putting their name on a glossy brochure. In the TC case, potentially the whole world can access the information,

²⁰² see in particular Sutton, S. G., Young, R., & McKenzie, P. (1995). An analysis of potential legal liability incurred through audit expert systems. *Intelligent Systems in Accounting, Finance and Management*, 4(3), pp. 191-204.

²⁰³ discussed by Cardozo C.J. in *Ultramares Corp. v. Touche*, 174 N.E., 255 N.Y. 170, 255 N.Y.S. 170 441 (NEW YORK 1931). who denied a liability that could expose the defendants and could not determinate in quantity, time and class.

making the TC attestation more similar to a “communication to the general public” that would be too ill defined to trigger reliance liability.

However three arguments can be used to counter this objection against extending Chandler to TC attestation. The first is that unlike the TMO discussed above, TC certification still is given on an “interaction by interaction” basis. So while TM’s might qualify as “general communication to the public”, TCs at least technically, are better understood as many 1:1 verifications between a requester of information and the certifier, bringing it closer to the facts of Chandler. Second, as the above cited case of the bookkeeper’s manual shows, courts have on occasions extended reliance liability also to publications to the general public, provided there was “rational” reliance due to the eminence of the source and the special role the publisher took on (there: on behalf of the bookkeepers association). This too applies in TC: the certificate is issued “on behalf of” the TCI group, which has taken on voluntarily the special role to ensure greater security. Finally, as we argued above, there is an argument that reliance liability can be extended even to TMs, and for them, the indeterminate number of people potentially relying on it, is a much more obvious problem.

4.7.3 “To what transactions does the duty of care extend?”

At this point we need to show to which transactions the duty of care of a TC attestator should extend. In our view this refers to the scope of use of the certificates and where these will be needed. In a nutshell, the duty of care should reach only the points which the certificate will reach. Of course, this can lead to an indeterminate liability as well, because the certification will be used for most – if not for all – of the transactions between a TC computer and any third party. It does not however lead to transitive liability. If A relies on my computer’s certificate, this certificate was unwarranted, and his computer is infected, and in turn infects C’s computer, then there should be no liability of my attestator to C – if on policy grounds only, to prevent everybody becoming responsible for

everything. This, admittedly, makes it more difficult to have the legal network of liability match the trust network which is strictly transitive. Here, however, a compromise between the logic of the computer and the logic of the law seems necessary.

Let us recap again: Trust is not only build on observation of past behavior, it can also be build on prediction of future behavior based on general laws known to experts. TC also has aspects of this type of expertise: it is build on formal modeling of possible future risks and threats, and incorporates knowledge about computer vulnerabilities in general. For this type of statements too, courts have been willing to impose liability. We discussed in some detail Chandler and the knowledge of accountants, and cited cases from aviation security and scientific publishing. Again the similarities to the TC attestation process seem strong enough to permit a direct analogous application, even though the “expert” in this case seems to be a computer program.

4.8 From examples to doctrine: Contractual liability on reliance

Having discussed specific examples, we now bring the discussion back to the general theory of reliance liability. According to Smith “*reliance* theories regard contractual obligations as being imposed by the law in order to ensure that those whom we induce to rely upon us are not made worse off as a consequence”.²⁰⁴ Although courts have been sometimes seeking for special relationship between parties or “relationship equivalent to contract”,²⁰⁵ there have been cases were this relationship equivalent was not so meaningful to be identified. Yet, the existence of a relationship, contributes to establish proximity. This fits well to our general framework of relational contract theory, that is sensitive to the particularities of the social interaction that surround and exchange.

²⁰⁴ Smith, S. A. (2004). *Contract theory*. Oxford: Oxford University Press.

²⁰⁵ Hedley Byrne & Co Ltd v. Heller & Partners Ltd, A.C. 465 (House of Lords 1964).

A discussion on the degree of knowledge on the defendant's side has been raised by the House of Lords in cases of third-party liability.²⁰⁶ This analysis further strengthens our claim on the duty of care for the TC certification to third parties, to the TC provider. As we argued, the information and power imbalance between TC and customers is particularly high, and the autonomy of the customer severely curtailed. The knowledge that the TC certificate – issued by the TC attestator when an upcoming connection to a third-party will rise – and the reliance that will follow it by any third-party, should also be taken into serious consideration by courts similar to the *Harris and Another v Wyre Forest District Council and Another* and *Smith v. Eric S Bush* cases.²⁰⁷ It is therefore not necessary for the third party to prove that his reliance and decision to undertake the TC vendor's professional activity was already known/ expected by them. We argue that it is fair, just and reasonable to place on the TC vendors *some* tortious duty of care towards any third-party, and also the duty of care should arise even in the absence of direct relations/affairs between the parties. Ultimately, this is in the benefit of all concerned: I as TC customer can trust TC not only that they will see me right, but also everybody in my network that relied on them. Third parties can act on a TC certificate, resulting in greater uptake and use of the technology. Extending liability regimes beyond the contractual parties creates thus network effects – the very reason why TC might be an answer to the thorny issue of Internet security.

²⁰⁶ *Harris and Another v Wyre Forest District Council and Another* W.L.R.2 1173, 1171 All E.R. 1691 (1 Q.B. 1988), *Smith v. Eric S Bush*, 1990 831 (A.C.1 1990).

²⁰⁷ *Harris and Another v Wyre Forest District Council and Another* W.L.R.2 1173, 1171 All E.R. 1691 (1 Q.B. 1988), *Smith v. Eric S Bush*, 1990 831 (A.C.1 1990).

CHAPTER 5 :

CONCLUSIONS

5.1 Conclusions

Throughout this thesis we have explored different issues enacting from the adverse of the Internet, the need for technological systems to ensure security for the user, and the implications that these technologies bring with them. As a case study/ example of regulation through code we have used the technology of Trusted Computing mainly because it is a paradigmatic solution and a highly plausible answer to various threats like cybercrime. Although this was one of its initial aims, we have explained why it failed to achieve the crucial economy of scale and the network effect that would indeed have made this technology a radical game changer.¹ The TC as a technological advancement would have meant a significant change in the way users relate to their machines, and amongst them in the digital era we live in.

However, TC has been treated as a mere technical fix, the wider societal implications of TC were ignored, and as a result the social and socio-legal environment were inappropriately prepared for such an approach. We have then explored the different roles that law can play under the circumstances. TC providers could be exposed with new and difficult to quantify litigation risks, thus hindering the development of TC, or it could fail to protect the reasonable expectation of TC consumers to have remedies in case TC causes them harm. On the other hand, it could promote TC by matching the technological concept of trust (“techno-trust”) with the legal or socio-legal concept of trust. Then it would be easier for the user that “trusts” a computer system and the legal system

¹ Chapter 1, Section 1.1

rewards this trust by protecting the reliance on this system through appropriate remedies, to accept the shortcomings associated with TC.

As we have showed in this thesis, this “matching” or “isomorphism” between technical and legal understandings of trust was never really developed or made fully explicit and this led to the limited success of TC. The thesis focused primarily on the conceptual clarification of the differences in the way in which computer scientists, psychologists and sociologists understand the term “trust”. We then argued that systemic features of the TC philosophy did not help to diffuse public trust in their product, as it inevitably creates legal issues, since beneath the technical aspects we identify fundamental legal and jurisprudential issues, for which the current legal system seems ill prepared. TC is based on the “scale free” trust and self-organizing trust networks and these issues that emerge, deter the “scale free law” of succeeding and leave the law on the back burner.

Further we have identified the related legal issues that are likely to emerge with the new applications of TC i.e. cloud computing, virtualizations and the Internet of Things and the demands that autonomous, flexible and decomposable systems bring along.² But as law is left behind, so is one of the major instruments for governments to instill social acceptance and *public* trust in institutions, as opposed to *personal* trust between individuals. TC could be based on individual trust relations merely because it is a computing network, however the core

² See e.g. Gessner, D., Olivereau, A., Segura, A. S., & Serbanati, A. (2012, 25-27 June 2012). *Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things*. Paper presented at the Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 998-1003), IEEE, Ukil, A., Sen, J., & Koilakonda, S. (2011, 4-5 March 2011). *Embedded security for Internet of Things*. Paper presented at the Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on (pp. 1-6), IEEE. Skeptical on the usefulness of TC for the IoT is Hoepman, J.-H. (2012). In *Things We Trust? Towards Trustability in the Internet of Things*. In R. Wichert, K. Van Laerhoven & J. Gelissen (Eds.), *Constructing Ambient Intelligence* (Vol. 277, pp. 287-295): Springer Berlin Heidelberg.

implementation of it, is crucially dependent on public trust in the TCG as an institution. This nexus between public and personal trust generates most of the arising most pressing conceptual issues.

5.1.1 TCG as an Internet Security provider

This thesis uses TCG as an ideal type of institution that is obliged to provide Internet security, and as such we contrast it to approaches that try to ensure Internet security through the state - as a core provision of the state towards citizens. Similarly, we treat TC as the security paradigm promoted as an entire suite of programming and development approaches to Internet security, and as such it has to reach the equilibrium in conflicting demands, including privacy, costs, security, user autonomy and transparency. For the purposes of this thesis TC is used as an example also because it proposes a very specific mix of these characteristics with different degree of emphasis in each one of them. As we have argued, although Trusted computing tries to make the Internet more secure, it is not what is technically known as “*secure computing*” where a machine will never do anything else but what is expected of it.³ On the contrary, TC is based on inductive inferences where if a machine seems to perform as intended, and had the same constant behavior is *trusted*. *Trustworthy* is a judgment that can be extrapolated from the past and present observed behaviors to the future.⁴ We noted that “trusted” in the computer sense only partially matches the concept of “trustworthiness” as understood in social life: “trusted” is what the technology gives us, “trustworthy” is what we want.

Here we researched the new dilemma that occurs – the one that every technological solution to computer vulnerabilities faces: secure computing is

³ Proudler, G., Chen, Liqun, Dalton, Chris. (2014). *Trusted Computing Platforms: TPM2.0 in Context* (1 ed.): Springer International Publishing. p. 9ff.

⁴ We assume Proudler means that behavior is trustworthy if it is predictably benevolent.

significantly costly and therefore cannot be afforded by simple public users. As a countersolution, trusted computing is cost-neutral and if benefited from the economies of scale, it could eventually deliver higher degree of protection at viable costs.⁵ But this dilemma introduces to two main questions for this thesis to explore: The legal one of liability and the techno-legal one of “risk compensation”. The first emerges because TC is a less-than-perfect solution to the security challenge, it is nonetheless increasing the costs of computing, and therefore consumers will only buy TC protected computers if they think that their investment will be a winning one by receiving increased security.⁶ Then the advertising group will extol the virtues of TC emphasizing the offered protection, and the legal department will add as many liability exclusion clauses into the contract with the customer as possible to protect their own company.⁷ But in this scenario consumers are left in ambiguity since they believe they invest in actual security systems, and not just a “trusted” system. We have argued that TC brings a significant shift of power away from the customers to the industry. The problem

⁵ Ibid. p.9

⁶ On the problem of cost benefit analysis in Internet security , see Anderson, R. (2001). *Why information security is hard - an economic perspective*. Paper presented at the Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual (pp. 358-365),IEEE. Particularly relevant for the point here his attempt to include psychological analysis of consumer behaviour in Anderson, R., & Moore, T. (2009). *Information security: where computer science, economics and psychology meet* (Vol. 367). On the empirical basis for making rational decisions on security investment see also Gordon, L., & Loeb, M. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, 8(5), pp. 335-337. doi: 10.1007/s10796-006-9010-7; This issue affects not only consumers, but also companies and public sector entities, see e.g. Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, 24(1), pp. 37-59. doi: <http://dx.doi.org/10.1016/j.jaccpubpol.2004.12.003>.

⁷ On this problem see the hart-hitting presentation by Virvilis, N. (2015). *Advanced Persistent Threats: The Empire Strikes Back!* , pp. 16-19.

becomes even worse if we consider the different understandings that consumers have for the everyday notion of “trusted” and the notion of “trustworthiness”.

The second emerges since the customer wrongly estimates that he is safe, as he paid for a secure system, he may engage in a more risky behavior and this is the so called “risk compensation problem”. This also poses a potential issue for legal regulation and an issue that this thesis tried to explore. In particular, we tried to walk around the issue that lies in the interface of law and technology which arises from the need for cybersecurity solutions based on certified trustworthiness. Cybersecurity technology solutions, have been in the center of attention in an effort to apply regulation through code, thus making it impossible to commit crime in the first place.⁸ TC which is used as an example throughout this thesis, is a security solution which has evolved from the need to address issues like data exposure on systems, system compromise as part of software attack and prevention of identity theft to mitigate the risks and dangers; and help to increase data management and identity security.

5.1.2 TC and regulation

Furthermore, in Chapter 4, we saw the fundamental issue lying underneath the contract law, which is if *any* classical, liberal contract law can provide the type of relation that is needed for TC to create the networks of security and trust that they intent. As it is well known, contracts cannot be dynamic, or complex because they are lacking transitivity.

⁸ See also Lessig, L. (1996). The Zones of Cyberspace. *Stanford Law Review*, 48(5), pp. 1403-1411. , Pagallo, U. (2015). Good onlife governance: On law, spontaneous orders, and design *The Onlife Manifesto* (pp. 161-177): Springer, Yeung, K. (2008). Towards an Understanding of Regulation by Design. In K. Yeung (Ed.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 79-108). Oxford: Hart, Yeung, K., & Dixon-Woods, M. (2010). Design-based regulation and patient safety: a regulatory studies perspective. *Social Science & Medicine*, 71(3), pp. 502-509.

Next, the thesis expanded on how TC tries to build complex dynamic trust networks “bottom up”, without central, let alone state, oversight or control. Through our analysis we also encounter the specific reasons that make TC as promoted by the TCG insufficient, in the absence of positively enabling legislative interference. Proudler et al’s analysis is used in particular to collate why TC has been rejected by the audience, which in our view perceived this technology as a power grab under the pretense of enhanced security.⁹

Guadamuz indicates that complex and dynamic security networks that can self-organise are essential for efficient Internet regulation,¹⁰ and we believe that this can only be achieved if we have a mix of at least a certain degree of social trust along with techno-trust. We then explained that TC delivers only techno-trust that falls short of what is needed, and creates two separate but causally connected issues for law and regulation. First, it causes potentially legal problems for users and wider society, problems that the law may need to rectify. Second, to achieve its aims it needs a more sympathetic regulatory framework that gives consumers better reasons to invest in TC. The two issues are connected: As long as potential users feel that TC exposes them to technical risks without legal redress, or legal risks without giving them the control to mitigate these risks, they will refrain from investing into the TCI model.

This thesis has also visited other issues that may occur from TC and its feature to approve with which technologies it accepts to communicate. This in our view is a monopoly position to force products and solutions on unwilling users, and competitors’ open source products are excluded from this synergy.

It has also been proved that social capital is lacking to marshal social trust, and TCG buyers reject the business proposition. According to Max Weber, people

⁹ Proudler, G., Chen, L., & Dalton, C. (2014). Futures for Trusted Computing *Trusted Computing Platforms* (pp. 21-36): Springer International Publishing. p.2.

¹⁰ Guadamuz, A. (2011). *Networks, Complexity and Internet Regulation: Scale-free Law*: Edward Elgar Pub.

should learn to trust in laws, and the bureaucracies that enforce them, rather than trusting the individual. This in turn requires trust in systems of law and administration, rather than people (or companies). We argue that TCG relied exclusively on market and network driven solutions insufficiently and the institutional-legal framework along with the pre-existing social trust rejected the model. “Metagovernance” for networks and markets has also been explored as a solution to the problem arising, and we identify two of the points that such a solution will need to address.

We even argue that it’s not just the trust relation towards a particular institution (i.e. TCI) that is the issue, rather, holistic trust in the form of a network where everybody is connected with and trusting in, everybody else is at stake. In our opinion “trust in institutions” is insufficient, and it also needs a high injection of pre-existing trust. We therefore argue that we need the right type of law, which “follows” and “enhances” transitive and dynamic network foundations.

Reliance liability is the exact type of private law we need to transform intransitive contract relations to transitive, and network-supporting ones. Relation contract theory is used to allow us to redraw the image of contract binary, static and atomistic relations.¹¹

To achieve higher levels of security, control is taken away from users and is remotely managed by trusted third parties. In Chapter 2, we have identified some of the legal problems this may cause, the regulatory alternatives that

¹¹ For an introduction to relational contract theory, see Gudel, P. J. (1998). Relational Contract Theory and the Concept of Exchange [comments] (pp. 763). For a comprehensive discussion that focuses on the economic exchange relation and its role in sociology discussed here see in particular Macneil, I. R. (1987). Relational Contract Theory as Sociology: A Reply to Professors Lindenberg and de Vos. *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft*(2), pp. 272-290. An important critical voice to which we will have to return is Fox Jr, J. W. (2003). RELATIONAL CONTRACT THEORY AND DEMOCRATIC CITIZENSHIP. *Case Western Reserve Law Review*, 54(1), pp. 1-67.

governments are facing, and their respective inadequacies. Mainly we have explored the radical legal issues of who should be appointed to minimize the harm, together with the rights and authority that comes with such a role, and if he should be held legally liable if harm occurs. The answers then lead to a larger issue, the one of reliance liability, which is a relation outside the contractual nexus. We believe that TC vendors should be held liable when a third party relying on the trusted certification they have issued, suffer losses. To make our point clearer, we used the regulation of electronic signatures under the Electronic Signatures Directive.¹² Most importantly, we stress the point that even in the absence of TC, governments in their efforts to improve the security of the Internet should use regulatory options for a possibility to impose delictual liability on software developers for security risks in their products (even outside the contractual nexus with their customers).

We explored and criticized the different regulatory strategies identified by the House of Lords' report,¹³ one of them is holding the private sector and the software industry responsible for the security of the Internet backed by legal sanctions. As this option has the major drawback - that it can scare software vendors and the private sector and deter them from creating secure systems and then face legal liability - efforts to reduce crime through architecture have risen.¹⁴

¹² Balboni, P. (2004). Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication. *Information & Communications Technology Law*, 13(3), pp. 211-242. doi: 10.1080/1360083042000219074

¹³ House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm>.

¹⁴ For a recent analysis of the state of the art in offline crime reduction through design, see Crowe, T. D. (2000). *Crime prevention through environmental design : applications of architectural design and space management concepts* (Second edition.. ed.). Boston, Mass.: Boston, Mass. : Butterworth-Heinemann.; For a cyberspace specific analysis

While technology has in recent years pushed crime prevention into the forefront of public debate, it is important to remember that first, these methods long predate modern ICT,¹⁵ and second post-crime analysis and investigation remains as important as ever.

TC is an architecture-based proactive crime control and through our research we show that while technology has been an enabling factor for greater involvement of the private sector in policing functions, reactive cybercrime investigations should also use private sector participants.¹⁶ We argue that TC's move in the field of crime investigation and computer forensics is inevitable, and TC as a technology is a perfect fit to assign state roles to the private sector guaranteeing or certifying Internet safety both for pre-crime protection and prevention, and post-crime investigation. In our view, by extending the demands that were strictly related to the police force, to TC providers, TC providers will be considered as a de-facto police force. This, we contest, wakes potentially more rights, but also more duties which promote social trust.

Due to TC's origins in DRM and its support by major IP rightholders, this thesis revealed the important problem that TC faces, where according to Shearing and Stenning on the privatization of policing "private police" and "property owner" become one and the same person, at least for some crimes and delicts.¹⁷ We note that while increased use of criminal law to act against copyright

see Katyal, N. K. (2003). Digital Architecture as Crime Control. *The Yale Law Journal*, 112(8), pp. 2261-2289. doi: 10.2307/3657476.

¹⁵ For an overview of early architecture-driven crime control offline, see Jeffery, C. R. (1977). *Crime prevention through environmental design*: Sage Publications Beverly Hills.

¹⁶ See e.g. Phillips, A., & Nance, K. L. (2010). *Computer Forensics Investigators or Private Investigators: Who Is Investigating the Drive?* Paper presented at the Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on (pp. 150-157), IEEE.

¹⁷ Shearing, C. D., & Stenning, P. C. (1981). Modern Private Security: Its Growth and Implications. *Crime and Justice*, 3, pp. 193-245.

violations is a general trend, it includes outsourcing of preventative and investigative policing to private sector actors, which in the case of TCI are also major IP right holders that used in the past technologies that were suggested for general online security.

5.1.3 TC and digital forensics

This thesis discussed that while TC providers will inevitably be involved in post-crime investigations, the same measures that protect a computer from criminals can be also used to protect them against legitimate police investigation methods, like remote forensic analysis. This shows the necessity to think of an appropriate legal environment that can address the concerns regarding rule of law, justice and individual liberty; and on the other hand reveals the paradox of whether it is desirable for the TC to provide the purported level of security from attacks. Using examples and analogies that added significant value to our research argument structure, we tried to answer critical questions regarding the issues that TC will probably face if seen as a privatized police function. Issues like circumvention of legal rules aimed for protecting citizens from the state, and the level of responsibilities that we impose on TC in exchange with the great powers it wields were in depth investigated. With such great powers, great responsibility should come, with a role for the law to address the arising ethical concerns and rebalance the interplay of power and responsibility. In short, governments (and citizens) should accept this power shift and its consequences only if a corresponding *increase* of responsibility occurs in the side of the TC provider.

Through our literature review, we have showed that unsophisticated users are the weakest link in the effort of making the Internet more secure against cyber attacks. An obvious solution to the problems arising from their inability which may also affect third-parties through botnets and DoS attacks, is to remove the responsibility of maintaining the security for the user's own computer from him, and assign it to a third party. Interesting legal issues then emerge for the

employees of these third parties, one of them being what his responsibility is, if incriminating material is located on a user's pc. The contractual relation between the user and the third party company should be one relying on trust, and for anyone to access the user's pc, the explicit consent of him should be granted.

DRM as heritage of TC is also discussed, in terms of the power given to TC providers and the knowledge on the content of the user's computer, since it seems that the information obtained from the user's computer is not gathered only to prevent unauthorized programs from running, but also for removing programs remotely. This, as we have depicted, raises – amongst others – legal, privacy and forensics investigations concerns. For us, this is one more argument why it might be desirable to create a *sui generis* framework for TC providers that recognizes that monitoring, analyzing and to a degree retaining data about suspicious activities is their very reason for existence.

To create further responsibility for TC developers, they could potentially be obliged to compromise their own product under certain circumstances. However, decisions would have to be taken on the degree of judicial oversight and warrant requirements towards TC providers. We note that balancing the legal obligations, privileges, immunities and burdens in an equitable way for both consumers and software vendors, requires much more complex legal responses from those envisaged by the House of Lords.¹⁸ Further, the type of knowledge required by various criminal offences and the amount of actual knowledge TC providers could or should have about the content of their customers' hard drive, are discussed as arguments. In our analysis we noted that special privileges may have to be created by law - possibly similar to the ones of ISSPs or even new tailor made exemptions - to exempt TC providers from an overly onerous reporting

¹⁸ House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldscstech/165/16502.htm>.

requirement, which may designate them as a surveillance authority on behalf of the state, potentially creating a dispute with their customers. We also explored a new perspective and parallelized TC with other professions that provide security functions and how law is dealing with them.

Although TCI can be seen a police force, as we have showed in Chapter 3, in the eyes of the law, it still remains under the private law sector, and the direct relation with its customers is mediated through contract law. Importantly enough, we explored why traditional contract law alone is insufficient to mediate TC, since we showed in detail that the very nature of contract poses a fundamental issue. Since TC relies on networks, which inherently requires transitive relations where everybody is connected to everybody, and everybody is affected by everybody, traditional contract law and the atomistic binary relation that it carries, is inadequate. We propose that “relational contract theory” is much more appropriate to regulate contracts in TC and we suggest using the concept of “reliance liability” as a cornerstone of TC regulation through private law as it introduces third parties into the emerging trust network.

5.2 Research significance

The research significance of this thesis arises from our attempt to “parallel read” the technical aspects of TC and the sociological reflection on the interaction between trust and law. We gave an in depth analysis of trust’s significance in sociology and how it relates to technology and the law feeding the discussion with important contributions from existing theories. Network complexity is an obstacle for Internet regulation, and through this thesis we state that if social trust relations in complex modern societies are self-organizing in dynamic complex networks, and if security “travels along” the trust nodes of this network, then the result will be an environment with ubiquitous security – the ultimate goal of TCI. According to our analysis this can raise several sociological problems and we researched each one of them. In particular, the first question is if social

trust networks are self-organizing, complex dynamic systems and if “security” in these systems follows trust. The relation between the two concepts of trust then comes into play and we tried to answer the question if the network effects that TC aimed to create, despite the different perceptions of trust, are isomorphic to the trust networks which exist in society. However, since the answer is not affirmative, we explained in detail the reasons we have to doubt all three premises, at least to a degree.

Law is the only mode of regulation that can play a crucial role in settling the issues that occur. According to Lessig and the four modes of the square of regulation, described in Chapter 2, we elucidated that TC follows just two of those modes. Using ideas from Max Weber and his analysis of the role of formal law in modern, market driven societies, we attempted to show that the TC network will only work when security and techno-trust are packed along with legally enabled social trust that follows the connected nodes of the network creating an emergent “web of trust”.¹⁹ Only then we will be able to achieve dynamic complex networks that are isomorphic to the communication network of the Internet, however we argue that this is a difficult proposition to achieve and list the systematic problems that arise with the very concept of law.

But even when we try to classify Trusted computing as a commercial product to identify the legal system that we should follow, the distinction is not clear – is it a service, hardware or software? TC tries to offer security, which is obviously the union of these three. Concerning law however, each of these categories is treated differently, and therefore is not suitable to handle this type of interdependent entity as we argue.

In Chapter 3, we argued that TC is best understood as privatization of centralized government functions, not a decentralized, emergent network governed by free contractual association only. Next, we contented that making

¹⁹ Lessig, L. (1999). *Code and other laws of cyberspace*: Basic books. esp. p.83ff

the TCI act as police, prosecution and jury all in one, creates a significant imbalance in procedural law and evidence, which can be resolved with regulation through law between customers and the TC provider.

Trusted computing is used throughout this thesis to discuss the *type* of response to cyber crime and this is the main interest of this manuscript. Our discussions stress the point that while TC offers “pre-crime” features, it is also relevant for post-crime and crime investigation purposes. More significantly we argue that if the trustworthiness of the Internet can be increased through technological rather than legal solutions, taking TC as such a solution, then the provider of such security will inevitably need access to the user’s hard drives and will be able to alter and reconfigure software on the machine. In a forensic context, TC features can give the computer evidence a much higher evidential value, since these deter the owner or any malicious third party from altering certain configurations. At the same time, a backdoor is left open, for alterations done by the TC provider who is certified as a trusted third party. Returning back to our initial argument, we believe that this requires significant amount of trust in the sociological sense and which we argue that TCI is unlikely to enact.

In our view, it is necessary to create a legal duty on TC providers to ensure that data integrity cannot be tampered by any employee for evidential purposes. Further, TC providers could be required to develop protocols with the explicit requirement of legal admissibility highlighting the privacy issues that TC raises. Thus, we approached the legal environment around TC from a public (criminal law) perspective and we answered critical questions like what the state or society can legitimately demand from TC providers, what rights can they be given, what obligations should they be under.

Importantly enough, we have identified that TC has not been given much attention from courts or governments, and this thesis along with the journal articles the author has published on the same area, aim to give at least a beginning of an academic debate on that issue. Computer scientists seem primarily

concerned with the technical feasibility of implementing TC, legal academics have concentrated on content control and privacy issues,²⁰ thus leaving the analysis of the implications of the imposition of legal liability in case of failure within a TC system, or potential responsibility for wider social and legal concerns, unexplored.

5.3 Future research

Due to the low uptake of TC, as acknowledged by the TCG themselves, it was difficult to test some of the conceptual claims of this thesis through empirical

-
- ²⁰ Anderson, R. (2003a). Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA – Version 1.1. (2003). <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>, Anderson, R. (2004). Cryptography and Competition Policy - Issues with 'Trusted Computing' *Economics of Information Security* (Vol. 12, pp. 35-52): Springer US, Bradgate, R. (1999). Beyond the Millennium - The Legal Issues: Sale of Goods Issues and the Millennium Bug. *The Journal of Information, Law and Technology (JILT)*, 2, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_1992/bradgate/, Chandler, A. J. (2003). Security in Cyberspace: Combatting Distributed Denial of Service Attacks. *University of Ottawa Law and Technology Journal*, 1(1-2), pp. 231-261., Charlesworth, A. (2005). DRM: the Straw to Break of Procrustean Approaches to Copyright? In F. Grosheide & J. J. Brinkhof (Eds.), *Intellectual Property 2004: Articles on Crossing Borders between traditional and actual (Molengrafica Series)* (pp. 405-422): Intersentia, Erickson, J. S. (2003). Fair use, DRM, and Trusted Computing. *Communications of the ACM*, 46(4), pp. 34-39., Hilley, S. (2004). Trusted computing - path to security or road to servitude? *Network Security*, 2004(8), pp. 12-15., Pearson, S. (2005, 23-26 May 2006). *Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy*. Paper presented at the Proceedings of the Trust Management: Third International Conference, iTrust 2005, Paris, France (pp. 305-320), Springer-Verlag GmbH, Reid, J., Gonzalez Nieto, J., Dawson, E., Okamoto, E. (2003). *Privacy and Trusted Computing*. Paper presented at the Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03) (2003), Washington (pp. 383-388), IEEE, Samuelson, P. (2003). DRM {and, or vs.} the Law. *Communications of the ACM*, 46(4), pp. 41-45., Turner, M., Budgen, D., Brereton, P. (2003). Turning software into a service. *Computer -- IEEE Computer Society*, 36(10), pp. 38- 44., Woodford, C. (2004). Trusted Computing or Big Brother? Putting the Rights back to Digital Rights Management. *U. Colo. L. Rev.*, 75, pp. 253-300.

research. In particular, there isn't yet a clear, discernible trend on how EULAs in this area will finally look like, and just how burdensome on the buyer they will be. Monitoring this situation, and incorporating a more substantive corpus analysis of contract terms and EULAs would be a logical next step to test empirically some of the theories put forward in this thesis.

The empirical study tried to establish in particular how computer scientists "make sense" of the law, how they match what they know intimately, and what they are doing, to how they understand the law operates. It was not possible to carry out a corresponding study on how practicing lawyers conceptualize TC - a study of the thinking of in-house law departments in large TC companies would be needed for that, which raises obvious methodological problems of access and confidentiality, but also "trustworthiness" of the answers, that would be given with possible future litigation in mind.

A second major development that took place during the work on this thesis was the emergence of the Internet of Things. This in many ways magnifies some of the issues discussed in this thesis. The human loses even more control (depersonalization)²¹, is even more taken out of the equation, and the power shift to the software developers becomes even more complete. Networks that combine in addition to hundreds of millions of connections between desktops or similar devices will become networks of hundreds of billions of entities, increasing exponentially in complexity. Security becomes as a result also an even more interdependent network of strong and weak links - an attack on a badly protected thermostat could follow down communication lines to entirely different computer systems. At the same time, vulnerabilities become even more threatening - hacking into my computer to steal credit card details or spam people in my address book is one thing, hacking into my car while I'm driving and disabling the brake system is a very different threat scenario. Leaving it to human

²¹ Schneier, B. Security in 2020. CryptoGram, Jan. 2011.

consumers to ensure the security of these new networks seems even less a proposition than it was on the Internet. Customers who forget to update their anti-virus system, despite frequent pop ups, are not likely to ensure that the connection between their freezer and their house thermostat are secure - or indeed would know how to do this. They have to trust even more their systems. As a consequence, trusted computing as a security paradigm could get a new lease of life, or as an industry insider said, we need “trusted computing of acid”.²² If our conceptual approach is valid, this increasing dependency, coupled with a loss of power, and the way in which IoT applications are going to be embedded in our daily lives as long-lasting commitments, should further push courts and legislators to use both public law regulation and civil liability rules as tools to protect customers of TC and address the necessarily widening power imbalance.

Another significant technology for the Internet is Blockchain which is a reliable strong cryptographic technology underlying bitcoins²³ - a new open and decentralized system resembling the bottom up network formation that TC tries to accomplish creating a chain of assurances about data. Blockchain does not reside on a single server, but like TC it is found on a distributed network of computers. The similarity of Blockchain with TC can be identified on the network formation by TC pc's when each TC pc certifies that another pc can be trusted and connected. In the same way a distributed authentication exists where each valid transaction in Blockchain is timestamped and then is added into a block which is then linked to the other blocks created thus forming a trusted chain. TC as we have argued in Chapter 2, was seen as a possible solution to the problem of trust

²² so an industry speaker at a Dagstuhl seminar on security in the IoT, under Chatham house rules

²³ See The Economist. (2015). Blockchains: The great chain of being sure about things. *The trust machine*. The concept was invented in 2008 as the basis for renegade online currency, bitcoin. In this context, the blockchain is a digital ledger that records every bitcoin transaction that has ever occurred. See Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

between machines and users, and Blockchain is another way in which strangers who have never met or trust each other can create networks of trust²⁴. Along with the original idea of using Blockchain systems and zero knowledge proofs to cryptographically argue on the properties of encrypted data without decrypting the data, ensuring the privacy of the transaction data is another goal to be achieved.²⁵ The similarities between Blockchains and TC technology should be further explored and we believe that eventually each technology will be able to benefit from the other.

²⁴ Based on the decentralised nature of blockchains and the limited possibility of malicious infections, they have been described as “trustless” because the need for trust between participants is no longer required

²⁵ Allison, I. (2016). Blockchains, banks and zero-knowledge proofs, *International Business Times*. Retrieved from <http://www.ibtimes.co.uk/blockchains-banks-zero-knowledge-proofs-1565764>

BIBLIOGRAPHY

CASES AND STATUTES/LAWS/DIRECTIVES LIST

- 18 U.S. Code § 2709 - Counterintelligence access to telephone toll and transactional records (1986).
- Akins v. Estes, 888 35 (S.W.2d 1994).
- Anti-terrorism, Crime and Security Act 2001 c. 24 § c. 24 (2001).
- Beta Computers (Europe) Ltd v. Adobe Systems (Europe) Ltd, 1996 367, 1996 S.L.T. 1604 (1996).
- Candler v. Crane Christmas & Co., 1 164 (K.B.2 1951).
- Caparo Industries Plc v. Dickman, A.C.2 605 (House of Lords 1990).
- Communications Decency Act of 1996, , Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996) C.F.R. (1996).
- Cm7234. (2007). *The Government reply to the fifth report from the House of Lords Science and Technology committee*. London: The Stationery Office Limited.
- Cm7642. (2009). *Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space*. London: The Stationery Office Limited.
- Cm7669. (2009). *A Better Deal for Consumers - Delivering Real Help Now and Change for the Future*. (ID 6192113 07/09). London: The Stationery Office.
- Cm7948. (2010). *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. London: The Stationery Office Limited.
- Cm7953. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: The Stationery Office Limited Retrieved from http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy.
- Cohen v. Wales, 133 A.D.2d 94, 518 N.Y.S.512d 633 (Supreme Court of the State of New York 1987).
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108 C.F.R. (1985).
- Criminal Code (Strafgesetzbuch, StGB) § 138 (1998).
- Daubert v. Merrell Dow Pharmaceuticals, Inc, No. No. 92-102, 509 U.S. 579 (Supreme Court 1993).
- Desautels, E. (2005). *Software license agreements: Ignore at your own risk*. End-User License Agreements: Security and Privacy Implications.
- The Digital Millennium Copyright Act of 1998 (1998).
- Donoghue v Stevenson 562 (A.C. 1932).
- Downing, E. (2011). *Cyber Security – A new national programme*. (SN/SC/5832). House of Commons Library.

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 43 C.F.R. (2000).
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995).
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (2000).
- Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (2005).
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (2006).
- Gutzan v. Altair Airlines, Inc., 766 F.2d 135 (United States Court of Appeals 1985).
- Harris and Another v Wyre Forest District Council and Another W.L.R.2 1173, 1171 All E.R. 1691 (1 Q.B. 1988).
- Hedley Byrne & Co Ltd v. Heller & Partners Ltd, A.C. 465 (House of Lords 1964).
- Hill v. Chief Constable of Yorkshire, 1988 238 (A.C. 53 1988).
- House of Lords Publications. (2007). *Personal Internet Security*. (HL Paper 165-I). London: The Stationery Office Limited Retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm>.
- IND. CODE ANN., Information Maintained by the Office of Code Revision Indiana Legislative Services Agency § 22-6-3-1 (1994).
- Office of Cyber Security and Information Assurance (OCSIA), & Detica. (2011). *The Cost of Cyber Crime*. Cabinet Office and Detica Retrieved from <http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime>.
- The Police and Criminal Evidence Act 1984, c.69 C.F.R. § Part VII - Evidence from computer records (1984).
- Petry v. Cosmopolitan Spa Intern., Inc, 641 S.W.2d 202 (Tenn: Court of Appeals, Eastern Section 1982).
- Randi v. Muroc Joint Unified School Dist. 1066, 1929 P.1062d 1582, 1060 Cal. Rptr. 1062d 1263 (14 Cal. 4th 1997).
- Restatement (Second) of Agency, § 213(b) (1958).
- Restatement (Second) of Agency, §311, NEGLIGENT MISREPRESENTATION INVOLVING RISK OF PHYSICAL HARM (1977a).
- Sale and Supply of Goods Act § c.35 (1994).
- Sale of Goods Act § c.54 (1979).

- Salvage Association v. CAP Financial Services Ltd, 1995 654 (1995).
 Saphena Computing Ltd v. Allied Collection Agencies Ltd, 1995 616 (F.S.R. 1995).
 Smith v. Eric S Bush, 1990 831 (A.C.1 1990).
 St Albans City and District Council v. International Computers Ltd, No. 1997-98,
 1996 481, 1995 F.S.R. 1686 (All E.R.4 1996).
 The Electronic Signatures Regulations 2002 (2002).
 Evidence in criminal proceedings:hearsay and related topics ; a consultation
 paper (1995).
 Ultramares Corp. v. Touche, 174 N.E., 255 N.Y. 170, 255 N.Y.S. 170 441 (NEW
 YORK 1931).
 US v. Cartier, No. No. 07-3222, 543 442 (Court of Appeals, 8th Circuit 2008).
 Wages, Hours and Dismissal Rights § 290.140, 3020 Stat. (1909).
 Youth Justice and Criminal Evidence Act 1999 c.23 § c. 27 (1999).

REFERENCE LIST

- Ab Manan, J.-L., Mubarak, M. F., Isa, M. A. M., & Khattak, Z. A. (2011). Security, Trust and Privacy–A New Direction for Pervasive Computing. *Information Security*, pp. 56-60.
- Abel, W., & Schafer, B. (2009). The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems - a case report on BVerfG, NJW 2008, 822. *SCRIPTed*, 6(1), pp. 106-123. doi: 10.2966/scrip.060109.106
- ACPO E-Crime Working Group, & Metropolitan Police Service. (2007). Good Practice Guide for Computer-Based Electronic Evidence *Official release version*.
- Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification*. Paper presented at the Proceedings of the 5th ACM conference on Electronic commerce (pp. 21-29),ACM.
- Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, pp. 94.
- Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy. *Digital Privacy: Theory, Technologies and Practices*, pp. 363-377.
- Adams, J. N., & Brownsword, R. (1993). Privity of Contract. That Pestilential Nuisance. *The Modern Law Review*, 56(5), pp. 722-732. doi: 10.2307/1096875
- Adams, S. A., & de Bont, A. A. (2007). More than just a mouse click: research into work practices behind the assignment of medical trust marks on the World Wide Web. *international journal of medical informatics*, 76, pp. S14-S20.

- Adler, R. S., & Peirce, E. R. (1996). Encouraging Employers to Abandon Their No Comment Policies Regarding Job References: A Reform Proposal [article] (pp. 1381).
- Africa, M. (2000). The Misuse of Licensing Evidence in Fair Use Analysis: New Technologies, New Markets, and the Courts. *California Law Review*, pp. 1145-1183.
- Aiken, K. D., Liu, B. S., Mackoy, R. D., & Osland, G. E. (2004). Building internet trust: signalling through trustmarks. *International Journal of Internet Marketing and Advertising*, 1(3), pp. 251-267.
- Akdeniz, Y., & Walker, C. (1998). UK Government policy on encryption: trust is the key. *JCL*, 3, pp. 110.
- Allen, T. (1995). Liability for References: The House of Lords and *Spring v Guardian Assurance*. *The Modern Law Review*, 58(4), pp. 553-560. doi: 10.1111/j.1468-2230.1995.tb02031.x
- Allen, T., & Widdison, R. (1996). Can computers make contracts. *Harv. JL & Tech.*, 9, pp. 25.
- Allison, I. (2016). Blockchains, banks and zero-knowledge proofs, *International Business Times*. Retrieved from <http://www.ibtimes.co.uk/blockchains-banks-zero-knowledge-proofs-1565764>
- Alpcan, T., & Başar, T. (2010). *Network security: A decision and game-theoretic approach*: Cambridge University Press.
- AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). *Cloud Computing Security: From Single to Multi-clouds*. Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on (pp. 5490-5499),IEEE.
- American Institute of Certified Public Accountants Inc., & Canadian Institute of Chartered Accountants. (2006). Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (Including WebTrust® and SysTrust®) *Trust Services Principles, Criteria, and Illustrations* (pp. 155).
- Anderson, R. (2001). *Why information security is hard - an economic perspective*. Paper presented at the Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual (pp. 358-365),IEEE.
- Anderson, R. (2003a). Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA - Version 1.1. (2003). <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>
- Anderson, R. (2003b). 'Trusted Computing' and Competition Policy - Issues for Computing Professionals. *Open Knowledge*, pp. 35.
- Anderson, R. (2004). Cryptography and Competition Policy - Issues with 'Trusted Computing' *Economics of Information Security* (Vol. 12, pp. 35-52): Springer US.
- Anderson, R., & Moore, T. (2009). *Information security: where computer science, economics and psychology meet* (Vol. 367).

- Andress, J. (2014). *Cyber warfare techniques, tactics and tools for security practitioners* (Second edition.. ed.): Waltham, Massachusetts : Syngress, an imprint of Elsevier.
- Aporta, C., & Higgs, E. (2005). Satellite culture: global positioning systems, Inuit wayfinding, and the need for a new account of technology. *Current Anthropology*, 46(5), pp. 729-753.
- Arbaugh, W. (2002). The TCPA; what's wrong; what's right and what to do about it. <http://www.cs.umd.edu/~waa/TCPA/TCPA-goodnbad.pdf>
- Ardia, D. S. (2010). Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act. *Loyola of Los Angeles Law Review*, 43(2), pp. 373-506.
- Arief, B., & Besnard, D. (2003). Technical and Human Issues in Computer-Based Systems Security. *TECHNICAL REPORT SERIES- UNIVERSITY OF NEWCASTLE UPON TYNE COMPUTING SCIENCE*(790), pp.
- Armitage, R. (2002). To CCTV or not to CCTV. *A review of current research into the effectiveness of CCTV systems in reducing crime*. London: Nacro, pp. 1-8.
- Arora, J. (2009, January 29-30, 2009). *Digital Preservation, an Overview*. Paper presented at the National Seminar on Open Access to Textual and Multimedia Content: Bridging the Digital Divide (pp.
- Aslam, M., Gehrman, C., & Björkman, M. (2013). *Continuous security evaluation and auditing of remote platforms by combining trusted computing and security automation techniques*. Paper presented at the Proceedings of the 6th International Conference on Security of Information and Networks, Aksaray, Turkey (pp. 136-143),ACM.
- Atran, S. (2002). *In gods we trust : the evolutionary landscape of religion*: Oxford ; New York : Oxford University Press, 2002.
- August, T., August, R., & Shin, H. (2014). Designing user incentives for cybersecurity. *Communications of the ACM*, 57(11), pp. 43-46.
- August, T., & Tunca, T. I. (2011). Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science*, 57(5), pp. 934-959.
- Austen-Baker, R. A Relational Law of Contract?",(2004). *Journal of Contract Law*, 20, pp. 125.
- Bainbridge, D. (2005). The Nature of Software Contracts. *IP & IT Law*, 10.6(3), pp.
- Bajikar, S. (2002). Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper. In M. P. G. I. Corporation (Ed.): Intel Corporation.
- Balacheff, B., Chen, L., Pearson, S., Proudler, G., & Chan, D. (2000). Computing Platform Security in Cyberspace. *Information Security Technical Report*, 5(1), pp. 54-63. doi: 10.1016/S1363-4127(00)87631-1
- Balboni, P. (2004). Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in

- Electronic Communication. *Information & Communications Technology Law*, 13(3), pp. 211-242. doi: 10.1080/1360083042000219074
- Balboni, P. (2008a). Model for an adequate liability system for Trustmark Organisations. *INTERNATIONAL JOURNAL OF LIABILITY AND SCIENTIFIC ENQUIRY*, 1(1/2), pp. 151-163.
- Balboni, P. (2008b). *Trustmarks: Third-party liability of trustmark organisations in Europe*. Retrieved from http://dbiref.uvt.nl/iPort?request=full_record&db=wo&language=eng&query=doc_id=3240350
- Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, 52(11), pp. 68-73. doi: 10.1145/1592761.1592780
- Bańkowski, Z. (2007). Bringing the outside in: the ethical life of legal institutions *Law and legal Cultures in the 21st Century: Unity and Diversity (Wolters Kluwer Polska, 2007)* (pp. 193-217).
- Banks, I. M. (1988). The Player of Games. pp. 1-320.
- Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace, . Retrieved 25/8/2015, from <http://homes.eff.org/~barlow/Declaration-Final.html>
- Barney, J. B., & Hansen, M. H. (1994). Trustworthiness as a source of competitive advantage. *Strategic management journal*, 15(S1), pp. 175-190.
- Barth, R. C., & Smith, C. N. (1997). International Regulation of Encryption: technology will drive policy. In C. N. Brian Kahin (Ed.), *Borders in Cyberspace: Information Policy and the Global Information Infrastructure* (pp. 283-300). Cambridge: MIT.
- Bautista, C. B. (2014, April 8, 2014). EU court dismantles law requiring phone companies to retain customer data, *Digital Trends*. Retrieved from <http://www.digitaltrends.com/mobile/eu-court-ruling-against-data-retention/#!DTzyQ>
- Bayer, U., Habibi, I., Balzarotti, D., Kirda, E., & Kruegel, C. (2009). *A view on current malware behaviors*. Paper presented at the LEET'09: Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more, Boston, MA, USA. http://www.eurecom.fr/people/vs_bayer.en.htm
- BBC. (2006, 30/08/2006). Amazon begins taking Vista orders, *BBC News*. Retrieved from <http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/5297892.stm>
- BBC News. (2014). Top EU court rejects EU-wide data retention law, *BBC News*. Retrieved from <http://www.bbc.com/news/world-europe-26935096>
- Becher, S. I. (2009). A'Fair Contracts' Approval Mechanism: Reconciling Consumer Contracts and Conventional Contract Law. *University of Michigan Journal of Law Reform*, 42, pp. 747-804.

- Beesley, M. E., & Littlechild, S. C. (1989). The regulation of privatized monopolies in the United Kingdom. *The RAND Journal of Economics*, pp. 454-472.
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, 11(3-4), pp. 245-270.
- Bellare, M., Micciancio, D., & Warinschi, B. (2003). Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions *Advances in Cryptology—Eurocrypt 2003* (pp. 614-629). Warsaw, Poland: Springer.
- Benedetti, D. T. (2013). How Far Can the Government's Hand Reach Inside Your Personal Inbox?: Problems With the SCA, 30 J. Marshall J. Info. Tech. & Privacy L. 75 (2013). *The John Marshall Journal of Information Technology & Privacy Law*, 30(1), pp. 5.
- Benkler, Y., Roberts, H., Faris, R., Solow-Niederman, A., & Etling, B. (2015). Social mobilization and the networked public sphere: Mapping the SOPA-PIPA debate. *Political Communication*(ahead-of-print), pp. 1-31.
- Berger, B. (2005). Trusted computing group history. *Inf. Secur. Tech. Rep.*, 10(2), pp. 59-62. doi: 10.1016/j.istr.2005.05.007
- Best, M. L. (2004). Can the internet be a human right. *Human Rights & Human Welfare*, 4(1), pp. 23-31.
- Bigami, F. (2007). Privacy and law enforcement in the european union: the data retention directive. *Chicago Journal of International Law, Spring*, pp. 233-255.
- Bilar, D. (2009). Known knowns, known unknowns and unknown unknowns: anti-virus issues, malicious software and internet attacks for non-technical audiences. *Digital Evidence & Electronic Signature Law Review*, 6, pp. 123 - 131.
- Birmingham, R. L. (1969). Breach of contract, damage measures, and economic efficiency. *Rutgers L. Rev.*, 24, pp. 273.
- Bitton, M. (2011). Rethinking the Anti-Counterfeiting Trade Agreement's Copyright Criminal Enforcement Measures. *The journal of criminal law and criminology* 102, 1, pp. 67-118.
- Blanchette, J.-F., & Johnson, D. G. (2002). Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness. *The Information Society*, 18(1), pp. 33-45. doi: 10.1080/01972240252818216
- Blankenburg, E. (1984). The Poverty of Evolutionism: A Critique of Teubner's Case for "Reflexive Law". *Law & Society Review*, 18(2), pp. 273-289. doi: 10.2307/3053405
- Blunden, B. (2013). *Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System*: Jones & Bartlett Publishers.
- Borchard, E. M. (1924). Government Liability in Tort. *Yale Law Journal*, pp. 1-45.

- Bosniak, L. S. (1988). Exclusion and Membership: The Dual Identity of the Undocumented Worker Under United States Law. *Wis. L. Rev.*, pp. 955-1042.
- Boulding, W., & Kirmani, A. (1993). A consumer-side experimental examination of signaling theory: do consumers perceive warranties as signals of quality? *Journal of Consumer Research*, pp. 111-123.
- Boyle, J. (1997). Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors. *U. Cin. L. Rev.*, 66, pp. 177.
- Bradgate, R. (1999). Beyond the Millennium - The Legal Issues: Sale of Goods Issues and the Millennium Bug. *The Journal of Information, Law and Technology (JILT)*, 2 pp. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_1992/bradgate/
- Bradgate, R. (2010). Consumer Rights in Digital Products (I. a. S. Department for Business, Trans.) *A research report prepared for the UK Department for Business, Innovation and Skills* (pp. 76). Sheffield: Institute for Commercial Law Studies, University of Sheffield.
- Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, 4(3), pp. 340-347. doi: 10.1177/1948550612455931
- Bratus, S., Lembree, A., & Shubina, A. (2010). Software on the witness stand: what should it take for us to trust it? *Trust and Trustworthy Computing* (pp. 396-416): Springer.
- Braucher, J. (1990). Contract Versus Contractarianism: The Regulatory Role of Contract Law. *Wash. & Lee L. Rev.*, 47, pp. 697.
- Breidhardt, A., & Strupczewski, J. (Apr 8, 2014). EU court rejects requirement to keep data of telecom users, *Reuters*. Retrieved from <http://www.reuters.com/article/2014/04/08/us-eu-data-ruling-idUSBREA370F020140408>
- Brenner, S. W. C., Brian; Henninger, Jef. (2004). The Trojan Horse Defense in Cybercrime Cases. *Santa Clara Computer & High Tech. L.J.*, 21(1), pp. 1-54.
- Brickell, E., Camenisch, J., & Chen, L. (2004). *Direct Anonymous Attestation*. Paper presented at the Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS 2004) (pp. 132-145), ACM.
- Bridy, A. (2012). Copyright policymaking as procedural democratic process: A discourse-theoretic perspective on acta, sopa, and pipa. *Cardozo Arts & Ent. LJ*, 30, pp. 153.
- Brodsky, S. L., Griffin, M. P., & Cramer, R. J. (2010). The Witness Credibility Scale: An outcome measure for expert witness research. *Behavioral Sciences & the Law*, 28(6), pp. 892-907. doi: 10.1002/bsl.917
- Bryson, J. (2011). AI robots should not be considered moral agents. In N. Berlatsky (Ed.), *Artificial Intelligence*. Detroit: Greenhaven Press.

- Bunduchi, R. (2005). Business relationships in internet-based electronic markets: the role of goodwill trust and transaction costs. *Information Systems Journal*, 15(4), pp. 321-341.
- Burmester, M., & Mulholland, J. (2006, April 23 - 27). *The advent of trusted computing: implications for digital forensics* Paper presented at the Proceedings of the 2006 ACM symposium on Applied computing, Dijon, France (pp. 283-287),ACM Press.
- Byars, B., O'Keefe, T., & Clement, T. (2008). *Google, Inc.: Procurer, Possessor, Distributor, Aider and Abettor in Child Pornography*. Paper presented at the Forum on Public Policy: A Journal of the Oxford Round Table (pp. 1-7),Forum on Public Policy.
- Camenisch, J. (2004). Direct Anonymous Attestation: Achieving Privacy in Remote Authentication. *ZISC Information Security Colloquium*.
- Cameron, A. (2004). Digital Rights Management: Where Copyright and Privacy Collide. *Canadian Privacy Law Review*, pp. 1-9.
- Caplan, J. (2001). "This or that particular person": protocols of identification in nineteenth-century Europe. *Documenting individual identity: The development of state practices in the modern world*, 1, pp. 49-66.
- Carroll, A., Juarez, M., Polk, J., & Leininger, T. (2002). Microsoft Palladium: A Business Overview: Microsoft Press Release.
- Cavoukian, A., & Hamilton, T. (2002). The Privacy Payoff, How Successful Business Build Consumer Trust: McGraw-Hill Ryerson Trade.
- CERT. (2009, February 12, 2009). CERT Statistics (Historical). *Cataloged vulnerabilities*. Retrieved April 2010, 2010, from http://www.cert.org/stats/cert_stats.html#vuls
- Chandler, A. J. (2003). Security in Cyberspace: Combatting Distributed Denial of Service Attacks. *University of Ottawa Law and Technology Journal*, 1(1-2), pp. 231-261.
- Chapman, M. R. R. (2006). *In Search of Stupidity: Over Twenty Years of High Tech Marketing Disasters*: Apress.
- Chari, N. V. (2010). Disciplining Standard Form Contract Terms Through Online Information Flows: An Empirical Study. *NYUL Rev.*, 85, pp. 1618.
- Charlesworth, A. (2005). DRM: the Straw to Break of Procrustean Approaches to Copyright? In F. Grosheide & J. J. Brinkhof (Eds.), *Intellectual Property 2004: Articles on Crossing Borders between traditional and actual (Molengrafica Series)* (pp. 405-422): Intersentia.
- Cheng-Hao, C., & Saeedi, M. (2006). Building a Trust Model in the Online Market Place. *Journal of Internet Commerce*, 5(1), pp. 101. doi: 10.1300/J179v05n01•06
- Cheng, E. K. (2004). Reenvisioning Law Through the DNA Lens. *NYU Ann. Surv. Am. L.*, 60, pp. 649.
- Cheung, A., & Weber, R. H. (2008). Internet governance and the responsibility of internet service providers. *Wis. Int'l LJ*, 26, pp. 403.

- Chopra, S., & White, L. F. (2011). *A legal theory for autonomous artificial agents*: University of Michigan Press.
- Christensen, A. M., Crowder, C. M., Ousley, S. D., & Houck, M. M. (2014). Error and its meaning in forensic science. *Journal of forensic sciences*, 59(1), pp. 123-126.
- Christianson, B., & Harbison, W. (1997). Why isn't trust transitive? In M. Lomas (Ed.), *Security Protocols* (Vol. 1189, pp. 171-176): Springer Berlin Heidelberg.
- Clarke, R. V., Field, S., & McGrath, G. (1991). Target hardening of banks in Australia and displacement of robberies. *Security Journal*, 2(2), pp. 84-90.
- Cohen, J. E. (2006). Pervasively distributed copyright enforcement. *Georgetown Law Journal*, 95, pp. 1-48.
- Cole, M., & Boehm, F. (2014). Data Retention after the Judgement of the Court of Justice of the European Union. *University of Luxemburg*, pp. 1-107.
- Colgrove, J., & Bayer, R. (2005). Manifold restraints: liberty, public health, and the legacy of Jacobson v Massachusetts. *Am J Public Health*, 95 (4), pp. 571-576.
- Collins, H. (1994). Good faith in European contract law. *Oxford Journal of Legal Studies*, pp. 229-254.
- Connerley, M. L., Arvey, R. D., & Bernardy, C. J. (2001). Criminal background checks for prospective and current employees: Current practices among municipal agencies. *Public Personnel Management*, 30(2), pp. 173-183.
- Cook, W. W. (1919). Hohfeld's Contributions to the Science of Law. *Yale Law Journal*, pp. 721-738.
- Cooper, A., & Martin, A. (2006). *Towards an open, trusted digital rights management platform*. Paper presented at the Proceedings of the ACM workshop on Digital rights management, Alexandria, Virginia, USA.
- Cornish, D. B., & Clarke, R. V. (1987). UNDERSTANDING CRIME DISPLACEMENT: AN APPLICATION OF RATIONAL CHOICE THEORY. *Criminology*, 25(4), pp. 933-948. doi: 10.1111/j.1745-9125.1987.tb00826.x
- Council, C. M. O. (2006). Secure the Trust of Your Brand, . CMO council webpage: CMO.
- Court of Justice of the European Union. (2014). The Court of Justice declares the Data Retention Directive to be invalid [Press release]. Retrieved from <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
- Craswell, R. (1987). Contract remedies, renegotiation, and the theory of efficient breach. *S. Cal. L. Rev.*, 61, pp. 629.
- Craswell, R. (1993). On the Uses of " Trust": Comment on Williamson," Calculativeness, Trust, and Economic Organization". *Journal of Law and Economics*, pp. 487-500.
- Craswell, R., & Calfee, J. E. (1986). Deterrence and uncertain legal standards. *JL Econ. & Org.*, 2, pp. 279.

- Crowe, T. D. (2000). *Crime prevention through environmental design : applications of architectural design and space management concepts* (Second edition.. ed.). Boston, Mass.: Boston, Mass. : Butterworth-Heinemann.
- Danidou, Y. (2006). *Legal Implications of Trusted Computing*. (MSc in Advanced Computing - Internet Technologies Master Thesis), University of Bristol, Bristol.
- De Bruin, R., Keuleers, E., Lazaro, C., Pouillet, Y., & Viersma, M. (2005). Analysis and Definition of Common Characteristics of Trustmarks and Web Seals in the European Union: Recuperado de http://ec.europa.eu/consumers/cons_int/e-commerce/e-commerce_final_report_annexe_en.pdf.
- Dean, D. H., & Biswas, A. (2001). Third-Party Organization Endorsement of Products: An Advertising Cue Affecting Consumer Prepurchase Evaluation of Goods and Services. *Journal of Advertising*, 30(4), pp. 41-57.
- DeFeo, M. A. (1966). Entrapment as a Defense to Criminal Responsibility: Its History, Theory and Application. *USFL Rev.*, 1, pp. 243.
- DeSimone, C. (2010). Pitting Karlsruhe against Luxembourg-German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German LJ*, 11, pp. 291.
- Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6), pp. 644-654. doi: 10.1109/TIT.1976.1055638
- Dixon, L., & Gill, B. (2002). Changes in the standards for admitting expert evidence in federal civil cases since the Daubert decision. *Psychology, Public Policy, and Law*, 8(3), pp. 251.
- Donohue, L. K. (2015). High Technology, Consumer Privacy, and US National Security. *Am. U. Bus. L. Rev.*, 4, pp. 11.
- Dorf, M. C. (2003). The Domain of Reflexive Law. *Columbia Law Review*, 103(2), pp. 384-402. doi: 10.2307/1123697
- Draper, H. (1978). *Private police*. Hassocks: Hassocks : Harvester Press.
- Draughn, M. (2014, September 20, 2014). Orin Kerr's Dangerous Thinking, *Windypundit*. Retrieved from <https://windypundit.com/2014/09/orin-kerrs-dangerous-idea/>
- Dulisse, B. (1997). Methodological issues in testing the hypothesis of risk compensation. *Accident Analysis & Prevention*, 29(3), pp. 285-292. doi: [http://dx.doi.org/10.1016/S0001-4575\(96\)00082-6](http://dx.doi.org/10.1016/S0001-4575(96)00082-6)
- Dunbar, P. (1997). What will be the Impact of Civilianization on Police Investigations by 2002 at the Oakland Police Department? *Command College Paper*, 2, pp. 1-8.
- Duranti, L., & Rogers, C. (2012). Trust in digital records: An increasingly cloudy legal area. *Computer Law & Security Review*, 28(5), pp. 522-531.
- Durkheim, E. (2014). *The division of labor in society*: Simon and Schuster.

- EC. (2009). Consumer Rights: Commission wants consumers to surf the web without borders. (IP/09/702). http://europa.eu/rapid/press-release_IP-09-702_en.htm#PR_metaPressRelease_bottom
- Economides, N. (2001). The Microsoft Antitrust Case. *Journal of Industry, Competition and Trade*, 1(1), pp. 7-39. doi: 10.1023/A:1011517724873
- Edwards, B., Locasto, M., & Epstein, J. (2014). *Panel Summary: The Future of Software Regulation*. Paper presented at the Proceedings of the 2014 workshop on New Security Paradigms Workshop (pp. 117-126), ACM.
- Edwards, J. L. J. (1954). The criminal degrees of knowledge *. *Modern Law Review*, 17(4), pp. 293-314. doi: 10.1111/j.1468-2230.1954.tb02157.x
- Edwards, L. (2006). Dawn of the Death of Distributed Denial of Service: How to Kill Zombies. *Cardozo Arts & Entertainment Law Journal*, 24(1), pp. 23-62.
- Eisenberg, M. A. (1999). Why there is no law of relational contracts. *Nw. UL Rev.*, 94, pp. 805.
- Elliott, J. (2000). Distributed denial of service attacks and the zombie ant effect. *IT professional*(2), pp. 55-57.
- Endeshaw, A. (2001). The Legal Significance of Trustmarks. *Information & Communications Technology Law*, 10(2), pp. 203-230. doi: 10.1080/13600830120074690
- England, P., Manferdelli, J., & Willman, B. (2003). A trusted open platform. *Computer*, 36(7), pp. 55-62. doi: 10.1109/MC.2003.1212691
- Epstein, J., Matsumoto, S., & McGraw, G. (2006). Software security and SOA: danger, Will Robinson! *IEEE Security & Privacy*(1), pp. 80-83.
- Epstein, R. A. (1975). Unconscionability: A critical reappraisal. *Journal of Law and Economics*, pp. 293-315.
- Epstein, R. A. (1989). Beyond Foreseeability: Consequential Damages in the Law of Contract. *The Journal of Legal Studies*, 18(1), pp. 105-138.
- Erickson, J. S. (2003). Fair use, DRM, and Trusted Computing. *Communications of the ACM*, 46(4), pp. 34-39.
- Espiner, T. (2009). EC wants software makers held liable for code, *ZDNet UK*. Retrieved from <http://www.zdnet.co.uk/news/it-strategy/2009/05/08/ec-wants-software-makers-held-liable-for-code-39649689/>
- European Commission. (2013a). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. In T. C. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS (Ed.): European Commission.
- European Commission. (2013b). "Information society statistics" - Statistics Explained Retrieved 15/10/2013 http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics#

- European Commission. (2015, 2/3/2015). Cybersecurity. Retrieved 26/6/2015, 2015, from <https://ec.europa.eu/digital-agenda/en/cybersecurity#Article>
- Eurostat - European Commission. (2009). *Consumers in Europe* (2009 ed.). Luxembourg: Office for Official Publications of the European Communities.
- Eurostat - European Commission. (2012). *Consumer Conditions Scoreboard – Consumers at home in the single market* (7th ed.). Luxembourg: Office for Official Publications of the European Communities.
- Eurostat. (2011). Nearly one third of internet users in the EU27 caught a computer virus 8 February 2011: *Safer Internet Day*. Luxembourg: Eurostat Press Office.
- Falliere, N., Murchu, L. O., & Chien, E. (2011). W32.Stuxnet Dossier *Security Response* (1.4 ed., pp. 69). Cupertino, CA: Symantec Corporation.
- Feinman, J. M. (2003). Liability of Accountants for Negligent Auditing: Doctrine, Policy, and Ideology. *FLORIDA STATE UNIVERSITY LAW REVIEW*, 31, pp. 17-66.
- Felten, E. W. (2003). Understanding Trusted Computing: Will Its Benefits Outweigh Its Drawbacks? *IEEE Security & Privacy*, 1, 60-62.
- Fleming, A. (2014). The Rise and Fall of Unconscionability as the 'Law of the Poor'. *Georgetown Law Journal*, 102(5), pp. 1383-1441.
- Flick, C. (2004). *The Controversy over Trusted Computing*. (Bachelor of Science), The University of Sydney, Sydney. Retrieved from http://liedra.net/misc/Controversy_Over_Trusted_Computing.pdf
- Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology*, 1(1), pp. 33-52.
- Fox Jr, J. W. (2003). RELATIONAL CONTRACT THEORY AND DEMOCRATIC CITIZENSHIP. *Case Western Reserve Law Review*, 54(1), pp. 1-67.
- Franz, M. (Producer). (2005). Practical Language-Based Security From The Ground Up "Verify Everything, Every Time & Prove It Remotely". [ppt] Retrieved from <http://www.doi.ics.keio.ac.jp/CIIP05/26/11-Franz.pdf>
- Friedman, D. (1996). A World of Strong Privacy: Promises and Perils of Encryption. *Social Philosophy and Policy*, 13, pp. 212-228. doi: 10.1017/S0265052500003526
- Fromm, J. (2004). *The emergence of complexity*: Kassel university press Kassel.
- Froomkin, A. M. (2000). The Death of Privacy? *Stanford Law Review*, 52(5), pp. 1461-1543.
- Fukuyama, F. (1995). *Trust: The Social Virtues and The Creation of Prosperity* (1st ed.). New York: Simon & Schuster Free Press Paperbacks book.
- Gallery, E. (2008). *Who are the TCG and what are the Trusted Computing concepts?* Paper presented at the TRUST2008, Villach, Austria. Presentation retrieved from <http://dblp.uni-trier.de/pers/hd/g/Gallery:Eimear>

- Gambetta, D. (2000). Can we trust trust. *Trust: Making and breaking cooperative relations, 2000*, pp. 213-237.
- Ganssle, J. (2011). Software liability laws - Part 2. Retrieved from <http://www.eetimes.com/electronics-blogs/other/4233623/Software-liability-laws---Part-2>
- Garfinkel, S. (2007). *Anti-forensics: Techniques, detection and countermeasures*. Paper presented at the 2nd International Conference on i-Warfare and Security (pp. 77),
- Garlinger, P. P. (2009). Privacy, Free Speech, and the Patriot Act: First and Fourth Amendment Limits on National Security Letters. *NYUL Rev.*, 84, pp. 1105.
- Gates, B. (2002, 18 July 2002). Executive E-mail: Trustworthy Computing. Retrieved 26 April 2006, 2006, from <http://www.microsoft.com/mscorp/execmail/2002/07-18twc.asp>
- Gatewood, R., & Hubert, F. (1998). *Human resource selection*. Fort Worth, Tex.: Dryden Press.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, 27(1), pp. 51-90.
- Gefen, D., & Straub, D. W. (2003). Managing user trust in B2C e-services. *E-service Journal*, 2(2), pp. 7-24.
- Gehring, A. R. (2006, 2006). Trusted computing for digital rights management. http://www.indicare.org/tiki-read_article.php?articleId=179. from http://www.indicare.org/tiki-read_article.php?articleId=179
- Gessner, D., Olivereau, A., Segura, A. S., & Serbanati, A. (2012, 25-27 June 2012). *Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things*. Paper presented at the Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 998-1003), IEEE.
- Giannelli, P. C. (1993). Daubert: Interpreting the Federal Rules of Evidence. *Cardozo L. Rev.*, 15, pp. 1999.
- Gibson, J. (2007). Risk aversion and rights accretion in intellectual property law. *Yale Law Journal*, 116, pp. 882.
- Gilens, N. (2014). The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures. Available at SSRN 2498150, pp. 525-546.
- Giliker, P. (2000). Osman and police immunity in the English law of torts. *Legal Studies*, 20(3), pp. 372-392.
- Gill, M., & Hart, J. (1997). Policing as a business: The organisation and structure of private investigation. *Policing and Society*, 7(2), pp. 117-141. doi: 10.1080/10439463.1997.9964768
- Gilling, D. (1997). *Crime prevention : theory, policy and politics*. London: London : UCL Press.
- Goldberg, V. P. (1976). Toward an expanded economic theory of contract. *Journal of Economic Issues*, pp. 45-61.

- Gollmann, D. (1999). *Computer security*. New York, NY, USA: John Wiley & Sons, Inc.
- Gonzalez-Rodriguez, J., Rose, P., Ramos, D., Toledano, D. T., & Ortega-Garcia, J. (2007). Emulating DNA: Rigorous quantification of evidential weight in transparent and testable forensic speaker recognition. *Audio, Speech, and Language Processing, IEEE Transactions on*, 15(7), pp. 2104-2115.
- Gordon, L., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), pp. 438-457. doi: 10.1145/581271.581274
- Gordon, L., & Loeb, M. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, 8(5), pp. 335-337. doi: 10.1007/s10796-006-9010-7
- Gorham-Oscilowski, U., & Jaeger, P. T. (2008). National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly*, 25(4), pp. 625-644. doi: <http://dx.doi.org/10.1016/j.giq.2008.02.001>
- GovTrack.us. (2009). H.R. 1076 (111th): Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009. *Bills*. Retrieved 22/8/2015, 2015, from <https://www.govtrack.us/congress/bills/111/hr1076>
- Graham, C. (2013, 21/1/2013). Fake anti-virus attack spread via bogus ADP anti-fraud update emails, *Naked Security*. Retrieved from <http://nakedsecurity.sophos.com/2013/01/15/bogus-adp-anti-fraud-update-emails/>
- Graham, M. H. (1986). Expert Witness Testimony and the Federal Rules of Evidence: Insuring Adequate Assurance of Trustworthiness. *U. Ill. L. Rev.*, pp. 43.
- Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *American Journal of Sociology*, 91(3), pp. 481-510. doi: 10.2307/2780199
- Green, L. (2002). Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers. *Presented in DEFCON 10*. from <http://www.cypherpunks.to/TCPADEFCON10.pdf>
- Green, S. P. (2002). Plagiarism, norms, and the limits of theft law: Some observations on the use of criminal sanctions in enforcing intellectual property rights. *Hastings Law Journal*, 54(1), pp. 167-242.
- Grossklags, J., & Acquisti, A. (2007). *When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*. Paper presented at the Online Proceedings of the Second Annual Workshop on Economics and Information Security (pp.
- Grossklags, J., Christin, N., & Chuang, J. (2008). *Secure or insure?: a game-theoretic analysis of information security games*. Paper presented at the Proceedings

- of the 17th international conference on World Wide Web, Beijing, China (pp. 209-218),ACM.
- Guadamuz, A. (2011). *Networks, Complexity and Internet Regulation: Scale-free Law*: Edward Elgar Pub.
- Guadamuz, A. (2013). *Networks, complexity and internet regulation scale-free law*: The University of Edinburgh.
- Gudel, P. J. (1998). Relational Contract Theory and the Concept of Exchange [comments] (pp. 763).
- Guez, M. (Producer). (2010). Technical measures in the context of the Hadopi Law (France). . *Presentation before the Stakeholders*. Retrieved from <http://fr.readwriteweb.com/wpcontent/uploads/2010/09/Slides-SCPP.pdf>
- Halboob, W., & Mahmud, R. (2012). State of the Art in Trusted Computing Forensics *Future Information Technology, Application, and Service* (pp. 249-258): Springer.
- Halpern, J. Y., & Moses, Y. (1990). Knowledge and common knowledge in a distributed environment. *Journal of the ACM (JACM)*, 37(3), pp. 549-587.
- Halpin, A. (2007). Rights, Duties, Liabilities, and Hohfeld. *Legal Theory*, 13(01), pp. 23-39.
- Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*, 3, pp. 44-49. doi: 10.1016/j.diin.2006.06.005
- Harshman, E., & Chachere, D. (2000). Employee References: Between the Legal Devil and the Ethical Deep Blue Sea. *Journal of Business Ethics*, 23(1), pp. 29-39. doi: 10.1023/a:1006218926970
- Hartshorne, J., Smith, N., & Everton, R. (2000). 'Caparo Under Fire': a Study into the Effects upon the Fire Service of Liability in Negligence. *The Modern Law Review*, 63(4), pp. 502-522. doi: 10.1111/1468-2230.00277
- Hassell, J., & Steen, S. (2003). Avoiding Spoliation of Electronic Discovery. <http://www.experts.com/Articles/Avoiding-Spoliation-of-Electronic-Discovery-By-Johnette-Hassell-PhD-Susan-Steen>
- Hassell, J., & Steen, S. (2005). Preserving and Protecting Computer Evidence. *Evidence Technology Magazine*, 3(4), pp. 16-18.
- Hazlett, T. W. (1999). Microsoft's Internet Exploration: Predatory or Competitive. *Cornell JL & Pub. Pol'y*, 9, pp. 29-60.
- Hedlund, J. (2000). Risky business: safety regulations, risk compensation, and individual behavior. *Injury Prevention*, 6(2), pp. 82-89. doi: 10.1136/ip.6.2.82
- Helman, L. (2010). Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement. *Tex. Intell. Prop. LJ*, 19, pp. 111.

- Henderson, S. E., & Yarbrough, M. E. (2002). Frontiers of Law: The Internet and Cyberspace: Suing the Insecure?: A Duty of Care in Cyberspace. *New Mexico Law Review*, 32(11), pp.
- Henrich, J. The evolution of costly displays, cooperation and religion. *Evolution and Human Behavior*, 30(4), pp. 244-260. doi: 10.1016/j.evolhumbehav.2009.03.005
- Heydon, J. (1973). The Problems of Entrapment. *The Cambridge Law Journal*, 32(02), pp. 268-286.
- Hilley, S. (2004). Trusted computing - path to security or road to servitude? *Network Security*, 2004(8), pp. 12-15.
- Hoepman, J.-H. (2012). In Things We Trust? Towards Trustability in the Internet of Things. In R. Wichert, K. Van Laerhoven & J. Gelissen (Eds.), *Constructing Ambient Intelligence* (Vol. 277, pp. 287-295): Springer Berlin Heidelberg.
- Hoey, A. (1995). Analysis of the Police and Criminal Evidence Act, s.69 - Computer generated evidence *Web Journal of Current Legal Issues*, 5, pp.
- Hoffmann, H., & Söllner, M. (2014). Incorporating behavioral trust theory into system development for ubiquitous applications. *Personal and Ubiquitous Computing*, 18(1), pp. 117-128. doi: 10.1007/s00779-012-0631-1
- Hohfeld, W. N. (1917). Fundamental legal conceptions as applied in judicial reasoning. *Yale Law Journal*, pp. 710-770.
- Holland, H. B. (2007). In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism. *Kansas Law Review*, 56(101), pp. 101-137.
- Holtfreter, R. E. (2011). Scareware Fraud: All Trick and No Treat?(part 1). *Fraud Magazine*, pp.
- Honsell, H. (1999). Die Haftung für Gutachten und Auskunft unter besonderer Berücksichtigung von Drittinteressen *Festschrift für Dieter Medicus* (pp. 211-233). Heymann: Köln.
- Horwitz, M. J. (1974). The historical foundations of modern contract law. *Harvard law review*, pp. 917-956.
- Hosmer, C. (2002). Proving the integrity of digital evidence with time. *International Journal of Digital Evidence*, 1(1), pp. 1-7.
- Hough, M., Jackson, J., Bradford, B., Myhill, A., & Quinton, P. (2010). Procedural Justice, Trust, and Institutional Legitimacy. *Policing: A Journal of Policy and Practice*, 4(3), pp. 203-210. doi: 10.1093/police/paq027
- Houston, R. W., & Taylor, G. K. (1999). Consumer Perceptions of CPA WebTrustSM Assurances: Evidence of an Expectation Gap. *International Journal of Auditing*, 3(2), pp. 89-105.
- Hu, X. R., Wu, G. H., Wu, Y. H., & Zhang, H. (2010). The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *DECISION SUPPORT SYSTEMS*, 48(2), pp. 407-418.

- Huanguo, Z., Jie, L., Gang, J., Zhiqiang, Z., Fajiang, Y., & Fei, Y. (2006). Development of trusted computing research. *Wuhan University Journal of Natural Sciences*, 11(6), pp. 1407-1413. doi: 10.1007/BF02831786
- Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), pp. 528-535. doi: 10.1016/j.clsr.2009.09.005
- Hussain, M., & Abdulsalam, H. (2011). *SECaaS: security as a service for cloud-based applications*. Paper presented at the Proceedings of the Second Kuwait Conference on e-Services and e-Systems (pp. 8), ACM.
- Intellect. (2010). Intellect reacts to the National Security Strategy and Strategic Defence and Security Review. <http://www.intellectuk.org/media-releases/6378>
- Ivens, B. S., & Blois, K. J. (2004). Relational exchange norms in marketing: A critical review of Macneil's contribution. *Marketing theory*, 4(3), pp. 239-263.
- Jabbar, M. (2010). Overcoming Daubert's shortcomings in criminal trials: making the error rate the primary factor in Daubert's validity inquiry. *NYUL Rev.*, 85, pp. 2034.
- Jeffery, C. R. (1977). *Crime prevention through environmental design*: Sage Publications Beverly Hills.
- Johnson, D. D., & Bering, J. M. (2006). Hand of God, mind of man: Punishment and cognition in the evolution of cooperation. *Evolutionary Psychology*, 4(1), pp. 219-233.
- Johnson, D. G., & Miller, K. W. (2006). *A dialogue on responsibility, moral agency, and IT systems*. Paper presented at the Proceedings of the 2006 ACM symposium on Applied computing (pp. 272-276), ACM.
- Johnson, S. D., Guerette, R. T., & Bowers, K. J. (2012). Crime displacement and diffusion of benefits. *The Oxford handbook of crime prevention*, pp. 337.
- Kallath, D. (2005). Trust in trusted computing - the end of security as we know it. *Computer Fraud and Security*, 2005(12), pp. 4-7. doi: 10.1016/S1361-3723(05)70283-9
- Kamp, P.-H. (2011). The software industry is the problem. *Queue*, 9(9), pp. 10.
- Karnow, C. E. (1996). Liability for distributed artificial intelligences. *Berkely Tech. LJ*, 11, pp. 147.
- Katsikas, S., Lopez, J., & Pernul, G. (2005). Trust, Privacy and Security in E-Business: Requirements and Solutions. In P. Bozaris & E. Houstis (Eds.), *Advances in Informatics* (Vol. 3746, pp. 548-558): Springer Berlin Heidelberg.
- Katyal, N. K. (2003). Digital Architecture as Crime Control. *The Yale Law Journal*, 112(8), pp. 2261-2289. doi: 10.2307/3657476
- Kaufman, L. M. (2010). Can a trusted environment provide security? *Security & Privacy, IEEE*, 8(1), pp. 50-52.

- Keeton, W. P. (1984). *Prosser and Keeton on Torts* (5 Sub edition ed.). St. Paul MN: West Group.
- Kenny, S., & Borking, J. (2002). The value of privacy engineering. *J. Inform. Law Technol.(JILT)*, 7(1), pp. 1-29.
- Kerr, O. (2014). The Volokh Conspiracy - Apple's dangerous game. <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/>
- Kesan, J., Majuca, R., & Yurcik, W. The Economic Case for Cyberinsurance: University of Illinois College of Law.
- Kessler, F. (1943). Contracts of Adhesion--Some Thoughts About Freedom of Contract. *Colum. L. Rev.*, 43, pp. 629.
- Kim, B. C., Chen, P. Y., & Mukhopadhyay, T. (2011). The effect of liability and patch release on software security: The monopoly case. *Production and Operations Management*, 20(4), pp. 603-617.
- King, S. T., Tucek, J., Cozzie, A., Grier, C., Jiang, W., & Zhou, Y. (2008). Designing and Implementing Malicious Hardware. *LEET*, 8, pp. 1-8.
- Knight, J. (2001). Social norms and the rule of law: Fostering trust in a socially diverse society. *Trust in society*, 2, pp. 354-373.
- Koehler, J. J. (2007). Fingerprint error rates and proficiency tests: What they are and why they matter. *Hastings LJ*, 59, pp. 1077.
- Koehler, J. J., Chia, A., & Lindsey, S. (1995). The random match probability (RMP) in DNA evidence: Irrelevant and prejudicial? *Jurimetrics Journal*, 35, pp. 201.
- Køien, G. (2011). Reflections on Trust in Devices: An Informal Survey of Human Trust in an Internet-of-Things Context. *Wireless Personal Communications*, 61(3), pp. 495-510. doi: 10.1007/s11277-011-0386-4
- Komesar, N. K. (1985). Lawyering versus Continuing Relations in the Administrative Setting. *Wis. L. Rev.*, pp. 751.
- Konieczny, P. (2014). The day Wikipedia stood still: Wikipedia's editors' participation in the 2012 anti-SOPA protests as a case study of online organization empowering international and national political opportunity structures. *Current Sociology*, 62(7), pp. 994-1016.
- Koniotou, M. (2013, 14/10/2013). EU Commissioner stresses need for digital skills, *Cyprus News Agency*. Retrieved from <http://www.cna.org.cy/webnews.asp?a=6304a8e0a2fd4321ba4b9c697231faee>
- Koops, B.-J. (1999). *The crypto controversy: a key conflict in the information society* (Vol. 6): Kluwer Law International.
- Koops, B.-J., Hildebrandt, M., & Jaquet-Chiffelle, D.-O. (2010). Bridging the accountability gap: Rights for new entities in the information society? *Minnesota Journal of Law, Science & Technology*, 11(2), pp. 497-561.
- Kornblum, J. (1998). FTC, GeoCities Settle on Privacy, *CNET News.com*. Retrieved from <http://news.cnet.com/news/0-1005-200-332199.html>

- Kovar, S. E., Burke, K. G., & Kovar, B. R. (2000). Consumer Responses to the CPA WEBTRUST Assurance. *Journal of Information Systems*, 14(1), pp. 17-35.
- Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7), pp. 509-520. doi: <http://dx.doi.org/10.1016/j.cose.2009.04.006>
- Krieger, M. (2013). Search Engine "Duck Duck Go" Experiences Traffic Surge in Wake of NSA Scandal. *Liberty Blitzkrieg*. <https://libertyblitzkrieg.com/2013/07/10/search-engine-duck-duck-go-experiences-traffic-surge-in-wake-of-nsa-scandal/>
- Krogh, C., & Herrestad, H. (1999). Hohfeld in cyberspace and other applications of normative reasoning in agent technology. *Artificial intelligence and law*, 7(1), pp. 81-96. doi: 10.1023/A:1008367514393
- Kühling, J., & Heitzer, S. (2015). Returning through the National Back Door? The future of data retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere. *European law review*, 2, pp. 263-278.
- Kwecka, Z., Buchanan, W., Schafer, B., & Rauhofer, J. (2014). 'I am Spartacus': privacy enhancing technologies, collaborative obfuscation and privacy as a public good. *Artificial intelligence and law*, 22(2), pp. 113-139.
- Lampson, B. W. (1974). Protection. *ACM SIGOPS Operating Systems Review*, 8(1), pp. 18-24. doi: 10.1145/775265.775268
- Landrum, S. (2014). Much Ado About Nothing?: What the Numbers Tell Us About How State Courts Apply the Unconscionability Doctrine to Arbitration Agreements. *Marquette Law Review*, 97(3), pp. 751-812.
- Lane Jr, D. M. (1988). Publisher Liability for Material That Invites Reliance. *Tex. L. Rev.*, 66, pp. 1155-1629.
- Langheinrich, M. (2003). *When trust does not compute-the role of trust in ubiquitous computing*. Paper presented at the Workshop on Privacy at UBICOMP (pp. 1-8),
- Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *Security & Privacy, IEEE*, 9(3), pp. 49-51. doi: 10.1109/MSP.2011.67
- Lee, C. (2011). Reasonableness with teeth: the future of Fourth Amendment reasonableness analysis. *Miss. LJ*, 81, pp. 1133.
- Lee, W., & Hwang, C. (2007). *A forensic computing system using a digital right management technique*. Paper presented at the Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on (pp. 258-262),IEEE.
- Leff, A. A. (1967). Unconscionability and the Code. The Emperor's New Clause. *University of Pennsylvania Law Review*, pp. 485-559.
- Lelarge, M., & Bolot, J. (2009). Economic Incentives to Increase Security in the Internet: The Case for Insurance (pp. 1494-1502).
- Leon, G. (1961). Foreseeability in Negligence Law. *Columbia Law Review*, 61(8), pp. 1401-1424.

- Leshed, G., Velden, T., Rieger, O., Kot, B., & Sengers, P. (2008). *In-car gps navigation: engagement with and disengagement from the environment*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1675-1684), ACM.
- Lessig, L. (1996). The Zones of Cyberspace. *Stanford Law Review*, 48(5), pp. 1403-1411.
- Lessig, L. (1999). *Code and other laws of cyberspace*: Basic books.
- Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age*: Penguin.
- Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, 63(4), pp. 967-985. doi: 10.1093/sf/63.4.967
- Lewis, J. D., & Weigert, A. J. (1985). SOCIAL ATOMISM, HOLISM, AND TRUST. *Sociological Quarterly*, 26(4), pp. 455-471. doi: 10.1111/j.1533-8525.1985.tb00238.x
- Leyden, J. (2007, 13/8/2007). Germany enacts 'anti-hacker' law - Will the last security expert to leave Germany turn off the lights? *The Register, Security*. Retrieved 19/7/2011, 2011, from http://www.theregister.co.uk/2007/08/13/german_anti-hacker_law/print.html
- Lilienthal, J. W. (1887). Privity of Contract. *Harvard law review*, 1(5), pp. 226-232. doi: 10.2307/1321337
- Lim, Y. J., & Sexton, S. E. (2011). Internet as a human right: a practical legal framework to address the unique nature of the medium and to promote development. *Wash. JL Tech. & Arts*, 7, pp. 295.
- Lipson, H. F. (2002). Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. In C. M. University (Ed.), *CERT Coordination Center, Special Report CMU/SEI-2002-SR-009*.
- Liu, G., Wang, Y., & Orgun, M. A. (2011). *Trust Transitivity in Complex Social Networks*. Paper presented at the AAAI (pp. 1222-1229), AAAI Press.
- Livingstone, K., & Hart, J. (2003). The Wrong Arm of the Law? Public Images of Private Security. *Policing and Society*, 13(2), pp. 159-170. doi: 10.1080/10439460308027
- Loader, I. (1997). Thinking Normatively About Private Security. *Journal of Law and Society*, 24(3), pp. 377-394. doi: 10.1111/j.1467-6478.1997.tb00003.x
- Lohmann von F. (2003). *Meditations on Trusted Computing*. Retrieved from http://www.eff.org/Infrastructure/trusted_computing/20031001_meditations.php
- Luhmann, N. (1988). The Third Question: The Creative Use of Paradoxes in Law and Legal History. *Journal of Law and Society*, 15(2), pp. 153-165. doi: 10.2307/1410051
- Luhmann, N., Davis, H., Raffan, J., Rooney, K., & Luhmann, N. (1979). *Trust and Power : two works by Niklas Luhmann*: Chichester : Wiley, 1979.

- Macaulay, S. (1985). Empirical View of Contract, *An. Wis. L. Rev.*, pp. 465.
- Macaulay, S. (2003). The real and the paper deal: empirical pictures of relationships, complexity and the urge for transparent simple rules. *The Modern Law Review*, 66(1), pp. 44-79.
- MacCormick, N. (1991). Donoghue v. Stevenson and legal reasoning. *Donoghue v. Stevenson and the Modern Law of Negligence, Continuing Legal Education of British Columbia, Vancouver*, pp. 191-213.
- MacDonald, J., & Stokes, R. J. (2006). Race, social capital, and trust in the police. *Urban Affairs Review*, 41(3), pp. 358-375.
- Machiavelli, N. (1952). The prince (L. Ricci, Trans.). *New York: New York American Library. (Original work published 1513)*, pp.
- MacKie-Mason, J. K., & Netz, J. S. (2006). Manipulating interface standards as an anti-competitive strategy. *Standards and public policy*, pp. 231-259.
- MacNeil, I., & Campbell, I. D. (2001). *The relational theory of contract : selected works of Ian MacNeil*. London: Sweet & Maxwell.
- Macneil, I. R. (1973). Many Futures of Contracts, *The. S. Cal. L. Rev.*, 47, pp. 691-816.
- Macneil, I. R. (1977). Contracts: adjustment of long-term economic relations under classical, neoclassical, and relational contract law. *Nw. UL Rev.*, 72, pp. 854.
- Macneil, I. R. (1985). Relational contract: What we do and do not know. *Wis. L. Rev.*, pp. 483.
- Macneil, I. R. (1987). Relational Contract Theory as Sociology: A Reply to Professors Lindenberg and de Vos. *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft*(2), pp. 272-290.
- Macneil, I. R. (2000). Contracting worlds and essential contract theory. *Social & Legal Studies*, 9(3), pp. 431-438.
- Manta, I. D. (2011). The Puzzle of Criminal Sanctions for Intellectual Property Infringement. *Harvard Journal of Law and Technology*, 24(2), pp. 2010-2030.
- Marsden, C. T. (2000). *Regulating the global information society*: Psychology Press.
- Marshall, J. (2009). On the Idea of Understanding Weinrib: Weinrib and Keating on Bipolarity, Duty, and the Nature of Negligence. *S. Cal. Interdisc. LJ*, 19, pp. 385.
- Marsico, C. V. (2005). Computer evidence v. daubert: The coming conflict *CERIAS Tech Report 2005-17* (pp. 1-21). Center for Education and Research in Information Assurance and Security Purdue University.
- Martin, B., & Newhall, J. (2013). Criminal Copyright Enforcement Against Filesharing Services. *NCJL & Tech.*, 15, pp. 101.
- Mason, S. (2005). Trusted computing and forensic investigations. *Digital Investigation*, 2(3), pp. 189-192.

- Mason, S. (2010). *Electronic Evidence* (2nd ed.): LexisNexis Butterworth.
- Mason, S. (Ed.). (2008). *International Electronic Evidence*. London: British Institute of International and Comparative Law.
- Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, 6(3), pp. 175-183. doi: 10.1007/s10676-004-3422-1
- Mattson, C. L., Campbell, R. T., Bailey, R. C., Agot, K., Ndinya-Achola, J. O., & Moses, S. (2008). Risk Compensation Is Not Associated with Male Circumcision in Kisumu, Kenya: A Multi-Faceted Assessment of Men Enrolled in a Randomized Controlled Trial. *PLoS ONE*, 3(6), pp. e2443. doi: 10.1371/journal.pone.0002443
- Mauldin, E., & Arunachalam, V. (2002). An Experimental Examination of Alternative Forms of Web Assurance for Business-to-Consumer e-Commerce. *Journal of Information Systems*, 16(1), pp. 33-54.
- May, C. (2007). *Digital rights management: The problem of expanding ownership rights*: Elsevier.
- McBeth, A. (2004). Privatising Human Rights: What Happens to the State's Human Rights Duties When Services are Privatised. *Melb. J. Int'l L.*, 5, pp. 133.
- McCarthy, J. (1999). TRUSTe Decides Its Own Fate Today, *Slashdot*. Retrieved from <http://slashdot.org/yro/99/11/05/1021214.shtml>
- McClurg, A. J. (2000). Armed and Dangerous: Tort Liability for the Negligent Storage of Firearms. *CONNECTICUT LAW REVIEW*, 32, pp. 1189-1246.
- McDowell Steve, S. G. (Producer). (2005). Pacifica – Next Generation Architecture for Efficient Virtual Machines. Retrieved from http://developer.amd.com/wordpress/media/2012/10/WinHEC2005_Pacifica_Virtualization.pdf
- McIntyre, T. (2012). Child abuse images and cleanfeeds: Assessing Internet blocking systems. *RESEARCH HANDBOOK ON GOVERNANCE OF THE INTERNET*, Ian Brown, ed., Edward Elgar, pp. 277-309.
- McKenzie, M. (2009). Software Liability Laws: Thinking The Unthinkable. Retrieved from <http://www.informationweek.com/news/smb/ebusiness/229206517>
- McKnight, D. H., & Chervany, N. L. (2001). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International journal of Electronic Commerce*, 6(2), pp. 35-59.
- McMahon, M. (1992). Dangerousness, confidentiality, and the duty to protect. *Australian Psychologist*, 27(1), pp. 12-16.
- Mendelson, D. (1994). The law of torts *Deakin Law Review*, pp. 255 - 260.
- Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of applied cryptography*. United States: CRC Press (Boca Raton).
- Meuleman, L. (2008). *Public management and the metagovernance of hierarchies, networks and markets: the feasibility of designing and managing governance style combinations*: Springer Science & Business Media.

- Meyer, T. (2012). Graduated response in France: The clash of copyright and the internet. *Journal of Information Policy*, 2, pp. 107-127.
- Meyers, M., & Rogers, M. (2004). Computer forensics: the need for standardization and certification. *International Journal of Digital Evidence*, 3(2), pp. 1-11.
- Microsoft. (2008, October 2008). Deployment Planning for BitLocker Drive Encryption for Windows Vista. from <https://technet.microsoft.com/en-us/library/dd126731.aspx>
- Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12), pp. 65-74.
- Misztal, B. (2013). *Trust in modern societies: The search for the bases of social order*: John Wiley & Sons.
- Mitchell, C. J. (2008). What is Trusted Computing? In C. J. Mitchell (Ed.), *Trusted Computing* (Vol. 6, pp. 1-10). London, UK: The Institution of Engineering and Technology (IET).
- Mnookin, J. L. (2001). Fingerprint evidence in an age of DNA profiling. *Brook. L. Rev.*, 67, pp. 13.
- Moohr, G. S. (2004). Defining Overcriminalization Through Cost-Benefit Analysis: The Example of Criminal Copyright Laws. *Am. UL Rev.*, 54, pp. 783.
- Moore, R. (2008). Towards a theory of digital preservation. *International Journal of Digital Curation*, 3(1), pp. 63-75.
- Mueller, M., Kuehn, A., & Santoso, S. M. (2012). Policing the network: Using DPI for copyright enforcement. *Surveillance & Society*, 9(4), pp. 348-364.
- Muir, A. (2013). Online copyright enforcement by Internet Service Providers. *Journal of Information Science*, 39(2), pp. 256-269. doi: 10.1177/0165551512463992
- Mulligan, D., & Perzanowski, A. K. (2008). The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident. *Berkeley Technology Law Journal*, 22, pp. 1157.
- Mulligan, D. K., Han, J., & Burstein, A. J. (2003). *How DRM-based content delivery systems disrupt expectations of personal use*. Paper presented at the Proceedings of the 3rd ACM workshop on Digital rights management (pp. 77-89), ACM.
- Mutz, D. C. (2005). Social Trust and E-Commerce: Experimental Evidence for the Effects of Social Trust on Individuals' Economic Behavior. *Public Opinion Quarterly*, 69(3), pp. 393-416. doi: 10.1093/poq/nfi029
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, pp. 47-66.
- Nagurney, A., & Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS: Economic*

- Research and Electronic Networking*, pp. 1-22. doi: 10.1007/s11066-015-9094-7
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Neisse, R., Holling, D., & Pretschner, A. (2011). *Implementing Trust in Cloud Infrastructures*. Paper presented at the Proceedings of the 2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.
- NetMarketShare. (2016). Desktop Operating System Market Share. from <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>
- Newitz, A. (2005). Dangerous Terms - A User's Guide to EULAs. *Electronic Frontier Foundation (EFF) - Defending Freedom in the Digital World*. from <http://www.eff.org/wp/eula.php>
- News, B. (2013). Profile: Cleveland abductor Ariel Castro, *BBC News*. Retrieved from <http://www.bbc.com/news/world-us-canada-22444882>
- Nguyen, T. (1996). Cryptography, Export Controls, and the First Amendment in *Bernstein v. United States Department of State*. *Harv. JL & Tech.*, 10, pp. 667.
- Nieland, A. E. (2006). National security letters and the amended PATRIOT Act. *Cornell L. Rev.*, 92, pp. 1201.
- Nimmer, M. B. (1969). Does copyright abridge the first amendment guarantees of free speech and press? *UCLA L. Rev.*, 17, pp. 1180 - 1204.
- Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*: Cambridge University Press.
- Nowey, T., & Federrath, H. (2007). *Collection of Quantitative Data on Security Incidents*. Paper presented at the Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on (pp. 325-334),IEEE.
- Odom, M. D., Kumar, A., & Saunders, L. (2002). Web Assurance Seals: How and Why They Influence Consumers' Decisions. *Journal of Information Systems*, 16(2), pp. 231-250.
- Olsen, J. P. (2006). Maybe It Is Time to Rediscover Bureaucracy. *Journal of Public Administration Research and Theory*, 16(1), pp. 1-24. doi: 10.1093/jopart/mui027
- Oppliger, R., & Rytz, R. (2005). Does Trusted Computing Remedy Computer Security Problems? *IEEE Security and Privacy*, 3(2), pp. 16-19. doi: <http://dx.doi.org/10.1109/MSP.2005.40>
- Organisation for Economic Co-operation and Development. (2005). Scoping Study for the Measurement of Trust in the Online Environment *Working Party on Indicators for the Information Society*: Organisation for Economic Co-operation and Development.
- Organisation for Economic Co-operation and Development. (2008). Measuring Security and Trust in the Online Environment: A View Using Official Data.

- In t. a. i. c. f. i. Directorate for science, computer and communications policy (Ed.), *Working Party on Indicators for the Information Society*: Organisation for Economic Co-operation and Development.
- Pacini, C., & Sinason, D. (1999). Auditor Liability for Electronic Commerce Transaction Assurance: The CPA/CA Webtrust. *American Business Law Journal*, 36(3), pp. 479.
- Pagallo, U. (2015). Good onlife governance: On law, spontaneous orders, and design *The Onlife Manifesto* (pp. 161-177): Springer.
- Palmer, J. W., Bailey, J. P., & Faraj, S. (2000). The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements. *Journal of Computer-Mediated Communication*, 5(3), pp. 0. doi: 10.1111/j.1083-6101.2000.tb00342.x
- Parsons, T. (1967). Durkheim's contribution to the theory of integration of social systems *Sociological theory and modern society* (pp. 3-34). New York: Free Press.
- Paulsen, M. G. (1961). The exclusionary rule and misconduct by the police. *The Journal of Criminal Law, Criminology, and Police Science*, pp. 255-265.
- Pearson, S. (2002). *Trusted Computing Platforms, the Next Security Solution*: Prentice Hall PTR.
- Pearson, S. (2005, 23-26 May 2006). *Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy*. Paper presented at the Proceedings of the Trust Management: Third International Conference, iTrust 2005, Paris, France (pp. 305-320), Springer-Verlag GmbH.
- Peguera, M. (2008). When the cached link is the weakest link: search engine caches under the Digital Millennium Copyright Act. pp. 1102-1157.
- Peguera, M. (2009). The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems. *Columbia Journal of Law & the Arts*, 32, pp. 481.
- Peltzman, S. (1975). The Effects of Automobile Safety Regulation. *Journal of Political Economy*, 83(4), pp. 677-725. doi: 10.2307/1830396
- Peppet, S. R. (2011). Freedom of contract in an augmented reality: The case of consumer contracts. *UCLA L. Rev.*, 59, pp. 676-745.
- Perahia, A., Dwoskin, S., & Goldman, L. (2013). Intellectual Property Crimes. *Am. Crim. L. Rev.*, 50, pp. 1199-1244.
- Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in Computing* (4th ed.). Upper Saddle River, NJ, USA: Prentice Hall PTR.
- Phillips, A., & Nance, K. L. (2010). *Computer Forensics Investigators or Private Investigators: Who Is Investigating the Drive?* Paper presented at the Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on (pp. 150-157), IEEE.
- Phillips, D. E. (1994). When Software Fails: Emerging Standards of Vendor Liability Under the Uniform Commercial Code. *The Business Lawyer*, 50(1), pp. 151-181.

- Phillips, R. O., Fyhri, A., & Sagberg, F. (2011). Risk Compensation and Bicycle Helmets. *Risk Analysis*, 31(8), pp. 1187-1195. doi: 10.1111/j.1539-6924.2011.01589.x
- Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, Measurement, Disinfection & Defence. In G. Hogben (Ed.), *ENISA's Emerging and Future Risk programme* (pp. 153): European Network and Information Security Agency (ENISA).
- Posner, E. A. (2003). Economic analysis of contract law after three decades: Success or failure? *Yale Law Journal*, pp. 829-880.
- Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2014). Digital Evidence Cabinets: A Proposed Frameworks for Handling Digital Chain of Custody. *Int. J. Comput. Appl*, 109(9), pp. 30-36.
- Proudlar, G. (2005). Concepts of trusted computing. In C. J. Mitchell (Ed.), *Trusted Computing* (Vol. 6, pp. 11-27). London, UK: The Institution of Engineering and Technology (IET).
- Proudlar, G., Chen, L., & Dalton, C. (2014). Futures for Trusted Computing *Trusted Computing Platforms* (pp. 21-36): Springer International Publishing.
- Proudlar, G., Chen, Liqun, Dalton, Chris. (2014). *Trusted Computing Platforms: TPM2.0 in Context* (1 ed.): Springer International Publishing.
- Quine, W. V. O. (1960). *Word & Object*. Cambridge: The MIT Press.
- Quinn, K. (2001). Computer Evidence in Criminal Proceedings: Farewell to the Ill-Fated s.69 of the Police and Criminal Evidence Act 1984. *Int'l J. Evidence & Proof*, 5, pp. 174 - 187.
- Quint, P. E. (1989). Free speech and private law in German constitutional theory. *Md. L. Rev.*, 48, pp. 247.
- Rae, A., Robert, P., & Hausen, H.-L. (1994). *Software Evaluation for Certification*. New York, NY: McGraw-Hill, Inc. .
- Rajab, M. A., Zarfoss, J., Monroe, F., & Terzis, A. (2006). *A multifaceted approach to understanding the botnet phenomenon*. Paper presented at the Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, Rio de Janeiro, Brazil.
- Ratcliffe, J. H. (2012). *Intelligence-led policing*: Routledge.
- Rawlings, P. (2003). Policing before the police. *Handbook of Policing*, 2, pp. 46-72.
- Reid, J., Gonzalez Nieto, J., Dawson, E., Okamoto, E. (2003). *Privacy and Trusted Computing*. Paper presented at the Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03) (2003), Washington (pp. 383-388),IEEE.
- Reutiman, J. L. (2012). Defective Information: Should Information Be a Product Subject to Products Liability Claims. *Cornell JL & Pub. Pol'y*, 22, pp. 181.
- RFC 1122. (1989). Requirements for Internet Hosts -- Communication Layers. *1.1.2 Architectural Assumptions*, pp.

- Riegelsberger, J., & Sasse, M. A. (2000). Trust me, I'm a .com. The Problem of Reassuring Shoppers in Electronic Retail Environments. *Intermedia*, 28(4), pp.
- Rodgers, G. (1988). Reducing bicycle accidents: A reevaluation of the impacts of the CPSC bicycle standard and helmet use. *Journal of Products Liability*, 11(4), pp. 307-317.
- Roemer, R. (2003). Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer. *UCLA JL & Tech.*, 2003, pp. 8-8.
- Rosinger, C., Uslar, M., & Sauer, J. (2013). *Threat Scenarios to evaluate Trustworthiness of Multi-agents in the Energy Data Management*. Paper presented at the EnviroInfo (pp. 258-264),
- Rosteck, T. (2008). Die Trusted Computing Group. In N. Pohlmann & H. Reimer (Eds.), *Trusted Computing* (pp. 15-20): Vieweg+Teubner.
- Rowland, D., & Macdonald, E. (2005). *Information Technology Law* (Third ed.). London, UK: Cavendish Publishing.
- Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Qishi, W. (2010, 5-8 Jan. 2010). *A Survey of Game Theory as Applied to Network Security*. Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on (pp. 1-10),IEEE.
- Ruedl, G., Pocecco, E., Sommersacher, R., Gatterer, H., Kopp, M., Nachbauer, W., & Burtscher, M. (2010). Factors associated with self-reported risk-taking behaviour on ski slopes. *British Journal of Sports Medicine*, 44(3), pp. 204-206. doi: 10.1136/bjism.2009.066779
- Russia US-CCU Special Report. (2009). Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008. In J. Bumgarner & S. Borg (Eds.): US Cyber Consequences Unit.
- Ružić, L., & Tudor, A. (2011). Risk-taking Behavior in Skiing Among Helmet Wearers and Nonwearers. *Wilderness & Environmental Medicine*, 22(4), pp. 291-296. doi: <http://dx.doi.org/10.1016/j.wem.2011.09.001>
- Ryan, K. V., & Krotoski, M. L. (2012). Caution Advised: Avoid Undermining the Legitimate Needs of Law Enforcement to Solve Crimes Involving the Internet in Amending the Electronic Communications Privacy Act. *USFL Rev.*, 47, pp. 291.
- Sadeghi, A.-R. (2012). *The rise, fall and reincarnation of trusted computing*. Paper presented at the Proceedings of the seventh ACM workshop on Scalable trusted computing, Raleigh, North Carolina, USA (pp. 1-2),ACM.
- Safford, D. (2002a). Clarifying Misinformation on TCPA. *White paper*. from http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf
- Safford, D. (2002b). The Need for TCPA. from http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf
- Sallavaci, O., & George, C. (2013). New admissibility regime for expert evidence: the likely impact on digital forensics. *International Journal of Electronic Security and Digital Forensics*, 5(1), pp. 67-79.

- Saltzman, A. (1997). Suppose they sue? *U.S. News & World Report*, 123(11), pp. 68.
- Samuelson, P. (2003). DRM {and, or vs.} the Law. *Communications of the ACM*, 46(4), pp. 41-45.
- Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). *Towards trusted cloud computing*. Paper presented at the Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California.
- Saper, N. (2012). International Cryptography Regulation and the Global Information Economy. *Nw. J. Tech. & Intell. Prop.*, 11, pp. xv.
- Saxton, B. (1995). Flaws in the Laws Governing Employment References: Problems of Overdeterrence and Proposal for Reform. *Yale L. & Pol'y Rev.*, 13, pp.
- Schafer, B. (2003). *It's just not cricket-RoboCup and fair dealing in contract*. Paper presented at the Proceedings of the Law and Electronic Agents workshop (LEA'03) (pp. 33-46),
- Schafer, B. (2006). The taming of the Sleuth—problems and potential of autonomous agents in crime investigation and prosecution. *International Review of Law, Computers & Technology*, 20(1-2), pp. 63-76. doi: 10.1080/13600860600580959
- Schafer, B. (2013). Crowdsourcing and cloud sourcing CCTV surveillance. *Datenschutz und Datensicherheit - DuD*, 37(7), pp. 434-439. doi: 10.1007/s11623-013-0173-3
- Schäfer, B., & Bankowski, Z. (2000). Mistaken identities: The integrative force of private law. *The Harmonisation of European Private Law*, pp. 21-47.
- Schäfer, B., & Bankowski, Z. (2003). Emerging Legal Orders. Formalism and the Theory of Legal Integration. *Ratio Juris*, 16(4), pp. 486-505.
- Scheck, B. C. (1993). DNA and Daubert. *Cardozo L. Rev.*, 15, pp. 1959.
- Schellekens, D., Wyseur, B., & Preneel, B. (2008). Remote attestation on legacy operating systems with trusted platform modules. *Science of Computer Programming*, 74(1-2), pp. 13-22. doi: <http://dx.doi.org/10.1016/j.scico.2008.09.005>
- Schellekens, M., & Prins, C. (2006). Unreliable information on the internet: a challenging dilemma for the law. *Journal of Information, Communication and Ethics in Society*, 4(1), pp. 49 - 59.
- Schiffman, J., Moyer, T., Vijayakumar, H., Jaeger, T., & McDaniel, P. (2010). *Seeding clouds with trust anchors*. Paper presented at the Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA.
- Schlesinger, S. R. (1978). Exclusionary Rule: Have Proponents Proven That It Is a Deterrent to Police, The. *Judicature*, 62, pp. 404.
- Schneider, S. R. (1998). Combating Organized Crime in (and by) the Private Sector A Normative Role for Canada's Forensic Investigative Firms. *Journal of Contemporary Criminal Justice*, 14(4), pp. 351-367.

- Schneier, B. (2007). Schneier on Security. Retrieved from http://www.schneier.com/blog/archives/2007/01/information_sec_1.html
- Schneier, B. (2008). Software makers should take responsibility, *The Guardian*. Retrieved from <http://www.guardian.co.uk/technology/2008/jul/17/internet.security>
- Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security (TISSEC)*, 2(2), pp. 159-176.
- Schoen, S. (2003). *Trusted Computing: Promise and Risk*. Electronic Frontier Foundation. Retrieved from http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.pdf
- Schoen, S. (2005). Compatibility, competition, and control in trusted computing environments. *Inf. Secur. Tech. Rep.*, 10(2), pp. 105-119. doi: <http://dx.doi.org/10.1016/j.istr.2005.05.005>
- Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *Academy of Management Review*, 32(2), pp. 344-354. doi: 10.5465/amr.2007.24348410
- Schultheis, N. (2015). Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry. *Brook. J. Corp. Fin. & Com. L.*, 9(2), pp. 661.
- Scott, M. (2005). Safe Harbors Under the Digital Millennium Copyright Act. *NYU Legis. & Pub. Pol'y*, 9, pp. 99.
- Scott, R. E. (1999). Case for Formalism in Relational Contract, *The. Nw. UL Rev.*, 94, pp. 847.
- Shapiro, S. P. (1987). The Social Control of Impersonal Trust. *American Journal of Sociology*, 93(3), pp. 623-658. doi: citeulike-article-id:6111856
- Shearing, C. D., & Stenning, P. C. (1981). Modern Private Security: Its Growth and Implications. *Crime and Justice*, 3, pp. 193-245.
- Shiffrin, S. V. (2000). Paternalism, unconscionability doctrine, and accommodation. *Philosophy & Public Affairs*, 29(3), pp. 205-250.
- Shiple, T. G. (2007). Collecting Legally Defensible Online Evidence. pp. 1-25.
- Shirey, R. (2000). *RFC2828: Internet Security Glossary*: RFC Editor.
- Simonite, T. (2012). The Antivirus Era Is Over, *MIT Technology Review*. Retrieved from <http://www.technologyreview.com/news/428166/the-antivirus-era-is-over/>
- Singleton, S. (2003). Sale and Supply. *ITLT*, 11.2(11), pp.
- Skepys, B. (2012). Is There a Human Right to the Internet. *J. Pol. & L.*, 5, pp. 15.
- Skopic, K. E. (1986-1987). Potential Employer Liability for Employee References. *University of Richmond Law Review*, 21, pp. 28.
- sKyWIper Analysis Team. (2012). sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks (Vol. v1.05): Laboratory of Cryptography and System Security (CrySyS Lab)

- Slobogin, C. (2000). Empirically Based Comparison of American and European Regulatory Approaches to Police Investigation, *An. Mich. J. Int'l L.*, 22, pp. 423.
- Smith, S. A. (2004). *Contract theory*. Oxford: Oxford University Press.
- Snodgrass, R. T., Yao, S. S., & Collberg, C. (2004). *Tamper detection in audit logs*. Paper presented at the Proceedings of the Thirtieth international conference on Very large data bases - Volume 30, Toronto, Canada.
- Sosis, R. (2000). Religion and Intragroup Cooperation: Preliminary Results of a Comparative Analysis of Utopian Communities. *Cross-Cultural Research*, 34(1), pp. 70-87. doi: 10.1177/106939710003400105
- Sperber, A. J. (1997-1998). When Nondisclosure Becomes Misrepresentation: Shaping Employer Liability for Incomplete Job References. *University of San Francisco Law Review*, 32(405), pp. 28.
- Stallman, R. (2002). Can you trust your computer?, *NewsForge-The Online Newspaper for Linux and OpenSource*. Retrieved from <http://www.newsforge.com/business/02/10/21/1449250.shtml?tid=19>
- Stallman, R. (2002). Can you trust your computer? *NewsForge-The Online Newspaper for Linux and OpenSource*. <http://www.zelig.org/business/02/10/21/1449250.shtml%3Ftid=19.html>
- Stats, I. W. (2009). Usage and Population Statistics. from <http://www.internetworldstats.com/stats.htm>
- Stoughton, S. (2015). Evidentiary Rulings as Police Reform. *U. Miami L. Rev.*, 69, pp. 429-519.
- Streff, F. M., & Geller, E. S. (1988). An experimental test of risk compensation: Between-subject versus within-subject analyses. *Accident Analysis & Prevention*, 20(4), pp. 277-287. doi: [http://dx.doi.org/10.1016/0001-4575\(88\)90055-3](http://dx.doi.org/10.1016/0001-4575(88)90055-3)
- Strogatz, S. H. (2001). Exploring complex networks. *Nature*, 410(6825), pp. 268-276.
- Summers, R. S. (1968). " Good Faith" in General Contract Law and the Sales Provisions of the Uniform Commercial Code. *Virginia Law Review*, pp. 195-267.
- Sutton, S. G., Young, R., & McKenzie, P. (1995). An analysis of potential legal liability incurred through audit expert systems. *Intelligent Systems in Accounting, Finance and Management*, 4(3), pp. 191-204.
- Swerdlow, J. (1990-1991). Negligent Referral: A Potential Theory for Employer Liability. *Southern California Law Review*, 64, pp. 30.
- Swire, P. P. (2001). What should be hidden and open in computer security: lessons from deception, the art of war, law, and economic theory. *arXiv preprint cs/0109089*, pp. 1-54.

- Symantec. (2012). Internet Security Threat Report. In P. Wood (Ed.), (2012 ed.): Symantec Corporation World Headquarters.
- Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, 24(1), pp. 37-59. doi: <http://dx.doi.org/10.1016/j.jaccpubpol.2004.12.003>
- TCG. (2003). TPM - Part 1 Design Principles, Specification v.1.2 (Revision 62 ed.).
- TCG. (2005). TCG Infrastructure Working Group Reference Architecture for Interoperability (Part I) v1.0 (Revision 1.0 ed.).
- TCG. (2006a). Membership. Retrieved 4th May, 2011, from http://www.trustedcomputinggroup.org/about_tcg/tcg_members
- TCG. (2006b). Membership Levels. Retrieved 4th May, 2011, from http://www.trustedcomputinggroup.org/join_now/
- TCG. (2006c). More Secure Computing TCG.
- TCG. (2006d). TCG Infrastructure Working Group Architecture Part II - Integrity Management v1.0. In T. Hardjono (Ed.), (Revision 1.0 ed.).
- TCG. (2007). TCG Credential Profiles v 1.1 *For TPM Family 1.2; Level 2* (Revision 1.014 ed.).
- TCG. (2010). Trusted Computing Group. 2010, from <http://www.trustedcomputinggroup.org/>
- TCG. (2011a). TCG Infrastructure Working Group Core Integrity Schema Specification v 2.0 (Revision 5 ed.).
- TCG. (2011b). TCG Infrastructure Working Group Integrity Report Schema Specification v 2.0 (Revision 5 ed.).
- Terry, N. P. (2000). Rating the "Raters": Legal Exposure of Trustmark Authorities in the Context of Consumer Health Informatics. *Journal of Medical Internet Research*, 2(3), pp. doi: 10.2196/jmir.2.3.e18
- Teubner, G. (1983). Substantive and Reflexive Elements in Modern Law. *Law & Society Review*, 17(2), pp. 239-285. doi: 10.2307/3053348
- Teubner, G. (1997). Breaking Frames: The Global Interplay of Legal and Social Systems. *The American Journal of Comparative Law*, 45(1), pp. 149-169. doi: 10.2307/840962
- The Economist. (2015). Blockchains: The great chain of being sure about things. *The trust machine*, pp.
- Thompson, D. C., Thompson, R. S., & Rivara, F. P. (2001). Risk compensation theory should be subject to systematic reviews of the scientific evidence. *Injury Prevention*, 7(2), pp. 86-88. doi: 10.1136/ip.7.2.86
- Thorvaldsen, Ø. E. (2006). *Geographical Location of Internet Hosts using a Multi-Agent System*. Norwegian University of Science and Technology.
- Tibbo, H. R. (2003). On the Nature and Importance of Archiving in the Digital Age *Advances in Computers* (Vol. Volume 57, pp. 1-67): Elsevier.
- Timberg, C., & Miller, G. (2014). FBI blasts Apple, Google for locking police out of phones. *The Washington Post*, pp. 1-7.

- Toby Constructions Products Pty Ltd. v. Computer Bar Sales Pty. Ltd [case]. (1983). 2 NSWLR 48 (pp. 288).
- Tracol, X. (2014). Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 30(6), pp. 736-746. doi: 10.1016/j.clsr.2014.09.008
- Trebilcock, M. J. (1997). *The limits of freedom of contract*: Harvard University Press.
- Trzaskowski, J. (2010). *Chapter 3 Legislation and requirements concerning Trustmarks*. In E. C. C. Denmark (Series Ed.) *E-Commerce Trustmarks in Europe* Retrieved from <http://dokumenter.forbrug.dk/forbrugereuropa/e-commerce-trustmarks-in-europe/helepubl.htm>
- Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology*, 11(2), pp. 105-112.
- Turner, J. A. (2005). Going after the Hired Guns: Is Improper Expert Witness Testimony Unprofessional Conduct or the Negligent Practice of Medicine. *Pepp. L. Rev.*, 33, pp. 275.
- Turner, M., Budgen, D., Brereton, P. (2003). Turning software into a service. *Computer -- IEEE Computer Society*, 36(10), pp. 38- 44.
- Tushnet, R. (2000). Copyright as a Model for Free Speech Law: What Copyright Has in Common with Anti-Pornography Laws, Campaign Finance Reform, and Telecommunications Regulation. *BCL Rev.*, 42, pp. 1.
- Tyler, T. R. (2002). *Trust in the law : encouraging public cooperation with the police and courts*. New York, [N.Y.]: New York, N.Y. : Russell Sage Foundation.
- U.S. DOJ. (2010). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*: Office of Legal Education Executive Office for United States Attorneys.
- UK Cabinet Office and National security and intelligence. (2011). *The Cost of Cyber Crime - full report*. UK: Detica Limited.
- Ukil, A., Sen, J., & Koilakonda, S. (2011, 4-5 March 2011). *Embedded security for Internet of Things*. Paper presented at the Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on (pp. 1-6),IEEE.
- Underhill, K. (2013). Study designs for identifying risk compensation behavior among users of biomedical HIV prevention technologies: Balancing methodological rigor and research ethics. *Social Science & Medicine*, 94(0), pp. 115-123. doi: <http://dx.doi.org/10.1016/j.socscimed.2013.03.020>
- Van Brakel, R., & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Technology-led policing*, 20, pp. 165.

- Van der Meulen, N. S., & Lodder, A. R. (2012). From Neutral Thirds to Private Law Enforcers: Toward a Criterial Framework for Requests Placed on Internet Service Providers (pp. 1-18). Vrije University of Amsterdam
- Van Eeten, M. J., & Bauer, J. M. (2008). Economics of malware: Security decisions, incentives and externalities: OECD Publishing.
- Vaughan-Nichols J. S. (2003). How Trustworthy is Trusted Computing? *IEEE Computer Society Press*, 36 (3), pp. 18-20.
- Verkerke, J. H. (1998). Legal Regulation of Employment Reference Practices. *The University of Chicago Law Review*, 65(1), pp.
- Virvilis, N. (2015). Advanced Persistent Threats: The Empire Strikes Back! , pp. 16-19.
- Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013). *Trusted Computing vs. Advanced Persistent Threats: Can a Defender Win This Game?* Paper presented at the Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC) (pp. 396-403),IEEE.
- Vishik, C., Sheldon, F., & Ott, D. (2013). Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment. In H. Reimer, N. Pohlmann & W. Schneider (Eds.), *ISSE 2013 Securing Electronic Business Processes* (pp. 133-147): Springer Fachmedien Wiesbaden.
- Voas, J., McGraw, G., Kassab, L., & Voas, L. (1997). A 'crystal ball' for software liability. *Computer*, 30(6), pp. 29-36.
- Vrolix, K. (2006). Behavioral adaptation, risk compensation, risk homeostatis and moral hazard in traffic safety. *Transportation Research Institut Economics and Public Policy Report*, pp. 1-59.
- Watanabe, J. M., & Smuts, B. B. (1999). Explaining Religion without Explaining it Away: Trust, Truth, and the Evolution of Cooperation in Roy A. Rappaport's "The Obvious Aspects of Ritual". *American Anthropologist*, 101(1), pp. 98-112. doi: 10.2307/683344
- Waters, D., & Garrett, J. (1996). *Preserving Digital Information. Report of the Task Force on Archiving of Digital Information*: ERIC.
- Weinrib, E. J. (1993). Jurisprudence of Legal Formalism, The. *Harv. JL & Pub. Pol'y*, 16, pp. 583.
- Weinrib, E. J. (1995). *The idea of private law*. Cambridge, Mass.: Cambridge, Mass. : Harvard University Press.
- Weitzenböck, E. M. (2001). Electronic agents and the formation of contracts. *International Journal of Law and Information Technology*, 9(3), pp. 204-234.
- Weitzenböck, E. M. (2004). Good faith and fair dealing in contracts formed and performed by electronic agents. *Artificial intelligence and law*, 12(1-2), pp. 83-110.

- Wendel, P. T. (2004-2005). The Evolution of the Law of Trustee's Powers and Third Party Liability for Participating in a Breach of Trust: An Economic Analysis. *Seton Hall L. Rev.*, 35, pp. 971 - 1028.
- Wexler, R. (2014). Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders. pp. 158-179.
- Wheate, R. M., & Jamieson, A. (2009). A Tale of Two Approaches-The NAS Report and the Law Commission Consultation Paper on Forensic Science. *International Commentary on Evidence*, 7(2), pp.
- White, A. (2014, Apr 8, 2014). EU Data-Retention Law Tramples on Privacy, Top Court Says, *Bloomberg*. Retrieved from <http://www.bloomberg.com/news/2014-04-08/eu-data-retention-law-tramples-on-privacy-top-court-says.html>
- Wikipedia. (2011, 16/7/2011). Botnet. Retrieved 28/6/2011, 2011, from http://en.wikipedia.org/wiki/Botnet#Types_of_attacks
- Wilkey, M. R. (1978). Exclusionary Rule: Why Suppress Valid Evidence, *The Judicature*, 62, pp. 214.
- Williams, J. W. (2005). Reflections on the Private Versus Public Policing of Economic Crime. *The British Journal of Criminology*, 45(3), pp. 316-339. doi: 10.1093/bjc/azh083
- Williamson, O. E. (1993). Calculativeness, trust, and economic organization. *Journal of Law and Economics*, pp. 453-486.
- Wilson, N. L., Xiong, W., & Mattson, C. L. (2014). Is sex like driving? HIV prevention and risk compensation. *Journal of Development Economics*, 106(0), pp. 78-91. doi: <http://dx.doi.org/10.1016/j.jdeveco.2013.08.012>
- Wolfe, D. (2000). Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption, *The Emory LJ*, 49, pp. 711.
- Woodford, C. (2004). Trusted Computing or Big Brother? Putting the Rights back to Digital Rights Management. *U. Colo. L. Rev.*, 75, pp. 253-300.
- Wright, J. D. (2011). Does Antitrust Enforcement in High Tech Markets Benefit Consumers? Stock Price Evidence from *FTC v. Intel*. *Review of Industrial Organization*, 38(4), pp. 387-404. doi: 10.1007/s11151-011-9297-5
- Xia Yu and Matthew Murphy, M. G. (2011). The Regulation of Encryption Products in China. *Bloomberg Law Reports - Asia Pacific*, 4(2), pp. 1-6.
- Yeung, K. (2008). Towards an Understanding of Regulation by Design. In K. Yeung (Ed.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 79-108). Oxford: Hart.
- Yeung, K., & Dixon-Woods, M. (2010). Design-based regulation and patient safety: a regulatory studies perspective. *Social Science & Medicine*, 71(3), pp. 502-509.
- Yung, M. (2003). *Trusted Computing Platforms: The Good, the Bad, and the Ugly*. Paper presented at the 7th International Conference, FC 2003, Guadeloupe, French West Indies (pp. 250-254), Springer.

- Zhidong, S., Li, L., Fei, Y., & Xiaoping, W. (2010, 11-12 May 2010). *Cloud Computing System Based on Trusted Computing Platform*. Paper presented at the Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on (pp. 942-945),
- Zhu, C. W. (2013). 'Copyleft' Reconsidered Why Software Licensing Jurisprudence Needs Insights from Relational Contract Theory. *Social & Legal Studies*, 22(3), pp. 289-308.
- Zhu, L., Zhang, Z., Liao, L., & Guo, C. (2012). A Secure Robust Integrity Reporting Protocol of Trusted Computing for Remote Attestation under Fully Adaptive Party Corruptions. In Y. Zhang (Ed.), *Future Wireless Networks and Information Systems* (Vol. 143, pp. 211-217): Springer Berlin Heidelberg.
- Zimmermann, P. R. (1995). *The official PGP user's guide*: MIT Press.
- Zimmermann, R., & Whittaker, S. (2000). *Good faith in European contract law*: Cambridge University Press.
- Zingales, N. (2012). *Digital Copyright, 'Fair Access' and the Problem of DRM Misuse*. Paper presented at the Boston College Intellectual Property & Technology Forum (pp. 1-36),
- Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven [Conn.]: New Haven Conn. : Yale University Press.