Beyond terrorism: data collection and responsibility for privacy

Cynthia M. Gayton
School of Engineering and Applied Sciences, George Washington University, Washington, DC, USA

Abstract

Purpose – The purpose of this paper is to examine privacy rights and the relationship between those rights and business and government interests in data collected from individuals.

Design/methodology/approach – This paper approaches legal issues from the perspective of the consumer or citizen.

Findings – While conducting research for this paper, it was found that the issues facing the citizenry on privacy protection have been addressed extensively in the not too distant past. The distinguishing characteristic is the speed with which data can be collected and disseminated and the infinitely more vast amount of personal data being collected not only by the government and businesses with whom consumers conduct transactions, but also by independent data brokers.

Originality/value – Privacy rights are ephemeral and difficult to measure. Businesses, therefore, appear to have difficulty determining the value of protecting consumers' privacy. Additionally, governments from which citizens derive many social services accumulate substantial personal information given in exchange for those services. Businesses and governments are increasingly negligent in protecting the data collected on individuals, which has been revealed by a series of reported data breaches, disclosures, thefts, and surveillance activities. This paper addresses the inherent value in protecting the privacy interests of individuals and proposes that more robust privacy laws, derived from established tort law, be developed and used by concerned persons.

Keywords Data collection, Law, Privacy, Human rights, Knowledge management, Consumers

Paper type Conceptual paper

Recent headlines capture it all: "Concerns raised over AT&T privacy policy," "List of data breaches grows," "AOL technology chief, two others leave after data-privacy breach," "NSA has massive database of Americans' phone calls," and "Bush officials defend financial monitoring." The list goes on. The knowledge-economy is in the throes of its own success, feeding a knowledge acquisition frenzy[1]. While the data breaches by the government and industry may seem unrelated at first blush because the parties' interests appear dissimilar, the failure of either adequately to secure and protect essentially captive participants' personal data reflects an increasing indifference to the welfare of customers and citizens.

In a previous article, "Legal issues for the knowledge economy in the twenty-first century" (Gayton, 2006), I identified privacy as a necessary ingredient for a prosperous economy. Little by little, seemingly insignificant pieces of data are being collected by not only the government entities and companies with whom consumers conduct business, but third party data brokers. This article is about information privacy and will address the commodity interest in personal information which can be transferred

VINE: The journal of information and knowledge management systems
Vol. 36 No. 4, 2006
pp. 377-394

0305-5728
DOI 10.1108/03055720610716647

to others for purposes about which individuals are uninformed and oftentimes to which they have not consented. I will set forth the proposition that strong privacy practices encourage the trust necessary to build a sound economy and a responsible government.

Initially, I will discuss some general privacy concerns and will outline the specific definition of privacy used for the balance of the article. Next, I will point out the benefits of privacy. The government's interest in and legal restrictions on infringement of privacy rights, cover the next sections, especially as it relates to the government's interest in monitoring terrorist activity. I will examine businesses interest in and responsibility to its customers over the following sections, as well as the government's responsibility for protecting privacy. Finally, I will suggest a solution for consumers and citizens to protect privacy interests under existing tort laws and conclude with what will hopefully be a convincing assertion that privacy protection enhances the welfare of the economy and reinforces good citizenship.

I. What is privacy?

According to Aristotle, privacy is a basic human desire. Because much of what is considered human behavior necessarily occurs away from the public view, a society that encourages privacy also encourages virtue, which was, to Aristotle, the ultimate goal of human society. Hence, "[b]y way of law, ruling, and education, the public should provide opportunities and resources to cultivate virtue. By facilitating the forming of families, ... a regime encourages kinship...; by allowing a free market, it invites citizens to cultivate judgment and self-restraint; and by furnishing a liberal arts education, it promotes moral and intellectual virtue" (Swanson, 1992, pp. 3-4). In other words, allowing families and other domestic arrangements the freedom to prepare its members for interaction with the public at large, e.g. by encouraging education, participation in civic activities, practicing religion, and respecting authority, the public will reap the fruits of such a healthy domestic environment. In Aristotle's view, privacy does not mean to conduct oneself in a manner which would otherwise be abhorrent to society, but rather, to encourage behavior that would benefit the public, e.g. learn virtuous behavior[2].

Privacy assumes a prominent role in a knowledge society:

> The human right to privacy assumes a new role and new meaning in the Knowledge Society ... [I]t is important to stress the existence of links among privacy, creativity and development of tacit knowledge. It is in private that people can reflect most usefully on their experiences and on the experiences of others. It is in private that for various cultural reasons people feel safe to experiment with that reflection, test ideas and come to lasting conclusions. It is in private that people play out their most personal emotions and relationships. Privacy is important for creativity and for building up the reservoir of tacit knowledge. Therefore, it must be in the interest of the Knowledge Society to carefully treat and protect the human right to privacy (Szeremeta, 2005, p. 56).

For my purposes, I am going to use the definition of privacy set forth in an essay by Samuel Warren and Louis Brandeis "The right to privacy," of 1890, which, I think, will capture the essence of Szeremeta's view, with an additional twist: The privacy right is a right to control information about oneself after which "include[s] protection against unwarranted searches, eavesdropping, surveillance, and appropriation and misuses of one's communications" (*Stanford Encyclopedia of Philosophy*, 2002).

II. Benefits of privacy

As mentioned earlier, privacy is important for economic wellbeing. Specifically, the following conditions are necessary to support innovation, leading to a prosperous economy:

- an open and democratic society;
- an opportunity to live and work to achieve full creative potential; and
- privacy (Szeremeta, 2005).

Unfortunately, few individuals can avoid interfacing with record-keeping organizations, which control access to medical care, insurance, employment, and government services[3]. The interest individuals have in information being collected about them is directly related to needed services, education, voting, and jobs. Because interests between business and government coincide frequently, individuals are experiencing increasingly an erosion of what he or she would consider "private space"[4]. According to Szeremeta (2005, emphasis added):

> *[i]f this trend is not reversed, chances are that the initial collection of individually identifiable data will weaken the position and change the behaviour of individuals in their negotiations with the government and with business about the breadth of private space. This would mean an erosion of human rights. And, importantly, in the context of our analysis this would narrow the space for creativity and development of tacit knowledge.*

Privacy is so amorphous, so immeasurable, businesses may have difficulty identifying the economic benefits of robust privacy protection. Instead, businesses concentrate on protecting the intellectual assets derived from compiled customer data[5] and focus on computer hacking and data theft along with the corresponding risk management analysis instead of consumer privacy[6] (see Figure 1). Some analysts believe that information abundance demanded by information societies creates more risk[7]. Privacy policies[8] serve consumers little, especially if by merely visiting a business' site, consumers consent to the business' use of any data culled during the visit[9].

The organization Business for Social Responsibility (BSR) has identified several key developments in recent years it attributes to an increased interest in privacy:

- Rapid growth in new technology affecting privacy, e.g. internet, e-mail, radio frequency identification (RFID).
- Widespread media and public attention, e.g. Do Not Call (DNC) registry.
- Growth in government regulation.
- Growth in industry self-regulation within trade groups and the private sector (privacy officer positions).
- Competing demands, where companies have to negotiate between individuals' privacy expectations and legal obligations to protect employees and government requirements for data for reasons of national security[10].

Importantly, BSR identified several economic benefits of enhanced privacy protection and enforcement:

(1) *Protects brand image and reputation*. Organizations are beginning to publish company privacy rankings which may influence consumer purchase decisions[11].

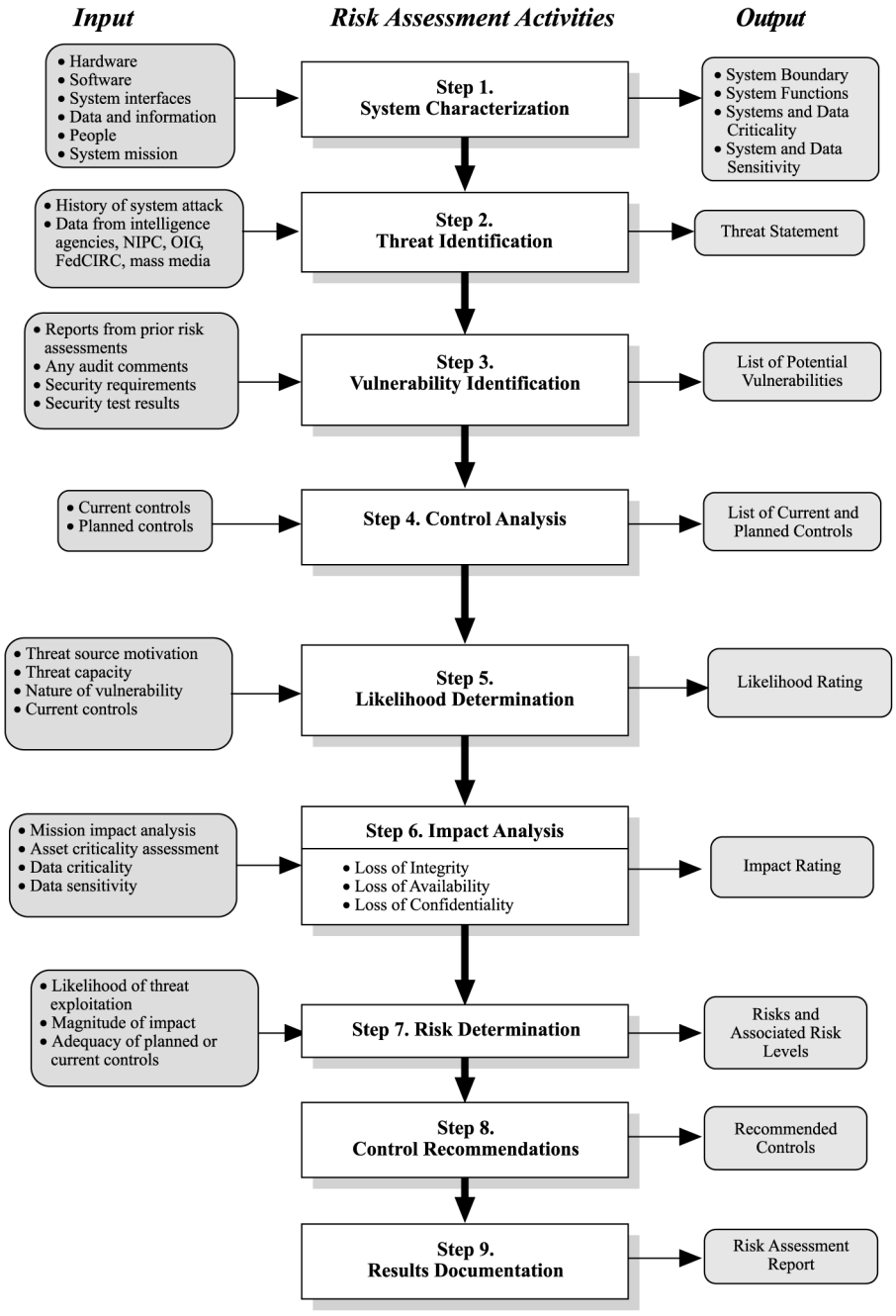

Figure 1.

Source: Stoneburner *et al.* (2002)

(2) *Enhances consumer trust and avoids consumer backlash*. BSR asserts that inadequate privacy protection practices may lead companies to lose sales due to consumers not patronizing those stores without adequate protection. Similarly, companies that rely on internet commerce may find that consumers decline to enter personal data on their sites.

(3) *Ensures compliance and avoids liabilities and fines*. The Federal Trade Commission (FTC) has stepped up enforcement and issued fines. Some companies have faced millions of dollars in liabilities for privacy infringement.

(4) *Enhances employee satisfaction*. The National Institute of Health (NIH) and the University of Wisconsin documented increased employee stress and other harmful health effects from electronic monitoring and surveillance at the workplace. Such activity hurts:
   - productivity;
   - retention; and
   - workplace morale (BSR, 2005).

Businesses are not the only entities interested in gathering information about individuals. The government is soliciting the services of businesses to buttress its existing data collection, as well as create new data from which it can derive information about the habits of its constituents most recently in response to terrorist threats.

III. Government interest in private activity

Individuals are hesitant to trust the government with personal information. In some instances, the level of trust granted is less than that of businesses, which people know secure personal information in order to make money. However, governments participate in endeavors that create commercial value, generating new meaning for the knowledge economy. Frequently, private enterprises are the beneficiaries of property rights transferred to them by the government, often via the government's financing of research and providing grants (Szeremeta, 2005, p. 60).

Ultimately, however, the government has an substantial interest in the state of its citizenry's mind[12]. This interest manifests itself most directly in providing public education. This is not as counterintuitive as it appears at first glance. Referring back to Aristotle's belief that encouraging the virtues, including increasing a citizen's knowledge, benefits the public, the government's involvement in education is logical. Moreover, the "*teaching power* is the inherent constitutional authority of the state to establish and direct the teaching activity and institutions needed to ensure its continuity and further its legitimate general and special purposes" (Tussman, 1977, p. 54).

The question is, then, how does the government cultivate useful knowledge in order to reach its goals? Indeed, "[a] polity must, if it is to continue, recruit and incorporate new members; it must provide for a fruitful life of communication; it must direct attention to its problems and cultivate the knowledge and wisdom it needs. Or it will die. There is, therefore, an overwhelming public interest in the condition of the mind, that, without exaggeration, may be regarded as the most fundamental part of the

public domain" (Tussman, 1977, pp. 10-11). Monitoring behavior is the method by which governments measure the success of its influence.

Having established that the government has an interest in the state of its citizenry's mind, how far the government and business should go in its investigation and surveillance of the mind as it relates to monitoring potential terrorist activity is discussed below.

A. Surveillance

Intelligence activity is currently focused on communication and not behavior. Several laws have been passed regulating wiretapping, access to information acquired by the government, and intelligence gathering. Recently, attention has been directed toward the methods by which the government monitors electronic communication to ascertain whether a person is planning subversive or terrorist activity. Such surveillance is subject to United States Code (USC) §2511 Title 18 and §1809-1810 of Title 50 which "provides specific criminal and civil penalties for individuals (law enforcement officials and private citizens alike) who conduct electronic or wire surveillance of communications [reference omitted] in a manner not legally authorized" (Dam and Lin, 1996).

Title III (the "Wiretap Act") of the Omnibus Crime Control and Safe Streets Act of 1968 provides for a higher standard of interception for oral and wire communications, where only certain, serious felonies may be investigated. Title III provides that "procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance ... may be conducted." Such interception may be accomplished by securing a warrant called an "intercept order" to show that other surveillance methods have failed. Because electronic surveillance can continue over a long period of time, and because it can be considered an invasion of privacy, law enforcement authorities must follow minimization procedures, which, if improperly followed, may lead to the suppression of evidence found (Dam and Lin, 1996).

The Electronic Communications Privacy Act (ECPA) amends Title III, extending Title III criminal and civil penalties for unlawful interception to electronic communications (Dam and Lin, 1996). The use of devices to collect information about origins and destinations of communications may be a criminal offense except when performed by a "law enforcement official with a court order, by a communication service provider for specified business purposes, or with the consent of the service user" (Dam and Lin, 1996).

The Privacy Act of 1974, 5 USC Section 552a, (FOIA) regulates an agency's disclosure of personal records (including surveillance records) to any person or another agency. Any employee or officer of an agency who violates FOIA disclosure provisions will be guilty of a misdemeanor and may be fined.

The Foreign Intelligence Surveillance Act was passed in direct response to the National Security Agency's receipt "from international cable companies millions of cables which had been sent by American citizens in the reasonable expectation that they would be kept private" (Church Committee, 1976, p. 12). Interception of communications is regulated by FISA only if there is a "reasonable expectation of privacy," inherent in the surveillance. Such surveillance requires a court order from FISA. The FISA court consists of United States District Court judges appointed by the Chief Justice of the Supreme Court and meets secretly two times a year in Washington,

DC (Dam and Lin, 1996). As of 1996, the FISA court has never denied a request for an order (Dam and Lin, 1996).

The Fourth Amendment and several federal and state statutes protect the right to communication privacy. The First, Fifth and Sixth amendments are invoked also in privacy actions where a defendant is being tried for a crime:

> *Amendment I*
> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people to peaceably to assemble, and to petition the Government for a redress of grievances.
>
> *Amendment IV*
> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
>
> *Amendment V*
> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject to the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall property be taken for public use, without just compensation.
>
> *Amendment VI*
> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall be committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.

As surveillance is examined more thoroughly below, it may be useful to gain an understanding of some basic features of surveillance, which, according to Zureik (2002, p. 42), are the following:

- ubiquitous in human societies and found in both public and private spheres of society;
- associated with governance and management;
- endemic to large-scale organizations;
- constitutive of the subject and has a corporeal aspect to it;
- disabling as well as enabling;
- understood in terms of distanciation, i.e. the control of space and time;
- becoming increasingly implicated in a system of assemblage which brings together diverse control technologies; and
- rhizomatic, as evident in the ability of convergent technologies to capture and assemble inordinate amounts of information about people from various sources.

B. Current surveillance activities requiring business participation

Two major surveillance activities have involved US business compliance with requests for information by the federal government. Obviously, when a business entity is under investigation by the government, that business is required to comply with discovery requests promulgated to them, or otherwise face contempt charges. In the two instances discussed below, the business entities are not under investigation, nor are their specific customers involved with pending legal action. Rather, the information is being passed on to the government in order to assist its terrorist seeking activity. The result of such activity is likely to cause a chilling effect on the exercise of the First Amendment[13].

1. Financial monitoring. A program devised after the September 11 attacks on the USA was recently revealed, disclosing the fact that the US government has obtained financial information from a database maintained by a Belgian company, SWIFTNet, which "routes 11 million financial transactions daily among 7,800 banks and other financial institutions in 200 countries" (Associated Press, 2006a). Some international banking officials were unaware of US access to information. While the consulting firm Booz Allen and Hamilton, retained to audit and review the US activities in the program, found that the government was not abusing the data, there is no guarantee that in the future the information will not be used for purposes other than those for which the subpoenas were issued to access the information in the first place. Indeed, as many as six federal agencies have experienced data breaches over the past several months[14].

State governments have not fared much better. In Florida, an auditor found that voter registration data is vulnerable to theft, corruption, unauthorized access and alteration, "despite the best efforts of elections officials" (Songini, 2006).

2. Telephone monitoring. The National Security Agency (NSA) is using data provided by AT&T, Verizon and Bell South, which provide local and wireless phone service to more than 200 million customers in order to conduct "social network analysis" to "study how terrorist networks contact each other and how they are tied together" (Cauley, 2006). The NSA domestic program is more expansive than the White House acknowledged previously. AT&T, Verizon and BellSouth are under contract with the NSA. While consumer names and addresses are not being handed over, that information can be obtained through other sources. Only one company, Qwest, refused to help the NSA, based on the concerned raised by its attorneys that disclosure of customer information may be illegal. Qwest, based in Denver, Colorado, provides service to 14 million customers in 14 states[15].

Historically, telephone companies have required law enforcement agencies to present a court order before disclosing customer data, which is required by law, Section 222 of the Communications Act. However, President Bush signed an executive order which disposed of the warrant requirement in order to engage in telephone surveillance without a warrant[16].

According to Koh (2006), the NSA program:

> [...] undermines, rather than enhances, our ability to combat terrorism through the criminal justice system. Under the ongoing NSA program NSA analysts are increasingly caught between following superior orders and carrying out illegal electronic surveillance. The nation can scarcely afford to lose analysts that are on the front lines protecting our national security. Furthermore, because evidence collected under the NSA electronic surveillance program will almost surely be challenged as illegally obtained, such evidence may prove inadmissible in

> cases against alleged terrorists, giving them greater leverage in plea bargains and making it far more difficult to prosecute them criminally.

The USA has gone down this road before[17]. As mentioned above, because of NSA's activities collecting the communications of several millions of communications by American citizens, laws were passed to ensure that such abuse wasn't tolerated again, to wit:

> Americans have rightfully been concerned … about the dangers of hostile foreign agents likely to commit acts of espionage. Similarly, the violent acts of political terrorists can seriously endanger the rights of Americans. Carefully focused intelligence investigations can help prevent such acts.
>
> But too often intelligence has lost this focus and domestic intelligence activities have invaded individual privacy and violated the rights of lawful assembly and political expression. Unless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature (Church Committee, 1976, p. 1).

As opposed to domestic intelligence gathering throughout most of our country's history (the Alien and Sedition Acts, the suspension of the writ of habeas corpus during the Civil War, deportation pursuant to the Palmer raids in the 1920s, and the incarceration of Japanese Americans during the Second World War) where the public and victims knew what was being done to them, our current "[i]ntelligence activity on the other hand, is generally covert. It is concealed from its victims (citation omitted) and is seldom described in statutes or explicit executive orders. The victim may never suspect that his misfortunes are the intended result of activities undertaken by his government, and accordingly may have no opportunity to challenge the actions taken against him" (Church Committee, 1976, pp. 2-3).

The Church Committee recommended that intelligence operations focus on imminent violence in order to avoid the "wasteful dispersion of resources". Indeed, the usefulness of the current domestic phone-call database being created by the NSA is unclear and perhaps will also be a similar wasteful dispersion[18]. The Committee also recommended clear legal standards and effective oversight to "ensure that domestic intelligence activity does not itself undermine the democratic system it is intended to protect".

To be sure, Fourth Amendment protections are at issue here. The activity outlined above flouts the intent and purpose of Congressional authority to ensure the protection of citizens' rights. The Supreme Court has spoken similarly on the issue of Fourth Amendment searches and seizures where "[i]t is not in the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property …" (*Boyd* v. *US*, 1886). Moreover, if these surveillance activities result in an arrest, the purpose of the Fourth Amendment as far as the accused is concerned, is of no value[19].

Epstein (1998) provides a more contemporary analysis of the Fourth Amendment as it applies to electronic surveillance:

> Linguistically, the coverage of "persons, houses, papers and effects" does not capture perfectly the nuances of the information age, but it takes very little tugging to see their contemporary relevance. In particular, "papers" are not protected because they are blank, but

> because of the sensitive information they contain. These records and information do not lose their protection because they are stored digitally or transferred electronically, only to regain that protection when printed out in hard copy.

The surveillance activity outlined above is not indicative of a democratic society where there is transparency and openness, but rather suspicion and guilt before a potential defendant has an opportunity to know from where the accusations are derived[20].

According to Attorney General Alberto Gonzales, the terrorist surveillance program conducted by the NSA since 9/11/2001, targets communications "where one party to the communication is outside the US and the government has 'reasonable grounds to believe' that at least one party to the communication is a member or agent of al Qaeda, or an affiliated terrorist organization" (Gonzales, 2006, p. 106). Gonzales asserts that this activity is authorized by Congress via the Authorization for Use of Military Force granted by Congress a few days after the 9/11 attacks. In addition, the Supreme Court analyzed the scope of AUMF in *Hamdi* v. *Rumsfeld* (2004), where the court stated that the AUMF authorized all necessary and appropriate force to combat the enemy. In addition, due to expediency and necessity, Gonzales stated that the President does not have time to follow FISA guidelines approved by Congress[21].

IV. Government and business responsibility to protect citizens'/customers' data

Government agencies are not entirely averse to protecting an individual's privacy. In a seminal case outlining Freedom of Information Act (FOIA) limitations , (*United States Department of Justice* et al. v. *Committee for Freedom of the Press* et al., 1989), where journalists requested, under FOIA, to obtain access to the FBI's criminal identification or rap sheet pertaining to four members of the Medico family who allegedly had obtained some defense contracts based on an arrangement with a corrupt congressman. The request was denied. Historically, the Department of Justice treated such records as confidential. The Supreme Court's point was this: FOIA's purpose is to assist the public understand activities of the government, not an individual's activities.

In the USA, all convictions and other criminal activity related materials is a matter of public record, and, therefore, available in all jurisdictions upon request. However, the availability of a compilation, or criminal history summaries is restricted in most states.

Further, in *Whalen* v. *Roe* (1977), where the Court discussed that the compilation of personal data threatens privacy, and admitted that such storage increases the potential for abuse of such data[22].

V. Solutions

My initial response to privacy and information protection abuses was to look for a property law-based solution for consumers and citizens[23]. Property rights have a broad and deep legal base from which many remedies can be derived[24]. Much like intellectual property rights, privacy rights can be seen as an "intangible" right where there is clearly a market and can be sold or licensed. On the other hand, if an individual did not want to give up privacy rights, a person could "lend" the rights to a company, and seek remedies based on bailment principles. In a bailment relationship, personal property can be entrusted by a bailor (the owner of the personal property) to a bailee

(the person to whom the bailor entrusts the personal property). Bailment principles are made up of three elements:

(1) title to the property remains with the bailor;

(2) possession of the property is completely surrendered by the bailor to the bailee; and

(3) the parties intend the return of the bailor's property at the end of the bailment period.

The amount of care given to the personal property is determined by the nature of the property involved and the purpose of the bailment. For example, a customer, in order to obtain a credit card, has to provide information about his/her income, marital status, social security number, checking and savings account information, previous credit history, etc. The information provided in this example is for the benefit of both parties and the bailee would be required to exercise ordinary care maintaining the confidential nature of that personal information. But if, as another example, similar information is provided primarily for the benefit of the bailee, great care is required. In situations absent contract language to the contrary, where the bailee was negligent in maintaining the privacy of such personal information, the bailee would be liable for any harm incurred by the bailor (see Gayton and Vaughn, 2004, pp. 306-308).

This solution would require the establishment of a personal property right in private information which is not established at this time. Moreover, and despite this property right in private information, there are simply no market mechanisms that protect privacy, ensure accuracy, or limit security breaches where there is no direct obligation to the person whose personal information is at risk, e.g. where there is a third party who is not a party to the initial agreement between the bailor and bailee? (Rotenberg, 2000).

Property solutions are also ineffective when confronted with the information broker industry, which is sometimes called "the true invisible hand of the information economy" according to Marc Rotenberg. In effect, he claims that a better way to deal with information brokers is to provide specific legislation to curtail the illicit market in personal data. Specifically, he asserts that legislators be aware that:

- Privacy breaches have real financial consequences[25].
- Market-based solutions fail because there is no direct relationship between the consumer and the data collecting organization[26].
- Current federal laws are inadequate and infrequently enforced and many information products circumvent privacy regulations[27].
- FTC pursues privacy concerns haphazardly which may produce "a loss of trust and confidence in the electronic marketplace."
- State-based approaches may be more appropriate.

In addition, Rotenberg found that personal information made available through public records has been transformed into a privatized commodity that "does little to further government oversight but does much to undermine the freedom of Americans." He is particularly concerned that "government interests are not served *when the government compels* the production of personal information, sells the information to private data

vendors, who make detailed profiles available to strangers. This is a perversion of the purpose of public records." (Rotenberg, 2000, emphasis added)[28].

So, I have come to agree with Jessica Litman's analysis that securing a tort right in personal information is the best approach. Tort law, like property law, has broad reach and depth, and it is not too far a stretch to fit privacy interests under the defamation umbrella. The tort approach may be most effective "[b]ecause it foregoes the privacy-rights-management market entirely, it is less likely to legitimize wholesale commercial exploitation of personal information." (Litman, 2000, p. 1312).

Similarly, under negligence theory, a person who believes privacy rights have been violated may be able to establish negligence, if the injured party can show the existence of a duty, a breach of such duty[29], some injury, and damages. Litman emphasizes that establishing damages is the most difficult element to prove. Even so, an injured party may be able to seek an equitable remedy, such as an injunction, preventing the party violating the privacy right from further exploiting the victim's privacy interests.

Another feature of tort law is that it requires consent, i.e. if consent is not obtained, the tort claim will stand. The anticipated result of such a privacy action under tort may be that "[d]ata collectors could use whatever method they choose to secure consumers' consent to data collection, resuse, sale, resale and so forth, subject to the understanding that courts might later evaluate that method to ascertain whether the consumers in fact appreciated and agreed to the data collectors' actions. Faced with that possibility, perhaps the data marketing industry would rethink its fair information practices" (Litman, 2000, p. 1311).

VI. Conclusion

While it appears that we are entering into a wilderness lacking respect and protection for privacy, the road has been prepared for us already. It is incumbent on thoughtful and concerned citizens to clear out the weeds on the path and in our minds to secure privacy rights despite daily fears of invasion and insecurity. These adversaries have been faced before and by asserting and securing rights to privacy, we ensure our productivity and sanity well into the twenty-first century.

This is one area where history has served us well in defense of personal rights that should be secured by our government and respected by businesses. Not everyone is called on to defend the borders, secure a nation's freedom, or relieve the burden of an ineffective government. But most of us can assert the rights to control and manage the information generated and manipulated about ourselves. Hopefully this article will encourage its readers to do so.

Notes

1. "It is, I think, rather fitting that the hard drive to inquire, the lust to know, should find itself checked and baffled by such soft notions as consent, dignity, and privacy. It has been on a long and glorious rampage. It has dispelled much ignorance and illusion, flouted orthodoxies, trampled on the sacred, defied taboo, freed itself, almost, from check by any external authority. What can withstand it? The lone, stubborn individual who doesn't care to be looked into, a sense of offended dignity, a tattered principle of privacy growing ever larger and more powerful in an impersonal world – privacy, the looming antithesis to the public and the social?" (Tussman, 1977, p. 49).
2. "If Aristotle lived in the twentieth-century Western world, he might agree with communitarian critics that disequilibrium between the public and private exists. But he

would attribute this not to citizens retreating to private life but to reserving it largely for letting go of virtue. As a consequence of their using the private in this way, the private has little to offer the public. Moreover, Aristotle would perhaps point out that the unpreparedness of people today to engage properly in private activity is in part the result of laws and educational institutions failing to encourage the proper use of privacy" (Swanson, 1992, p. 208).

3. "In a larger context, [people] must also be concerned about the long-term effect that record keeping practices can have not only on relationships between individuals and organizations, but also on the balance of power between government and the rest of society. Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. Thus, growth in society's record-keeping capability poses the risk that existing power balances will be upset" (Privacy Protection Study Commission, 1977).
4. "Historically, private business has negotiated and often enshrined in law a very advanced degree of lack of transparency. While much of this can be justified by a healthy attempt to keep the government out of private business, and by the rules of free competition, evidence suggests that the public is being short-changed by the licence that the State gives on its behalf to business, allowing it to operate in this manner ... The issue is about the right of the public to know, debate and in some way agree to the policies of business firms [whose] research agendas, product development and deployment plans, investment plans, product safety research and reports, etc. have a profound impact on human development ... Rarely do we witness a public debate about them and when it happens, as a rule it is because the issue becomes important to another (rival?) interest group. ... There is little doubt that as long as the economy is driven by individual material gain ... removing or decreasing [intellectual property rights] would undercut some ... of the motivation to create new meaning that can be converted into saleable products and services" (Szeremeta, 2005, p. 60).
5. Except, see recent case between Pennsylvania State Employees Credit Union (PSECU) against Fifth Third Bancorp where PSECU, which had to spend $100,000 to cancel and reissue 235,000 Visa cards which had been compromised at BJ's Wholesale club, claimed that BJ had an obligation to ensure that it was in compliance with Visa's security regulations. The court found that PSECU was not a third party beneficiary to the contract between Fifth Third and Visa and therefore not entitled to reimbursements (Vijayan, 2006a; *PSECU* v. *Fifth Third Bank and BJ's Wholesale Club*, 2005).
6. Indeed, the National Institute of Standards and Technology's (NIST) *Risk Management Guide for Information Technology Systems*, identifies specific human threats such as inadvertent data entry, network based attacks, malicious software upload, and unauthorized access to confidential information as a common threat-source. Recent security breachers fall outside of the usual suspects who are often disgruntled, dishonest, and poorly trained employees, particularly when AOL executives released 650,000 subscribers' internet search terms (AOL) and Ohio University's IT supervisors exposed the Social Security numbers and other personal data of 137,000 people (Vijayan, 2006b).
7. "I suggest ... that information societies are in fact 'risk societies' [where] technical innovation, the heterogeneous qualities of information, and uncertain demand for ICTs generate more risk, not less" (Winseck, 2003, p. 178).
8. "Consumer advocates said yesterday that a new privacy policy from AT&T Inc. marks the first time a major telecom company has asserted that customer calling and Internet records are corporate property and raises concerns about how the company tracks consumer behavior and shares data with government and law enforcement agencies" (Goo, 2006). AT&T's broadband internet customers are faced with an assertion of AT&T's property interest in its customer's account information, e.g. "While your account information may be personal to you, these records constitute business records that are owned by AT&T ... As

such, AT&T may disclose such records to protect its legitimate business interests, safeguard others, or respond to legal process" (Goo, 2006).

9. For example, Universal Music Group's privacy policy states: "We may share your information with other third parties with whom we have business relationships and in some cases we cannot control or know their privacy practices. *By visiting our sites*, you affirmatively consent to our collection, use, and distribution of your data." (Universal Music Group, n.d., emphasis added). Holtzman (2006) notes that he could not find "a single instance of a major company discussing when and if they will ever delete your valuable data, even after you're no longer their customer".
10. See also, Marquis (2003, p. 19): "It is no accident that interest in privacy has grown by leaps and bounds in the past decade. This shift maps exactly onto the increased levels and pervasiveness of surveillance in commercial as well as in governmental and workplace settings. By the same token, it also relates to increased surveillance of middle-class and male populations. Lower socio-economic groups and women have long been accustomed to the gaze of various surveillants. As well, growth of privacy concerns has to be seen in the context of increasing individualized societies, [cite omitted] and above all on the individualizing oof risk, as social safety nets deteriorate one by one. Information privacy, based almost everywhere on 'fair information practices,' relates to communicative control, that is, how far data subjects have a say over how their personal data are collected, processed, and used. Such privacy policies are now enshrined in law and in voluntary self-regulation in many countries and contexts".
11. The Top Ten privacy organizations based on a report published by Ponemon Institute and TrustE were eBay, American Express, Proctor & Gamble, Amazon, Hewlett-Packard, United States Postal Service, IBM, Earthlink, Citibank and Dell (BSR, 2005).
12. "It is not enough, although it is necessary, that sanity is pervasive. The public mind must be seen as the mind of the Sovereign and cultivated into fitness for the dignity of that office"(Tussman, 1977, p. 133).
13. See the Church Committee (1976, p. 17) where they committee found that "[t]he government's surveillance activities in the aggregate ... tends ... to deter the exercise of First Amended rights by American citizens who became aware of the government's domestic intelligence program".
14. The Federal Government's record in maintaining the privacy of its own employee and veterans' data has been dismal in recent months. Social security numbers and other personal data for 28,000 sailors and family members have been found on the Internet. In addition, at the Agriculture Department, a computer hacker may have obtained the Social Security numbers and photos of 26,000 Washington, DC area employees and contractors. Finally, as many as 26.5 million veterans and military troops may have been affected by the theft of a computer containing similar information. Military officials in that instances waited several weeks before notifying potentially affected veterans of the incident (Associated Press, 2006b). State governments have not fared much better. In Florida, an auditor found that voter registration data are vulnerable to theft, corruption, unauthorized access and alteration, "despite the best efforts of elections officials" (Songini, 2006).
15. It appears that Qwest's attorneys made a wise decision. On May 22, 2006, Verizon customers in Maine filed a complaint requesting that the Public Utilities Commission to investigate whether Verizon violated privacy laws by cooperating with the NSA's surveillance program. According to an article written by Wack (2006), the Bush administration has threatened to sue if Maine regulators decide to go forward with the investigation.
16. "Presidents have long contended that the ability to conduct surveillance for intelligence purposes is a purely executive function, and have tended to make broad assertions of authority while resisting efforts on the part of Congress or the courts to impose restrictions. Congress has asserted itself with respect to domestic surveillance, but has largely left

matters involving overseas surveillance to executive self-regulation, subject to congressional oversight and willingness to provide funds"(Bazan and Elsea, 2006, p. 7).

17. According to Harrow (2005, pp. 8-9), intelligence abuses are the reasons why "in the 1970s Congress shut down domestic intelligence operations that had led to so many abuses by the FBI, CIA, the US Army and others. It's also why it passed information and privacy laws. These not only restricted how the government could collect and use information about citizen. They required agencies to be more open. The new legal authorities and the government's partnership with private information companies now pose a direct threat to this three-decade-old effort toward openness. It's a simple fact that private companies can collect information about people in ways the government can't. At the same time, they can't be held accountable for their behavior or their mistakes the way government agencies can. Their capabilities have raced far ahead of the nation's understanding and laws. The legacy of these efforts will be with us for many years".
18. "The usefulness of the NSA's domestic phone-call database as a counterterrorism tool is unclear. Also unclear is whether the database has been used for other purposes" (Cauley, 2006).
19. "If letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the 4th amendment, declaring his right to be secure against such searches and seizers, is of no value, and, so far as those thus placed are concerned, might as well be stricken from the Constitution. The efforts of the courts and their officials to bring the guilty to punishment, praiseworthy as they are, are not to be aided by the sacrifice of those great principles established by years of endeavor and suffering which have resolved in their embodiment in the fundamental law of the land." (*Weeks* v. *US*, 1914).
20. "[T]here is, in democratic societies, a basic right to know, to be informed about what the government is doing and why. … there should be a strong presumption in favour of transparency and openness in government … secrecy … has strong adverse effects on investment and economic growth" (Stiglitz, 1999, p. 745). "At some point, the Constitution can't bear the kind of continued strains that are being imposed by the demands of the fight on terrorism", said Harold J. Krent, dean and professor of law at Kent College of Law in Chicago. "What I am worried about is that there is a potential for amassing huge databases of individuals – linked by phone records, linked by financial records – that can be kept and used without any kind of real oversight. It's frightening" (Associated Press, 2006c).
21. "In order to authorize emergency surveillance under FISA, the Attorney General must personally 'determine that … the factual basis for issuance of an order under [FISA] to approve such surveillance exists'. *FISA requires the attorney general to determine in advance that this condition is satisfied. That review process can of necessity, take precious time. And that same process takes the decision away from the officers best situated to make it during an armed conflict*" (Gonzales, 2006, p. 112, emphasis added). Exactly the point.
22. "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures" (*Whalen* v. *Roe*, 1977, pp. 605, 607).
23. "Self-regulation is an abject failure; meaningful privacy regulation appears to be untenable as a political matter; and accepting that privacy is an outmoded notion from a bygone age seems unacceptable. The proposal that has been generating the most buzz, recently, is the idea that privacy can be cast as a property right. People should own information about themselves and, as owners of property, should be entitled to control what is done with it" (Litman, 2000, p. 1287).

24. "Absent a strong claim of ownership for personal data, it will become increasingly difficult to force respectful and equitable treatment online from many companies. Congress should establish the ownership issue now, before AT&T's trial policy becomes an industry standard" (Holtzman, 2006).
25. "Consumers suffer harms both from information that is used for fraud and inaccurate information that leads to lost opportunities through no fault of the individual" (Rotenberg, 2000).
26. "The market in personal data is the problem, market solutions based on a property rights can be recognized as a matter of state common law without invoking the federal regulatory machinery, which seems too helpless, pernicious, or corrupt … to offer any meaningful solutions" (Litman, 2000, p. 1303).
27. "We don't quite have the laws yet that make people liable for security as a matter of statutory law" according to Ethan Preston of Kambert & Associates, LLC law firm. "It's unfortunate, because there is a lot of harm that can be caused because of negligent security" (Vijayan, 2006a).
28. A recent example is the data collected pursuant to the Help America Vote Act (HAVA) which requires that ever state create a centralized voter information repository to protect against computer fraud. A committee formed by the Association for Computing Machinery, examined the state of voter registration databases and concluded that lacked adequate security measures (Songini, 2006, p. 12).
29. "The fact that businesses respond to consumer privacy complaints with defensive apologies rather than toughing it out suggest that [the perception that the trafficking of personal information is a breach of confidence] is one businesses are aware of, intentionally cultivate and may even to some extent share" (Litman, 2000, p. 1309).

References

Associated Press (2006a), "Bush officials defend financial monitoring", *The Journal*, p. A3.

Associated Press (2006b), "Sailors' data, Social Security, found on internet", *The Journal*, p. A3.

Associated Press (2006c), "Some question expansion of presidential power", *The Journal*, p. A3, available at: www.journal-news.net/custserv/index.asp.

Bazan, E. and Elsea, J. (2006), "Presidential authority to conduct warrantless electronic surveillance to gather foreign intelligence information", Congressional Research Service memorandum.

Boyd v. *US* (1886), 116 US 616.

Business for Social Responsibility (BSR) (2005), "BSR issue briefs: privacy (consumer and employee)",available at: www.bsr.org/CSRResources/IssueBriefDetail.cfm?DocumentID=50970 (accessed June 20, 2006).

Cauley, L. (2006), "NSA has massive database of Americans' phone calls", *USA Today*, available at: www.usatoday.com/news/washington/2006-05-10-nsa-x.htm (accessed June 14, 2006).

Church Committee (1976), *Intelligence Activities and the Rights of Americans. Book II, Final Report*, US Senate, Washington, DC.

Dam, K.W. and Lin, H.S. (Eds) (1996), *Cryptography's Role in Securing the Information Society*, Computer Science and Telecommunications Board, National Research Council, Washington, DC, available at: www.nap.edu/readingroom/books/crisis

Epstein, R. (1998), Testimony before the Senate Judiciary Subcommittee on the constitution, federalism and property rights.

Gayton, C. (2006), "Legal issues for the knowledge economy in the twenty-first century", *VINE*, Vol. 36 No. 1, pp. 17-26.

Gayton, C. and Vaughn, R. (2004), *Legal Aspects of Engineering*, 7th ed., Kendall-Hunt Publishing, Dubuque, IA.

Gonzales, A.R. (2006), "Prepared statement of Hon. Alberto R. Gonzales, Attorney General of the United States", February, available at: http://149.101.1.32/ag/speeches/2006/ag_speech_060206.html

Goo, S. (2006), "Concerns raised over AT&T privacy policy", *The Washington Post*, p. D5.

Hamdi v. *Rumsfeld* (2004), 542 US 507.

Harrow, R. Jr (2005), *No Place to Hide*, Simon & Schuster, New York, NY.

Holtzman, D. (2006), "Viewpoint: the privacy pirates – corporate policies on the collection and management of personal data do precious little to protect your privacy", *BusinessWeek*, available at: http://businessweek.com/print/technology/content/jul2006/tc20060724_816608.htm (accessed August 9, 2006).

Koh, H. (2006), Testimony of Professor Harold Hongju Koh, Dean, Yale Law School, before the Senate Judiciary Committee regarding wartime executive power and the National Security Agency's Surveillance Authority.

Litman, J. (2000), "Information privacy/information property", *Stanford Law Review*, Vol. 52, p. 1283.

Marquis, G. (2003), "From the 'dossier' society to database networks", *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London.

PSECU v. *Fifth Third Bank and BJ's Wholesale Club* (2005), USDC MD Pa, Case No. CV04-1554.

Privacy Protection Study Commission (1977), *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission*, US Government Printing Office, Washington, DC.

Rotenberg, M. (2000), Testimony and statement of record of Marc Rotenberg, hearing on identity theft and data broker services before the Committee on Commerce, Science and Transportation.

Songini, M. (2006), "Auditor's report criticizes Florida's voter database", *ComputerWorld*, June 26, p. 12.

Stanford Encyclopedia of Philosophy (2002), "Privacy", May 14, available at: http://plato.stanford.edu/entries/privacy (accessed June 29 2006).

Stiglitz, J. (1999), "On liberty, the right to know, and public discourse: the role of transparency in public life", Oxford Amnesty Lecture, Oxford, available at: http://siteresources.worldbank.org/NEWS/Resources/oxford-amnesty.pdf (accessed February 2, 2006).

Stoneburner, G., Goguen, A. and Feringa, A. (2002), *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology (NIST)*, United States Department of Commerce, Washington, DC, available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (accessed July 5, 2006).

Swanson, J. (1992), *The Public and the Private in Aristotle's Political Philosophy*, Cornell University Press, New York, NY.

Szeremeta, J. (2005), *Understanding Knowledge Societies*, United Nations Publishing Section, New York, NY.

Tussman, J. (1977), *Government and the Mind*, Oxford University Press, New York, NY.

United States Department of Justice et al. v. *Committee for Freedom of the Press* et al. (1989), 789 US 749.

Universal Music Group (n.d.), "Universal Music Group privacy policy", available at: http://privacypolicy.umusic.com (accessed June 14 2006).

Vijayan, J. (2006a), "Judge dismisses data breach lawsuit", *ComputerWorld*, p. 12.

Vijayan, J. (2006b), "School out to improve its marks on security", *ComputerWorld*, p. 6.

Wack, K. (2006), "US threatens suit if Maine probes Verizon ties to NSA", *Portland Press Herald*, available at: http://pressherald.mainetoday.com/news/state/060804verizon.shtml (accessed August 9 2006).

Weeks v. *US* (1914), 232 US 383.

Whalen v. *Roe* (1977), 429 US 589, 605.

Winseck, D. (2003), "Netscapes of power: convergence, network design, walled gardens, and other strategies of control in the information age", *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London.

Zureik, E. (2002), "Theorizing surveillance – the case of the workplace", in Lyon, D. (Ed.), *Surveillance as Social Sorting*, Routledge, London.

Further reading

Associated Press (2006), "AOL technology chief, two others leave after data-privacy breach", *Wall Street Journal, p.*, p. 6.

Garrison, W. and Ramamoorthy, C. (1970), *Privacy and Security in Data Banks*, Technical Memorandum No. 24, Information Systems Research Laboratory, Urbana-Champaign, IL.

Healy, G. (2003), "Beware of total information awareness", available at: www.cato.org/daily/01-20-03.html (accessed June 14, 2006).

Jensen, J. (1991), *Army Surveillance in America, 1775-1980*, Yale University Press, New Haven, CT.

Lyon, D. (Ed.) (2003), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London.

Medford, C. (2006), "AT&T: we own your records", *Red Herring*, June 22, available at: www.redherring.com (accessed August 9, 2006).

OECD (1979), "Transborder data flows and the protection of privacy", *Proceedings, Information Computer Communications Policy, Paris*.

About the author

Cynthia M. Gayton holds a Bachelor of Arts degree in International Affairs from The George Washington University and a Juris Doctor degree from George Mason University in Arlington. Cynthia is a member of both the State Bar of Virginia and the District of Columbia Bar. Before joining the AIA, Cynthia had her own practice specializing in intellectual property and corporate law. In addition, she worked as an attorney at Morgan Lewis & Bockius, concentrating in complex antitrust litigation. Additionally, Cynthia is a part time adjunct professor of engineering law at The George Washington University School of Engineering and Applied Sciences. Cynthia is the co-author of *Legal Aspects of Engineering*, released in August of 2004 by Kendall/Hunt publishers and "Knowledge management in the large law firm" available at www.knowledgeboard.com Cynthia Gayton can be contacted at cgayton@gwu.edu