Accountability as the Basis for Regulating Privacy: Can Information Security Regulations Inform Privacy Policy?

By
Mary J. Culnan
Slade Professor of Management and Information Technology
IPM Department
Bentley University
mculnan@bentley.edu

July 20, 2011

An earlier version of this paper was presented at the 2011 Privacy Law Scholars Conference, Berkeley, CA., June 2-3, 2011. The author acknowledges the assistance of Krysta Wasiewski, Bentley 2011 MBA with the comparative analysis of the security regulations and the helpful comments of Mark MacCarthy and the PLSC attendees. Alan Friedman coined "shock and awe" as one way to describe enforcement actions.

Accountability as the Basis for Regulating Privacy:
Can Information Security Regulations Inform Privacy Policy?

Mary J. Culnan
Slade Professor of Management and Information Technology
IPM Department
Bentley University

Abstract

This paper argues that the current approach to regulating privacy based on "notice and choice" or "harm" is not effective and needs to be revisited. This approach places too much burden on the individual, frequently deals with harm only after the fact, and has failed to motivate organizations to proactively prevent privacy or security incidents resulting from their information processing activities. As an alternative, the paper proposes augmenting the current approach with new regulations based on accountability where firms are delegated responsibility to develop risk management programs for privacy tailored to their individual circumstances. The paper analyzes the requirements of three information security laws (GLB Safeguards Rule, HIPAA Security Rule and the Massachusetts Standards for the Protection of Personal Information) against the elements of accountability and concludes that these laws provide a starting point for designing a new privacy regulatory regime. Based on this analysis, the paper describes what a sample privacy program might look like including the types of evidence that could be maintained to demonstrate compliance. An accountability analysis of three recent FTC enforcement actions illustrates how this approach might work in practice. While current security laws provide a good starting point, privacy also raises new implementation challenges that will need to be addressed including the absence of standards for "reasonable privacy," identifying the types of records organizations need to maintain to document their compliance with the regulations, and how firms with different contexts should operationalize fair information principles. The paper concludes by reviewing arguments in favor of the more flexible delegation approach to privacy regulation rather than the traditional "command and control" compliance model.

Accountability as the Basis for Regulating Privacy:
Can Information Security Regulations Inform Privacy Policy?

> *Managers should be aware of the possible consequences of blind acceptance of external dictates, and regulators should take heed of companies that strictly obey the law.* Alfred A. Marcus (1988), p. 251

Introduction

There is an emerging consensus that the current regulatory approach to consumer privacy based largely on two models, "notice and choice," or "harm" is not effective and needs to be revisited. In general, the current approach places too much burden on individuals, usually deals with privacy only after harm has occurred, and has failed to motivate organizations to implement effective governance processes for privacy to proactively prevent privacy problems.

This paper will argue that a new approach is needed and that progress will not be made until organizations become accountable for their information practices. Current information security laws at both the federal and state levels require affected organizations to develop security programs appropriate to the organization's size, its available resources, and the amount and sensitivity of stored data (Smedinghoff 2008). The paper addresses the question: can these information security laws which require organizations to implement formal governance programs serve as a starting point for developing a new privacy policy regime, and if so, what would this new regime look like? The paper will be organized as follows. First, the paper will discuss problems with the current approaches and argue why a focus on accountability is both necessary and appropriate. Next, the requirements of three information security laws will be analyzed against the elements of accountability and the feasibility of adapting these requirements to privacy will be assessed. Based on this analysis, the paper will describe what a sample privacy program might look like including the types of evidence that could be maintained to demonstrate compliance. An accountability analysis of three recent FTC enforcement actions illustrates how this approach might work in practice. Finally, implementation issues and challenges for a new policy regime for information privacy based on delegation and accountability will be discussed.

Current Privacy Legal Landscape

Currently, privacy in the U.S. is regulated largely on a sectoral basis. Some industries (e.g. financial services and healthcare) and practices (e.g. telemarketing, online marketing to children, data breaches, video rental records) are regulated by a patchwork of federal and state privacy laws, some of which prohibit certain uses of personal information. The Federal Trade Commission (FTC) has also used its authority under Section 5 of the FTC Act to bring enforcement actions against commercial firms engaged in information practices found to be unfair or deceptive. Section 5 defines unfairness as an act or practice that causes, or is likely to cause, substantial harm to consumers, which is not reasonably avoided by consumers, and is not outweighed by countervailing benefits to either consumers or to competition, such as a

data breach caused by a failure to protect against common vulnerabilities. The FTC defined deception as a representation, omission or practice that is likely to mislead a consumer acting reasonably to the consumer's detriment, such as a privacy notice that is at odds with the firm's actual practices (FTC 1983). See FTC (2010) for a summary of the FTC's privacy enforcement actions based on unfair or deceptive practices. Some of the FTC's enforcement activities reflect "shock and awe" where "shock" reflects the magnitude of the surprise or outrage generated by the incident, and "awe" reflects the magnitude of the incident in terms of number of people affected, the financial impact resulting from the incident, or the level of negligence[1].

In its 2010 Staff Report, the FTC characterized its approach to privacy as based on two primary models: the "notice and choice" model and the "harm-based" model. Under the "notice and choice" model, the FTC encouraged companies to develop, post and abide by privacy notices describing their information practices to promote informed choice by consumers. The "harm-based" model focused on protecting consumers from specific harms such as economic injury or unwanted intrusion into people's private lives (FTC 2010). While both of the notice and choice and harm approaches are central and have advanced the FTC's goal of protecting consumer privacy and making companies accountable for their information practices, both approaches as well as existing laws also have their shortcomings.

First, the current privacy regime is overly burdensome for consumers. The notice and choice approach has led to overly long, legalistic privacy notices which are often unreadable and incomprehensible and as a result, of little value to consumers (FTC 2010; Milne & Culnan 2004; Milne, Culnan & Green 2006). Further, efforts to develop a standardized, simplified format for privacy notices modeled after nutritional labels have largely failed to gain wide acceptance with the exception of the GLB model privacy notice which while based on a common vocabulary and a narrow set of homogeneous information practices, still required a multi-year inter-agency development effort before it was approved for use (FTC 2009).

Second, the current regulatory approach only addresses a limited range of harms. It fails to recognize a broad range of privacy concerns ranging from nuisances, unfair surprises and concerns about surveillance to tangible economic harm. Both the FTC and Department of Commerce (2010) reports argue that even harms at the lower end of the continuum diminish trust and may jeopardize the adoption of useful or socially beneficial applications of new technologies. Further, many laws fail to prevent harm as they are only enforced after the fact. For example, despite the recent enforcement actions in the wake of major data breaches, forensic analyses performed by Verizon Business continue to find that a majority of the breaches they investigated could have been prevented had organizations implemented basic security measures and better governance (Culnan & Williams 2009; Verizon Business 2011).

Finally, laws are often reactive and outdated by the time they are enacted, failing to keep up with changing technologies and new business models. When these laws are based on

[1] The TJX (Culnan and Williams 2009) and Google (FTC 2011) enforcement actions are good examples of "shock and awe."

a “command and control” model of enforcement, they can result in companies adopting a legalistic approach to compliance aimed at maintaining their legitimacy rather than developing effective programs to address the spirit of the law (Bamberger 2006; Bamberger & Mulligan 2011a, 2011b; Bilton 2011; Culnan & Williams 2009; Sitkin & Bies 1993). For example, Milne et. al. (2006) found that online privacy notices increased in length and declined in readability between 2001 and 2003. They hypothesized that this may be attributed to a number of several highly-publicized FTC enforcement actions leading companies to revise their privacy notices to be more comprehensive and legalistic in order to avoid any possibility of their practices being at odds with the policies in their privacy notices rather than developing solutions to communicate more effectively with consumers as part of an overall risk management program. Efforts at industry self-regulation have also been criticized for failing to effectively address shortcomings in the law on a timely basis (FTC 2010). Taken together, these problems suggest a need for a new approach to privacy regulation which builds on these existing approaches.

Shifting the Regulatory Focus from Consumers to Organizations

There is a major shortcoming of the current individual perspective on privacy generally and the “notice and choice” approach specifically which argue for expanding the regulatory focus from the individual to the organization. Consumers are vulnerable in their dealings with organizations because they suffer from deficits of information and control. In addition to the problems with privacy notices described above, these deficits make it impossible for individuals to gain access to full information about an organization’s information practices on an ongoing basis. Individuals are also limited in their ability to exercise control over the ways organizations use their personal information once it has been disclosed (Culnan & Williams 2009). As a result, consumers depend on organizations to act in their best interest and to do no harm.

Much of the prior research on privacy has typically defined information privacy from the perspectives of individuals in terms of their ability to control or limit access to their personal information (Xu et. al. 2008). The “notice and choice” approach is one operationalization of this view of privacy as its goal is to provide individuals with a measure of control. The notice element is supposed to help people decided initially whether or not to disclose personal information based on the organization’s practices. The choice element provides an opportunity for people to place some limits on how their personal information is subsequently reused. The goal of providing control in this way is to increase the willingness of consumers to disclose personal information by minimizing the risks of disclosure (Xu et. al. 2008).

While information privacy is a multidimensional concept that is dependent on context and varies with a person’s life experiences, it also suffers from definitional ambiguity (Solove 2008). As an alternative to the individual perspective, Solove (2008) correctly characterized privacy as consisting a set of problems resulting from the ways organizations process personal information. He developed a taxonomy of information processing activities that have the

potential to result in harm to individuals and should be avoided[2]. For the purposes of this analysis, most of these activities may be grouped into two broad categories: *information reuse* and *unauthorized access* to personal information.

Typically, information reuse involves organizations making legal decisions about new uses for the personal information they have collected including data aggregation and data mining, and repurposing or sharing information originally collected for a different reason. Privacy problems potentially arising from information reuse include incorrect inferences, decisions based on errors in the data, exclusions or intrusions.

Unauthorized access, the second category of privacy problem includes two types of activities related to information security: browsing and data breaches. In the case of browsing, employees view personal information they are not authorized to view as in the case of individuals who browse a celebrity's records. Breaches involve unauthorized access to personal information, resulting from a variety of security incidents including hackers breaking into systems or networks, third parties accessing personal information on lost laptops or other mobile devices, or organizations failing to dispose of personal information securely. Harms resulting from unauthorized access can include a breach of confidentiality and trust, or the financial harm to individuals resulting from identity theft or identity fraud. If organizations implement appropriate security measures, they can typically prevent most types of unauthorized access.

Consistent with Solove, here security is defined as one aspect of privacy. However, privacy includes more than security as the prior discussion illustrates. Security is about protecting personal information, while privacy is broader and encompasses issues related to permission and use of personal information. Privacy is difficult to achieve without security. However, organizations can successfully secure the personal information in their custody and still make bad decisions about how the personal information they have collected is subsequently used, resulting in the privacy problems described above as recent FTC enforcement actions illustrate. Because security is one element of privacy, experience with developing security regulations targeted at organizations should provide some insights for regulating privacy given both privacy and security are based on organizations developing processes to minimize risk. Without robust governance processes for both privacy and security, organizations are likely to continue suffer privacy problems. Therefore, as organizations cause most privacy problems, new regulations should focus on making organizations more accountable for their decisions in addition to providing transparency (e.g. notice and choice) which enables consumer choice. Current privacy laws are not doing this effectively and a new approach based on accountability is needed.

[2] Solove's taxonomy contains four principal groups of activities related to information collection (e.g. surveillance), information processing (e.g. aggregation, identification, insecurity, secondary use, or exclusion), information dissemination (e.g. breach of confidentiality, disclosure, exposure, increased accessibility, distortion) and Invasion (e.g. intrusion).

Accountability & Governance

Accountability is well-established as a critical element of effective data protection. For example, the OECD 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the laws of Europe, Canada and the US, and industry guidelines such as the AICPA's Generally Accepted Privacy Principles (GAPP) all include provisions stating that organizations should be responsible for the personal information under their control. While there is consensus that accountability is critical to effective data protection, the concept has not been clearly operationalized for practice (Hunton & Williams 2009).

Accountability emphasizes rationality, responsiveness, and reviewability (Bamberger 2006). The report from the Paris Project (Hunton & Williams 2010) identified a set of essential elements of accountability which apply to existing laws and regulations, industry self-regulatory programs to which organizations belong, and the privacy promises an organization makes in its privacy policies and privacy notices:

- Organization commitment to accountability and adoption of internal policies consistent with external criteria,
- Mechanisms to implement privacy policies including tools, training and education.
- Systems for internal, ongoing oversight and for external verification.
- Transparency and mechanisms for individual participation, and
- Means for remediation and external enforcement.

Accountability, then, is a concept that has both governance and ethical dimensions, applies across a variety of legal regimes and cultures, and is implemented by ongoing risk assessment and mitigation processes. As a result, it promotes the implementation of scalable, practical mechanisms which focus on processes leading to specific outcomes. Because accountability is not a "one-size-fits all" approach, organizations have considerable flexibility to develop governance programs appropriate to their particular context. Programs based on accountability principles are sensitive to cultural and social norms about acceptable use and responsive to changing business models and new technologies without imposing unnecessary burdens on organizations (European Union 2010; Hunton & Williams 2010). Accountability has been proposed as an approach to effective governance for the business use of data analytics (Schwartz 2011) and for cloud computing (Pearson and Charlesworth 2009). The elements of the EU's Binding Corporate Rules also reflect accountability principles (European Union 2008).

Accountability has the potential to address the shortcomings with the current privacy regime identified above. First, and most important, by establishing robust governance processes, organizations reduce the likelihood that their information practices will cause privacy problems. Because the requirements focus on implementing risk management processes to achieve desired outcomes, compliance cannot be fully realized by developing legalistic compliance efforts which involve merely "checking the box" on a list of specific

requirements (Bamberger 2006; Sitkin & Bies 1992). Second, accountability creates requirements that are both flexible and scalable, and are therefore appropriate for all types of organizations as implementation of the regulations is tailored by each organization to its particular context. The advantages of this delegation approach to regulation will be discussed in greater detail in a subsequent section of the paper.

Accountability Provisions of Security Laws

The FTC Staff Report (2010) recommends that companies should incorporate substantive privacy and security protections into their routine business practices, with security being one element in a comprehensive privacy program. Privacy should be considered throughout the life cycle of products and services at all stages of the lifecycle of products and services. To accomplish this objective, the FTC suggests organizations should implement a comprehensive privacy program, consider privacy in advance of making product design decisions, and develop and enforce sound privacy procedures throughout the organization. In other words, organizations should be accountable for their information practices. Current security laws provide an example of how to incorporate accountability principles into law for one class of privacy problem: avoiding the harm caused by unauthorized access to and use of personal information. An analysis of these laws should prove insights about the feasibility of basing comprehensive privacy legislation on accountability principles.

This paper is based on an analysis of one state and two federal security regulations, the Massachusetts Standards for the Protection of Personal Information (201 CMR 17.00), The GLB Safeguards Rule, and the HIPAA Security Rule. GLB and HIPAA are sectoral regulations governing information which is traditionally considered sensitive. They apply to financial institutions and covered health organizations respectively.

The Massachusetts regulation applies to any person who maintains personal information on a Massachusetts resident, independent of where the information is housed. It is interesting for two reasons. First, it is a state law with national scope which defines personal information broadly unlike the two sectoral federal laws[3]. Second, the genesis of the Massachusetts regulation was a requirement in the 2009 Massachusetts data breach law (Chapter 93H, Massachusetts General Law), making it the first state breach law to require organizations to proactively safeguard personal information in addition to the requirement to notify consumers and regulators after a breach occurred.

An original motivation for the state breach laws was to create an incentive structure for organizations to implement internal risk management processes in order to avoid reputational and other damages associated with making a breach public (Bamberger & Mulligan 2011b). As compliance with government regulation leads to organizational legitimacy, or the acceptance of an organization by its external environment, it was reasonable to expect that notice laws should have the desired effect of preventing breaches (DiMaggio & Powell 1983; Meyer &

[3] It should be noted that the national reach of the Massachusetts regulation has yet to be tested in court.

Rowan 1977). This was the case in some instances (Bamberger & Mulligan 2011b). However, the fact that serious breaches continue in the wake of the majority of states enacting breach laws suggests that this approach has had limited success due to the absence of real repercussions (Bilton 2011; Verizon Business 2011; Westby 2010). Massachusetts, then, was the first state to require organizations to proactively safeguard personal information rather than assuming the requirement to notify after a breach would adequately motivate all organizations to develop such programs on their own.

The three regulations were analyzed to the extent to which each reflects accountability principles. The principles were adapted from the Paris Project (Hunton & Williams 2010) and include:

- the requirement to create a formal policy,
- executive oversight,
- ongoing risk assessment, mitigation, oversight and validation,
- education and awareness,
- the requirement to main additional documentation beyond a written policy,
- internal enforcement,
- requirements for business partners, and
- transparency and redress requirements for individuals.

Table 1 summarizes the scope of the three laws and the analysis of their respective accountability provisions.

Insert Table 1 about here

In general, while the GLB Safeguards Rule contains fewer specific requirements than the HIPAA Security Rule and the Massachusetts Regulation, all three laws are similar and include requirements to create and maintain formal, written security policies, to designate at least one employee who is responsible for security, to perform risk assessments and engage in regular monitoring and evaluation, to provide education and awareness programs for employees, and to have contracts requiring business partners to protect personal information.

In addition, the HIPAA Rule and the Massachusetts Regulation require organizations to implement a range of specific physical and technical safeguards and to enforce internal sanctions in the case of violations. Both also require the maintenance of additional documentation in addition to having a written policy. HIPAA requires organizations to document the security measures chosen as part of risk assessment while the Massachusetts regulation requires organizations to document actions taken in response to a data breach and the accompanying post-incident review. The GLB Safeguards Rule only requires organizations to implement technical and physical safeguards that are appropriate for the context. Further, GLB does not contain any provisions related either to internal enforcement or the need to maintain additional documentation beyond the written policy.

None of the three laws contain any language related to transparency and redress for individuals. However, these issues are more appropriately addressed by privacy legislation and data breach legislation respectively. For example, both GLB and HIPAA define requirements for transparency in the form of rules for privacy notices. State data breach laws define notice and redress requirements for data breaches. Therefore, it appears that these laws can provide a starting point for designing comprehensive privacy legislation based on accountability. Recent FTC enforcement actions also provide support for this conclusion as will be described below. However, developing accountability-based privacy regulation also poses new challenges that do not apply to information security. The paper now turns what a privacy regime based on accountability might look like, and to a discussion of these implementation challenges.

Proposed Elements of a Comprehensive Privacy Program

To prevent privacy problems resulting from either privacy (information use or reuse) or security (unauthorized access), organizations need governance programs that are based on some common accountability elements as described above. As with programs designed to avoid unauthorized access, effective governance of privacy is also process-based and requires organizations to implement a formal policy, designate executive oversight, perform ongoing risk assessment, mitigation, oversight and validation, education and awareness, internal enforcement, and provide controls over their business partners. Additionally, organizations need to address transparency and redress issues in their privacy programs. Table 2 illustrates what one version of a comprehensive privacy program based on accountability might look like including sample activities for each element.

Insert Table 2 about here

Three FTC enforcement actions illustrate how privacy regulation based on accountability might work in practice: Google Inc. (Buzz), Eli Lilly and Chitka. Tables 3A, 3B and 3C summarize the three cases respectively and describe how each could have been avoided by implementing a governance program based on accountability. Each will be discussed briefly.

Google Buzz.

Google Inc. launched Google Buzz, a social media platform which runs on top of a user's existing Gmail contacts. In its complaint, the FTC argued that Google launched Buzz without providing notice or gaining consent to use Gmail information for a new purpose, in violation of Google's Gmail privacy policy and the Safe Harbor agreement. The FTC also argued that the privacy controls Google implemented did not work as promised. FTC alleged that Google had engaged in an unfair or deceptive trade practice, in violation of section 5(a) of the Federal Trade Commission Act. The settlement required Google to establish and implement a comprehensive privacy program, and to maintain documentation to demonstrate compliance.

Insert Table 3 A about here

Eli Lilly.

An Eli Lilly employee sent an email to subscribers to Eli Lilly's Prozac Medi-messenger service announcing the termination of the service. The employee created a new program to access the subscribers' email addresses and to send the email. The email unintentionally disclosed personal information, the email addresses of all 669 subscribers, in the "To" line of the message. As a result, Eli Lilly unintentionally disclosed personal information in violation of its privacy notice. The FTC attributed the incident to Eli Lilly's failure to provide appropriate training and appropriate oversight for an employee who had no prior experience in creating, testing or implementing the program used to send the message. While this case involved unauthorized disclosure of personal information and is technically a security rather than a privacy case, it is instructive here because it is based on an organizational failure by an employee who was authorized to access the information to perform a specific task, rather than a more typical security breach resulting from unauthorized access to an unprotected network. The FTC alleged Eli Lilly engaged in an unfair or deceptive trade practice, in violation of section 5(a) of the Federal Trade Commission Act. The settlement required Eli Lilly to implement a comprehensive security program and to maintain documentation to demonstrate compliance.

Insert Table 3B about here

Chitika.

Chitika is an online behavioral advertising firm that acts as an intermediary between website publishers and advertisers wishing to advertise on websites. Chitika offered an opt out, however, the opt out cookies it delivered expired after 10 days. Chitika's privacy notice did not inform consumers that the opt out cookies would expire after 10 days. The FTC alleged that Chitika engaged in a deceptive trade practice under section 5(a) of the Federal Trade Commission Act. The settlement required Chitika to implement effective notice and choice procedures and prohibited the use or reuse of any personal information collected prior to the date when the problem was corrected.

Insert Table 3C about here

As the three cases illustrate, each could have been avoided if the firms had implemented privacy programs based on accountability. Notably, all three cases reflected a failure to implement privacy controls that worked as promised, suggesting a failure by the companies to incorporate privacy into their software development processes. Of particular note, in the Google settlement, the FTC for the first time called for an organization to implement a comprehensive privacy program.

The Google settlement appears to have been modeled after the GLB Safeguards Rule. It includes a number of elements of accountability such as requirements to develop a written privacy program, designate employee(s) to be responsible for the privacy program, perform ongoing risk assessments including design and implementation of reasonable privacy controls,

procedures to address identified risks, ongoing testing, monitoring and evaluation. It also requires contracts to ensure Google's business partners implement and maintain appropriate privacy protections. The FTC does not define what each of these elements should look like, leaving it up to Google to determine what specific procedures and controls will be effective given its size and complexity, the nature of its business activities, and the sensitivity of the personal information Google collects and maintains. However, the agreement does imply the need to for organizations to base their privacy programs on Privacy by Design principles.[4] Finally, the agreement also included requirements for transparency and specified the types of records that Google needs to maintain to demonstrate their compliance. The terms of the settlement were described by one law firm as establishing a new norm for privacy enforcement (Goodwin Procter 2011).

Implementation Challenges for New Privacy Regulations

The Google Buzz settlement suggests that in fact existing security laws can provide the basis for defining the elements of a comprehensive privacy program. However, there are three substantive issues that differentiate security from privacy and need to be addressed in developing any new public policy regime for privacy based on accountability.

First, there is consensus that unauthorized access is wrong and potentially harmful. While organizations may quibble about what types of unauthorized access trigger the requirement to notify, there is little if any dispute about what constitutes unauthorized access and that it constitutes a privacy problem with the potential for harm; therefore, firms need to provide reasonable security for customer and employee data (FTC 2010). Further, enforcement actions in the event of a security breach typically begin by assessing whether the organization's security program complied with widely-accepted technical and procedural standards for information security. While there is agreement that privacy is not absolute, no comparable standards exist for the collection and use or reuse of personal information (Culnan & Bies 2003).

It is interesting to note that the FTC settlement did not prohibit the three firms from going forward with their use of personal information once they addressed the problems in the complaint. Only Chitika was only prohibited from using personal information it collected deceptively, but was not prohibited offering online behavioral advertising services in the future or using the personal information collected after it resolved the problem. Given the variety of business models, changing technologies and given the contextual nature of much use of personal information, it is unrealistic to expect any new regulation to include a comprehensive list of acceptable or prohibited uses of personal information, providing the information is collected, used and reused fairly and lawfully and does not result in harm as the cases described above illustrate**.**

[4] Privacy by Design consists of seven foundational principles including proactive not reactive, preventative not remedial, privacy embedded into design, and full lifecycle protection. See: Cavoukian (2010). Microsoft (2008) also provides suggestions for incorporating privacy into the software development process.

Given this flexibility, governance programs based on accountability principles provide an attractive means alternative for organizations to avoid enforcement actions. Here, an organization would be responsible for performing a risk assessment such as a PIA for new uses of personal information to determine if the practice could result in a privacy problem. Solove's (2008) taxonomy of privacy problems could provide a starting point for such an analysis, as could an assessment of whether the new use is compatible with the original reason for collecting the information. If the analysis suggests that the practice being reviewed has the potential to create a privacy problem but is still legal and consistent with public norms for acceptable use, the organization can then design a remedy to avoid the problem. Remedies could include something as basic as insuring a new practice is consistent with the firm's privacy policy. If not, the firm will need to modify its policy, align its privacy notice with the policy, notify its customers of the change, and obtain customer consent as appropriate. For new uses which significantly violate public norms, the remedy for avoiding the privacy problem could be a decision not to go forward with the proposal. The Google Buzz complaint (FTC 2011) is instructive in illustrating shortcomings in one organization's decision to develop an application based on secondary use of personal information and the steps it could have taken to avoid the resulting privacy problems.

Second, organizations will need to keep formal records to document their risk processes in order to demonstrate their commitment to accountability and their compliance with any new regulations. Again, it will be difficult to develop a comprehensive list that is appropriate for all situations. However, Table 2 provides examples of typical business records that could be maintained to demonstrate compliance for each element of accountability. The Google proposed settlement includes documentation requirements the FTC considered relevant for this case and includes the results of audits, privacy or security incidents and how they were addressed as well documentation of how the firm handled privacy complaints. Other candidates for retention include records documenting an organization's risk assessment programs including the results of any PIA's, minutes of cross-functional privacy committee meetings, copies of all contracts with business partners, records documenting the firm's education and awareness programs, and records of any internal enforcement actions.

Finally, privacy programs need to be grounded in fair information practices. A major cause of enforcement actions is a failure of organizations to comply with their published privacy notices as the Google, Eli Lilly and Chitika settlements illustrate. While there is general consensus about the principles, there continue to be many unresolved issues and challenges related to widespread implementation of the principles as they relate to information use and reuse. These first include how to create more standardized privacy notices that are both comprehensive and comprehensible and can be applied across all industries, business models and technology platforms. Other issues include questions about compatible and acceptable uses of personal information, developing effective mechanisms to provide choice or consent, and questions about what constitutes reasonable access and how to provide it[5]. We now turn

[5] The FTC proposed a limited set of "commonly accepted practices" for which companies should not be required to seek consent once a consumer has chosen to use a product or service. These practices include product &

to a discussion of the advantages of flexible enforcement based on accountability over more traditional approaches based on compliance.

Regulation by Delegation as the New Paradigm for Privacy

There are two primary approaches to regulation: the compliance model and the delegation model (Bamberger 2006). While both approaches impose civil or criminal penalties for violations, they differ in terms how the desired outcomes are achieved. The compliance model represents the dominant paradigm of regulation. Here, firms comply by ensuring their practices comport with a clear set of rules specified in the law. The costs and the likelihood of punishment in the event of a violation are high enough to deter noncompliance. The compliance approach assumes that one set of rules will achieve the goals of the legislation across all regulated organizations (Bamberger 2006).

In contrast, the delegation model has its roots in the delegation principle of administrative law and is based on accountability principles (Bamberger 2006). It recognizes that one-size solutions do not exist and instead regulations based on delegation specify outcomes and assume firms have superior information and expertise to develop local solutions that will result in lead to the desired results. Regulations require firms to make their decision processes related to implementation sufficiently transparent to provide meaningful review as appropriate. It further makes firms answerable for ensuring their decisions are consistent with public norms (Bamberger 2006). The security regulations described in Table 1 above which require "reasonable security" but leave the determination of what this means in any given context to individual firms are examples of the delegation approach.

The delegation approach is particularly appropriate for privacy (and security) as the primary challenge of privacy (and security) is that both are based on avoiding incidents. Preventing privacy problems involves firms developing processes to reduce risks on an ongoing basis, something which is unlikely to be accomplished by merely satisfying a checklist and punishing violations after an incident has been reported (Bamberger 2006; Culnan & Williams 2009). With the compliance approach, there is often no way to monitor or assess a firm's performance effectively until it reports an incident, thereby revealing possible shortcomings in its risk management programs. In contrast, with the delegation approach, the focus is on developing processes to achieve desired outcomes in advance of incidents.

The delegation approach also represents a new way to structure relations between regulators and regulated organizations. With this approach, the government agencies act as educators as the FTC has done (c.f. Bamberger & Mulligan 2011b). Regulators can also provide guidance in the form of suggested best practices without making universal prescriptions as the FTC has done for implementation of the GLB Safeguards Rule.

---

service fulfillment, internal operations, fraud prevention, legal compliance and public purposes, and first-party marketing. See FTC (2010), p. 53-54

There is empirical research in support of the delegation approach. For example, Marcus (1988) studied compliance versus delegation approaches to the implementation of safety regulations by nuclear power plants[6]. He found that a rule-based approach with little autonomy perpetuated poor safety results while allowing plants autonomy in developing safety programs resulted in improved safety records for plants with both strong or poor safety records. He argued when organizations have autonomy in deciding how to implement a regulation, the end result is likely to be more effective because firms rather than regulators have greater local knowledge, and top-down compliance approach may deskill those who carry out the policy resulting in errors while autonomy encourages high levels of commitment and knowledge. Similarly, Bamberger and Mulligan (2011a; 2011b) studied nine firms known to be leaders on privacy. They found that these organizations had voluntarily developed effective distributed architectures for governing privacy. This suggests that the delegation approach based on implementing "reasonable privacy" is both promising and feasible as an approach for future regulation.

Conclusion

This paper has argued that the current approach to regulating privacy based on "notice and choice" or "harm" alone is not effective. This approach places too much burden on the individual, frequently deals with harm only after the fact, and has failed to motivate organizations to proactively prevent privacy or security incidents. It proposed as an alternative, augmenting the current approach with new regulations based on accountability where firms are delegated responsibility to develop risk management programs for privacy tailored to their individual circumstances. These regulations would be modeled after current security regulations which require firms to implement "reasonable security." Based on an analysis of security regulations, the paper described what a sample privacy program might look like including the types of evidence that could be maintained to demonstrate compliance. An accountability analysis of three recent FTC enforcement actions illustrated how this approach might work in practice. The paper also identified three challenges to developing privacy laws based on "reasonable privacy": the absence of standards for "reasonable privacy," identifying the types of records organizations need to maintain to document their compliance with the regulations, and how firms with different contexts should operationalize fair information principles.

Delegating responsibility for compliance with regulations based on accountability was argued to have advantages over regulations based on the compliance paradigm. In particular, the delegation approach assumes individual organizations rather than regulators have the local knowledge to develop solutions that will be effective for a particular context. But more important, new regulations which require organizations to implement risk processes have the potential to create an external shock that places privacy on the radar screen of senior management (Bamberger 2006: Marcus 1988; Smith 1994). Due to their fiduciary responsibilities, the duty of care for both CEO's and boards of directors increasingly includes

[6] Marcus characterized these two approaches as rule-bound versus autonomous rather than compliance versus delegation.

responsibility for protecting both personal information and the organization's information systems (Smedinghoff 2008). However, there is evidence that organizations have been slow to accept this responsibility (Westby 2010). Robust privacy programs are both costly and difficult. Since there is no obvious return from avoiding incidents and there are few restrictions on the ways organizations can reuse the information they have collected, the firm's risk calculations may not justify the costs of a comprehensive privacy program (Austin & Darcy 2003; Osterhus 1997). Therefore, it is unlikely an organization will succeed in moving from a compliance mind-set to a culture of accountability unless there is commitment from top management (Culnan & Williams 2009).

Current security regulations reflect a basic set of best practices for effective risk management. Despite the fact that these requirements describe risk programs that organizations should already have in place, when the various security regulations were initially adopted, there was great consternation among affected organizations about what it meant to have "reasonable security." Today, the idea that firms should provide reasonable security for both customer and employee data is well-settled (FTC 2010). The reach of these existing regulations combined with the PCI-DSS requirements which impose similar requirements on all organizations accepting payment cards means that the majority of U.S. businesses have or should have experience complying with regulations that require the development of risk programs related to personal information. These existing risk programs can provide the basis for expanding these programs to privacy.

There is likely to be controversy about the proposed new privacy regulations due in part to the implementation challenges described previously. As it has done in the past, the FTC can assist by providing education and guidance through discussions with individual firms, public workshops, examples of best practices, and targeted enforcement actions including making an example of firms who experience privacy problems exceeding the "shock and awe" threshold. Therefore, there is every reason to believe the idea that organizations need to provide "reasonable privacy" can also become well-settled over the next decade. Personal information is an increasingly valuable asset and deserves to be treated with the same care that organizations accord their financial assets. The failure of existing approaches to privacy regulation combined with the emerging global consensus about the merits of accountability argue for using accountability as the basis for a new regime for regulating privacy.

Table 1
Analysis of Accountability Provisions of Three Security Laws

	Massachusetts Standards for the Protection of Personal Information 201 CMR 17.00	**GLB Safeguards Rule 16 CFR Part 314**	**HIPAA Security Rule 45 CFR 164.306(a)**
What information is covered	Personal information defined as a MA resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relates to a resident: 1) Social Security Number; 2) driver's license number or state issue identification card number; or 3) financial account number, or credit or debit card number.	Nonpublic personal information about a customer of a financial institution in any form	Electronic protected health Information (ePHI). ePHI defined as "individually identifiable health information" held or transmitted by a covered entity or its business associate, in electronic form.
Who must comply?	Every person that owns or licenses personal information about a resident of the Commonwealth of Massachusetts.	Financial institutions and their affiliates or service providers .	Covered entities that use and/or store individually identifiable ePHI and their business associates.
Objectives	Administrative, technical and physical safeguards that are appropriate to the size, scope and type of business, the amount of available resources, the amount of stored data, and the need for security and confidentiality of both consumer and employee information: • Insure the security and confidentiality of customer information in a manner fully consistent with industry standards • Protect against anticipated threats or hazards • Protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer	Technical and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue • Insure security and confidentiality of customer information • Protect against an anticipated threats • Protect against unauthorized access or use that could result in substantial harm or inconvenience to the customer	Maintain reasonable and appropriate administrative, technical and physical safeguards for protecting e-PHI: • Ensure the confidentiality, integrity and availability of e-PHI • Identify and protect against reasonably anticipated threats • Protect against reasonably anticipated, impermissible uses or disclosures • Ensure compliance by the covered entities workforce The covered entity should consider its size, complexity and capabilities, its technical, hardware and software infrastructure, the costs of security measures, and the likelihood and possible impact of potential risks to e-PHI.

	Massachusetts Standards for the Protection of Personal Information 201 CMR 17.00	GLB Safeguards Rule 16 CFR Part 314	HIPAA Security Rule 45 CFR 164.306(a)
Required Accountability Elements			
Policy Requirement	A formal information security program must be written, implemented, maintained and kept in more than one readily accessible place.	Must develop, implement and maintain a comprehensive written information security program	Must create and maintain written security policies for at least 6 years after creation or last effective date.
Executive Oversight	Designate one or more employees to maintain the comprehensive information security program.	Designate one or more employees to coordinate the information security program	Designate a security official who is responsible for developing and implementing its security policies and procedures.
Ongoing Risk Assessment, Mitigation, Oversight and Validation	• Identify and assess reasonably foreseeable internal and external risks to the security or confidentiality of personal information • Regular monitoring to ensure the security program is operating reasonably and upgrading as necessary • Reviewing scope of security measures at least annually or when there is a material change in business practices	• Identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information • Detecting, preventing and responding to attacks, intrusions or other system failures • Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures	• Ongoing process to identify and analyze potential risks to e-PHI, and implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level • Periodically evaluate the effectiveness of security measures put in place
Education & Awareness	Education and training of employees on the proper use of the computer security system and the importance of personal information security.	Employee training and management required	Train all workforce members regarding its security policies and procedures.
Additional documentation Requirements (beyond written policy)	Document actions taken involving a data breach, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information	None specified	As part of risk assessment, document the chosen security measures and where required, the rationale for adopting those measure

	Massachusetts Standards for the Protection of Personal Information 201 CMR 17.00	GLB Safeguards Rule 16 CFR Part 314	HIPAA Security Rule 45 CFR 164.306(a)
Internal Enforcement	Impose disciplinary measures for policy violations	Not mentioned in rule. Recommended in FTC guidance on complying with the Rule	Apply and enforce appropriate sanctions against workforce members who violate policies and procedures
Requirements for Business Partners	• Take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measure to protect such personal information consistent with these regulations and any applicable federal regulations • Contracts to require such third-party service provider to implement and maintain appropriate security measures for personal information	• Take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue • Contracts to require service providers to implement and maintain such safeguards	• Satisfactory written assurance (contract or other agreement) that the business associate will use e-PHI only for specified purposes and will safeguard the information from misuse. • In the event of a material breach or contract violation, covered entity is required to take reasonable steps to cure the breach or end the violation. If efforts are unsuccessful, terminate the contract or agreement.
Transparency and redress for individuals	Not mentioned	Not mentioned	Not mentioned

Note: Accountability elements adapted from the Paris Project (Hunton & Williams 2010)

Table 2
Sample Elements of a Comprehensive Privacy Program

Program Element	Sample Activities	Sample Evidence of Compliance
Executive oversight	Appoint appropriate individual(s)	• Job description(s) • Organization chart
Written privacy program	Policy elements include: • Governance • Polices & procedures • Risk management processes • Compliance • Redress and enforcement	• Copy of policy • Document changes to policy
Ongoing risk assessment	• Cross-functional privacy committee or other governance body • Privacy Impact Assessments for new systems and new uses of PII • Regular internal audits or other reviews	• Minutes of committee meetings • Privacy impact assessment reports • Audit reports
Employee training	• Formal training program • Training for new employees • Retraining for existing employees	• Training materials • Records of who was trained and when
Implement and monitor privacy controls	• Comprehensive personal information inventory • Guidelines for building privacy controls into new systems • Guidelines for testing privacy controls • Data retention policy	• Results of inventory • Copies of guidelines and policies • System sign-offs • Results of system tests & ongoing monitoring
Third parties	• Contracts	• Copies of contracts • Records of 3rd party assurance
Internal enforcement	• Policies for assuring compliance • Sanctions for violations of policies	• Copies of policies • Reports of violations and how handled
Transparency and redress for consumers	• Consumer privacy notice • Procedures for providing notice for material changes to policy and gaining consent for new uses of PII • Procedures for handling consumer inquiries and complaints	• Copy of notice • Document changes to notice • Document consent for new uses of PII • Complaint handling records

Table 3A
Analysis of Google Buzz FTC Decision

Google Inc. (2011)[7]		
Description of Case	Google Buzz is a social media platform which runs on top of a user's existing Gmail contacts. People automatically became followers of other users. Further, if people opted out of Buzz, some of their information was still made public. Google launched Buzz without providing notice or asking consent to use Gmail information for a new purpose, in violation of Google's privacy policy for Gmail and the Safe Harbor agreement. The FTC alleged Google engaged in an unfair or deceptive trade practice.	
Terms of Consent Agreement	• Maintain a comprehensive privacy program to address privacy risks of new products or services and protect privacy of covered information o Executive oversight o Ongoing risk assessments o Design and implement reasonable privacy controls to address identified risks o Contracts for service providers o Evaluate and adjust privacy program to address issues identified • Maintain documentation to demonstrate compliance	
Accountability Analysis of Case		
Relevant Accountability Elements	**What Google Did Wrong**	**Potential Solution**
Ongoing risk assessment	Failure to perform a privacy impact assessment (PIA)	PIA should have surfaced need to comply with privacy policy before launch (notice & consent)
Implement and monitor privacy controls	• Privacy controls did not work as promised • Buzz was only tested on Google employees before launch	• Formal procedures for testing software • Ongoing monitoring to ensure applications work as intended • Beta testing with customers outside of Google

[7] US Federal Trade Commission, "In the Matter of Google Inc., File No. 102 3136," March 2011. Available at: http://www.ftc.gov/os/caselist/1023136/index.shtm

Table 3B
Eli Lilly

Eli Lilly and Company (2002)[8]		
Description of Case	An Eli Lilly employee sent an email to subscribers to Eli Lilly's Prozac Medi-messenger service announcing the termination of the service. The employee created a new program to access the subscribers' email addresses and to send the email. The email disclosed the email addresses of all 669 subscribers in the "To" line of the message. As a result, Eli Lilly unintentionally disclosed personal information in violation of Eli Lilly's privacy notice. The FTC alleged Eli Lilly engaged in an unfair or deceptive trade practice.	
Terms of FTC Consent Agreement	• Create a comprehensive security program: o Executive oversight o Risk assessment o Monitoring and evaluation of management and training of personnel, information systems, and prevention of unauthorized access and other information systems failures • Maintain documentation to demonstrate compliance	
Accountability Analysis of Case		
Relevant Accountability Elements	**What Eli Lilly Did Wrong**	**Potential Solution**
Employee Training	Failed to provide appropriate training for employees	Formal training program for all employees who access personal information
Implement and Monitor Privacy Controls	• Failed to test new email program before sending message • Failed to provide appropriate oversight for the employee who had no prior experience in creating, testing or implementing the program used	• Formal procedures for testing software applications involving PII • Monitoring to ensure procedures are followed.

[8] US Federal Trade Commission, "In the Matter of Eli Lilly and Company, Docket No. C-4047," May 2002. Available at: http://www.ftc.gov/os/caselist/0123214/0123214.shtm

Table 3C
Chitika Inc

Chitika, Inc. (2011)[9]		
Description	Chitika is an online behavioral advertising firm that acts as an intermediary between website publishers and advertisers wishing to advertise on websites. Chitika offered an opt out, however, the opt out cookies it delivered expired after 10 days. Chitika's privacy notice did not inform consumers that the opt out cookies would expire after 10 days. The FTC alleged that Chitika engaged in a deceptive trade practice.	
Terms of FTC Consent Agreement	• Provide clear notice and choice • Prohibit use or reuse of any information collected prior to 3/1/10 when problem was corrected • Maintain documentation to demonstrate compliance	
Accountability Analysis		
Relevant Accountability Element	**What Chitika Did Wrong**	**Potential Solution**
Implement and Monitor Privacy Controls	Failed to test opt out cookies on an ongoing basis to ensure they worked as expected	• Formal procedures for testing software • Ongoing monitoring to ensure applications work as intended

[9] US Federal Trade Commission, "In the Matter of Chitika, Inc., Docket No. C-4324," June 2011.. Available at: http://www.ftc.gov/os/caselist/1023087/index.shtm

References

Austin, R.D. and Darcy, C.A.R. (2003), The Myth of Secure Computing, *Harvard Business Review*, 81, 6 (June), 120-126.

Bamberger, Kenneth A. (2006), Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State, *Duke Law Journal* 56, 2 (November), 437-468.

Bamberger, Kenneth A. and Mulligan, Deirdre K. (2011a), Privacy on the Books and on the Ground, *Stanford Law Review*, 63, forthcoming.

Bamberger, Kenneth A. and Mulligan, Deirdre K (2011b), Catalyzing Privacy: New Governance, Information Practices, and the Business Organization, *Law & Policy*, forthcoming.

Bilton, N. Holding Companies Accountable for Privacy Breaches, *New York Times Bits*, April 27, 2011. Available at: http://www.nytimes.com (Accessed April 28, 2011).

Cavoukian, A. (2010). *Privacy by Design 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*. Available at: http://www.futureofprivacy.org/the-privacy-papers (Accessed June 24, 2011).

Culnan, Mary J. and Bies, R.J. (2003), "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, 59, 2, 323-342.

Culnan, Mary J. and Williams, Cynthia Clark (2009), How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches, *MIS Quarterly*, 33, 4 (December), 673-687.

DiMaggio, P.J. and Powell, W.W. (1983), The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in the Organizational Field, *American Sociological Review*, 48, 2, 146-160.

European Union, Article 29 Data Protection Working Party (2008), *Working Document Setting Up a Table with the Elements and Principles to be Found in Binding Corporate Rules*, June 24. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf (Accessed April 23, 2011).

European Union, Article 29 Data Protection Working Party (2010), *Opinion 3/2010 on the Principle Accountability*, July 13. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (Accessed April 23, 2011).

Goodwin Procter (2011). *Alert: FTC Settlement with Google Establishes New Norm for Privacy Enforcement*. April 21. Available at: http://www.goodwinprocter.com/Publications/Newsletters/Client-Alert/2011/FTC-Settlement-with-Google-Establishes-New-Norm-for-Privacy-Enforcement.aspx (Accessed: April 21, 2011).

Hunton & Williams, Centre for Information Policy Leadership (2009), *Data Protection Accountability: The Essential Elements – A Document for Discussion*. October. Available at: http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (Accessed April 21, 2011).

Hunton & Williams, Centre for Information Policy Leadership (2010), *Demonstrating and Measuring Accountability: A Discussion Document (Accountability Phase II – The Paris Project*). October. Available at: http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF (Accessed April 21, 2011).

Marcus, A.A. (1988), Implementing Externally Induced Innovations: A Comparison of Rule-Bound and Autonomous Approaches, *Academy of Management Journal*, 31, 2 (June), 235-258.

Meyer, J.W. and Rowan, B. (1977), Institutionalized Organizations: Formal Structure as Myth and Ceremony, *American Journal of Sociology*, 83, 2 (September), 340-363.

Microsoft Corporation (2008), *Privacy Guidelines for Developing Software Products and Services*. Available at: http://www.microsoft.com/downloads/en.

Milne, George R. and Culnan, Mary J. (2004), Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices, *Journal of Interactive Marketing*, 18, 3 (Summer), 15-29.

Milne, George R., Culnan, Mary J., and Greene, Henry (2006), A Longitudinal Assessment of Online Privacy Notice Readability, *Journal of Public Policy and Marketing*, 25, 2 (Fall), 238-249.

Osterhus, T.L. (1997), Pro-Social Consumer Influence Strategies: When and How Do They Work?, *Journal of Marketing*, 61, 4, 16-29.

Smedinghoff, Thomas J. (2008), Information *Security Law: The Emerging Standard for Corporate Compliance*, Cambridgeshire: IT Governance Publishing.

Pearson, Siani and Charlesworth, Andrew (2009), Accountability as a Way Forward for Privacy Protection in the Cloud, *Cloud Computing: Proceedings of the First International*

Conference, CloudCom 2009, Beijing, China, p. 90-106. Available at: http://www.hpl.hp.com/techreports/2009/HP-2009-178.pdf (Accessed April 21, 2011).

Schwartz, Paul M. (2001), Data Protection Law and the Ethical Use of Analytics, *BNA Privacy & Security Law Report*, 10 PVLR 70, January 10.

Sitkin, S.B. and Bies, R.J. (1992), The Legalistic Organization: Definitions, Dimensions and Dilemmas, *Organization Science*, 4, 3 (August), 345-351.

Smith, H. Jeff (1994), *Managing Privacy: Information Technology and Corporate America*, Chapel Hill: University of North Carolina Press.

Solove, Daniel J (2008), *Understanding Privacy*, Cambridge: Harvard University Press.

US Department of Commerce (2010), Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework. Washington: Department of Commerce Internet Policy Task Force, December 16. Available at: http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf (Accessed April 11, 2011).

US Federal Trade Commission (1983), FTC Policy Statement on Deception: Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174, October 14. Available at: http://www.ftc.gov/bcp/policystmt/ad-decept.htm (Accessed February 2, 2011).

US Federal Trade Commission (2009), Federal Regulators Issue Final Model Privacy Notice Form, November 17. Available at: http://www.ftc.gov/opa/2009/11/glb.shtm (Accessed April 11, 2011).

US Federal Trade Commission (2010), *Protecting Consumer Privacy in an Era of Rapid Change: Preliminary Staff Report*, Washington: Federal Trade Commission, December. Available at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (Accessed April 11, 2011).

US Federal Trade Commission (2011), In the Matter of Google Inc., File No. 102 3136, March 5. Available at: Available at: http://www.ftc.gov/os/caselist/1023136/index.shtm (Acessed June 27, 2011).

Verizon Business (2011), *Verizon 2011 Data Breach Investigations Report*, Available at: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf (Accessed: April 27, 2011)

Westby, J.R. (2010), Governance of Enterprise Security: Carnegie Mellon CyLab 2010 Report, *BNA Privacy and Security Law Report*, 9 PVLR 915, June 21.

Xu, H., Dinev, T., Smith, H.J. and Hart, P. (2008), Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View, *Proceedings of the 29th International Conference on Information Systems*. Paris, December 2008. Available at: http://aisel.aisnet.org/icis2008 (accessed April 27, 2011).