Chapter 11
Data Breach Disclosure: A Policy Analysis

Melissa Dark
Purdue University,USA

ABSTRACT
As information technology has become more ubiquitous and pervasive, assurance and security concerns have escalated; in response, we have seen noticeable growth in public policy aimed at bolstering cybertrust. With this growth in public policy, questions regarding the effectiveness of these policies arise. This chapter focuses on policy analysis of the state data breach disclosure laws recently enacted in the United States. The state data breach disclosure laws were chosen for policy analysis for three reasons: the rapid policy growth (the United States have enacted 45 state laws in 6 years); this is the first instantiation of informational regulation for information security; and the importance of these laws to identity theft and privacy. The chapter begins with a brief history in order to provide context. Then, this chapter examines the way in which historical, political and institutional factors have shaped our current data breach disclosure policies, focusing on discovering how patterns of interaction influenced the legislative outcomes we see today. Finally, this chapter considers: action that may result from these policies; the action type(s) being targeted; alternatives that are being considered, and; potential outcomes of the existing and proposed alternative policies.

KEYWORDS: data breach, identity theft, privacy, data breach disclosure, policy analysis.

INTRODUCTION
Although advances in computing promise substantial benefits for individuals and society, trust in computing and communications is critical in order to realize such benefits. The hope for cybertrust is a society where trust enables technologies to support individual and societal needs without violating confidences and exacerbating public risks. Cybertrust, in part, depends upon software and hardware technologies upon which people can justifiably rely. However, the cybertrust vision requires looking beyond technical controls to consider how other forms of social control contribute to the state of cyber trust. This chapter focuses on public policy. While the chapter does not specifically use the word *ethics*, it should be noted that ethical issues and public policy are intimately intertwined. Policy is not formed in a moral vacuum; on the contrary, policy is inherently normative in that it prescribes, sometimes explicitly and often implicitly, what *should be*.

The increased reliance on and utilization of information technology in society has created the

need for new regulation regarding the use and abuse of these systems. We see this clearly just by briefly inventorying some of the regulations that have been enacted to protect security and privacy.

- Freedom of Information Act (1966)
- Fair Credit Reporting Act (1970)
- Bank Secrecy Act (1970)
- Privacy Act (1974)
- Family Educational Rights and Privacy Act (FERPA) (1974)
- Right to Financial Privacy Act (1978)
- Foreign Intelligence Surveillance Act (1978)
- Electronic Communications Privacy Act (ECPA) (1986)
- Telephone Consumer Protection Act (1991)
- Communications Assistance for Law Enforcement Act (1994)
- Driver's Privacy Protection Act (1994)
- Health Insurance Portability and Accountability Act (HIPAA) (1996)
- Computer Fraud & Abuse Act (1996)
- Children's Online Privacy Protection Act (COPPA) (1998)
- Digital Millennium Copyright Act (1998)
- Gramm-Leach-Bliley Act (GLBA) (1999)
- USA PATRIOT Act (2001)
- Federal Information Security Management Act (2002)
- Fair and Accurate Credit Transactions Act (2003)
- CAN-SPAM Act (2003)
- 45 State Data Breach Disclosure Laws[i] law (2003-present)

Eight of these laws were enacted between 1966 and 1986, while the last thirteen items in the list have been enacted between 1991 and 2009. This is not an exhaustive list, but it is representative and shows the increasing growth in legislation. This chapter focuses on the 45 State Data Breach Disclosure laws enacted in United States between 2003-2009 – a mere six year time span. Data breach has become a policy concern due to the rise in identity theft crimes and the erosion of privacy.

Identity theft is the crime of obtaining and using another person's personal information in order to commit fraud. There are four types of identity theft: (1) financial – illegally using someone else's identity to obtain good and services, (2) criminal – posing as another person when apprehended for a crime, (3) identity cloning – using another person's information to assume his/her identity in daily life, and (4) business/commercial identity theft – using another business' name to obtain credit (Identity Theft Resource Center, 2008). Identity theft is a concern because of the escalating incidence and costs for individuals, companies, and our nation. It is estimated that there were 8.4 million U.S. adult victims of identity fraud in 2007 resulting in losses of $49.3 billion (Javelin Strategy and Research Survey, 2007). A study by the Ponemon Institute (2008) surveyed 35 U.S. organizations and found the total average cost of a data breach in 2007 was $202.00 per record breached. The Privacy Rights Clearinghouse maintains a chronology of data breaches (www.privacyrights.org) that includes data elements considered useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. According to this chronology, there were approximately 34,000,000 records breached in 2008 in the United States.[ii] If the number of records breached and costs per breach in 2009 are commensurate with the 2008 costs, the estimated costs for data breaches 2009 will be $6,868,000,000 ($197 x 34,000,000).

Clearly, identity theft and data breach are an economic concern.

Escalating data breach problems further erode privacy. However, unlike identity theft, which has a legal definition and can be quantified in terms of incidents, privacy has no single definition or meaning. Generically speaking, privacy is the condition of being left alone, out of public view, and being in control of one's personal information. From a policy perspective, privacy can be classified in two basic categories: the reductionist view and the coherentist view (Schoeman, 1984). From the reductionist perspective all privacy claims are reducible to claims of other sorts, for example, property rights and trespass. According to this view, there is no purpose for considering privacy as a distinct issue of concern – existing policy can be extended to address it. In contrast, coherentism suggests that privacy consists of a number of fundamental, integrated, and distinct concerns. This view does not dispute what is addressed elsewhere. Rather, the coherentist concern is that disparate privacy components interact with each other and with other social priorities so that the whole of privacy is more than the sum of its parts. In which case, existing policies will not suffice. For both reductionists and coherentists, privacy begins with control of information, which is the ability to determine for ourselves when, how, and to what extent information about us is communicated to others (Westin, 1967). But for coherentists, privacy cannot be restricted to this 'information flow' definition. Doing so relegates it to the status of a moral or legal right, which is insufficient. The coherentist notion is that privacy is a condition (i.e., a state or modifying circumstance) that is inextricably linked to other desirable human conditions, such as human dignity, intimacy, social relationships, and personhood. Viewing privacy is this manner positions it as a collective good in addition to an individual good.

Given that information security and privacy are becoming more important, as evidenced by the growth in public policy, policy analysis in this area is timely and relevant. Policy analysis aims to address questions such the following. What do governments choose to do or not to do? How effective are the proposed or enacted solutions to public problems? How are issues that affect large numbers of citizens introduced to the public arena? What are the historical, political, and institutional factors that shape the formulation of public policy? In light of the relationships among policies, which of various alternative policies will be most effective in achieving a given set of social goals? How can policy making be improved through research and analysis?

This chapter seeks to advance information security and privacy policy analysis by specifically examining the data breach disclosure laws recently enacted in the United States. The background section includes a brief history of these laws and serves to provide context. The laws are analyzed using an institutional analysis and development framework (Ostrom[iii], 1999)[iv], which is overviewed in section two. Then, historical, political, and institutional factors that shaped our current data breach disclosure policies are analyzed with a focus on how patterns of interaction influenced the legislative outcomes we see today. In this way, the chapter is retrospective; we see how questions of *what should be* have shaped the current policy landscape. Last, this chapter considers how these policies may structure action with an eye toward alternatives and outcomes. In this way, the chapter is prospective and serves to question *what should be* moving forward.

BACKGROUND

Given that the data breach disclosure laws aim to ameliorate identity theft and privacy concerns, we start with an overview of other legislation in these areas. The first U.S. law that specifically addressed identity theft was passed in 1998 – the Identity Theft and Assumption Deterrence Act. The law was passed in response to the dramatic rise in identity theft in the 1990s. Prior to this act, ID theft was not regulated per se.

With regard to privacy, there is no provision for privacy in the U.S. constitution. There is no

independent privacy oversight agency in the United States, and the United States has no comprehensive privacy law. Instead, the United States has taken a sectoral approach to privacy regulation so that records held by third parties (such as financial and personal records at banks, educational and personal records at universities, membership and personal information at associations, medical and personal records at community hospitals) are generally not protected unless a legislature has enacted a specific law. As a result, we have a patchwork of laws enacted to address privacy and data security. These are outlined next, starting with the laws that pertain to the federal government, followed by laws that pertain to the private sector and finally, state laws.

Federal Laws

The Federal Trade Commission (FTC) Act was established by the Federal Trade Commission in 1914 with the purposes of promoting consumer protection and eliminating and preventing anticompetitive business practices. Jurisdiction of the FTC Act extends to a variety of entities. Section 5 of the FTC Act forbids unfair or deceptive practices in commerce, where unfair practices are defined as those that cause or will likely cause substantial injury to consumers. Section 5 of the Federal Trade Commission Act has been used with regard to privacy and security where companies have been accused of deceptive claims regarding use of personal information (e.g., Choicepoint). In 2003, the FTC Act was amended to include a provision regarding the privacy of consumers' credit data (the Fair and Accurate Transactions Act of 2003 - 15 U.S.C. 1681-1681x).

The Privacy Act of 1974 (5 U.S.C. 552a) governs the federal government's information privacy program. The intent of the Privacy Act is to balance the government's need to maintain information about individuals and the privacy rights of individuals. The Privacy Act protects individuals against unwarranted invasions of privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information (U.S. Department of Justice, 2008). The act was passed by the United States Congress in response to revelations of privacy abuse during President Richard Nixon's administration. A second goal of the Privacy Act is to address potential abuses stemming from government's increasing use of computers to store and retrieve personal data. The Privacy Act focuses on four basic policy objectives:

> (1) To restrict the disclosure of personally identifiable records that are maintained by federal agencies.
> (2) To grant individuals increased rights of access to federal agency records that pertain to themselves.
> (3) To grant individuals the right to seek amendment of federal agency records maintained on themselves given evidence that the records are inaccurate, irrelevant, untimely, or incomplete.
> (4) To establish a code of "fair information practices" that requires federal agencies to comply with statutory norms regarding collection, maintenance, and dissemination of records.

The Privacy Act specifies that agencies will not disclose any record that is contained in a system of records by any means of communication to any person or to another agency without the prior written consent of the individual to whom the record pertains - barring exceptions such as law enforcement. The Privacy Act also mandates that each federal agency have in place an administrative and physical security system to prevent unauthorized release of personal records. While the Privacy Act also applies to records created by government contractors, it does not apply to private databases.

The Federal Information Security Management Act (44 U.S.C. 3544) (FISMA), enacted in 2002, is the principal law governing the information security program for the federal government.

FISMA calls for agencies to develop, document, and implement agency-wide information security programs. This includes information systems used or operated by an agency or by a contractor of an agency. A goal of FISMA is to see that information security protections are commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. FISMA requires procedures for detecting, reporting, and responding to security incidents. Notification of security incidents must be provided to a federal information security incident center, law enforcement, and relevant Offices of the Inspector General. The Office of Management and Budget Breach Notification Policy, issued in 2007, reemphasizes agencies' obligations under the Privacy Act and FISMA by outlining two new privacy requirements and five new security requirements, which include explicit requirements for breach notification.

The Veterans Affairs Information Security Act (38 U.S.C. 5722) was enacted in 2006 in response to the May, 2006 breach of 26.5 million veterans' personal data. The Veterans Affairs Information Security Act requires the Veterans Administration (VA) to implement agency-wide information security procedures to protect the VA's sensitive personal information and information systems. While the VA Secretary is expected to comply with FISMA, this act includes other requirements not in FISMA, which are not specified here due to the narrow scope of this law, i.e., it only applies to the VA.

Private Sector Laws

In addition to the laws that shape the behavior of federal agencies, a suite of information security and privacy laws apply to the private sector. The two main laws are the Health Insurance Portability and Accountability Act (42 U.S.C. 1320) of 1996 (HIPAA) and the Gramm-Leach-Bliley Act (15 U.S.C. 6801-6809), enacted in 1999 (GLBA). HIPAA requires health plans, health care clearinghouses, and health care providers to ensure the privacy of medical records and prohibits disclosure without patient consent. While HIPAA includes privacy provisions, it is important to note that the primary purpose of HIPAA was job mobility. According to Hinde (2003):

> It was perceived that the disclosure of pre-existing medical conditions or claims to a new employer and that employer's health plan might discourage job mobility if those conditions were excluded by the new health plan insurer. Thus, the concept of providing privacy over identifiable information for those covered by the plan (p. 379).

The security standards that require health care entities to maintain administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic "protected health information" were added to HIPAA in 2003.

The Gramm-Leach-Bliley Act pertains to financial institutions. The impetus for GLBA was to "modernize" financial services. This included the removal of regulations that prevented the merger of banks, stock brokerage companies, and insurance companies. These financial institutions regularly bought and sold information that many would consider private, including bank balances and account numbers. Therefore, the

> removal of these regulations raised significant risks that these new financial institutions would have access to an incredible amount of personal information with no restrictions upon its use. Prior to GLBA, the insurance company that maintained your health records was distinct from the bank that

> mortgaged your house and the stockbroker that traded your stocks. Once these companies merged, however, they would have the ability to consolidate, analyze, and sell the personal details of their customers' lives. (EPIC, 2008).

GLBA requires financial institutions (businesses that are engaged in banking, insuring, stocks and bonds, financial advice, and investing) to safeguard the security and confidentiality of customer information, to protect against threats and hazards to the security or integrity of these records, and to provide customers with notice of privacy policies. Section 501 (b) of GLBA requires banking agencies to establish industry standards regarding security measures such as risk assessment, information security training, security testing, monitoring, and a response program for unauthorized access to customer information and customer notice. In this way, GLBA is considered self-regulatory because it calls for financial institutions to appoint an intermediary to determine best practices for information security and to monitor the performance of financial institutions against these industry standards.

State Data Breach Disclosure Laws

The most recent spate of activity is in the 45 state data breach disclosure laws. California was the first state to establish a data breach disclosure law in 2003; 10 other states enacted laws in 2005, 19 in 2006, eight in 2007, five in 2008, and two in 2009. Questions and concerns about the efficacy of these laws are many. All of these laws address three common elements: personal information definition, notification requirements, and notification procedures and timelines. However, the definitions of "personal information", "breach", "encryption", and "potential risk" are not consistent across the various state laws. This creates challenges for companies that operate in more than one state. The need to comply with multiple state laws can be cumbersome and costly. Thus far, we do not know if consumer notification is effective and under what circumstances. Given that the laws vary with regard to what is protected, to what degree, and when, consumer advocates fear that that lack of consistency diminishes the effectiveness of the laws. By allowing consumer rights to vary, consumers lose their power; by meaning many different things, these consumer protections mean no one thing. Questions also arise about the use of personal notification as a mitigation strategy. Is it effective, and if so, under what circumstances does it work? The next four sections discuss these definitions in greater detail highlighting the differences among the 45 state data breach disclosure laws.

Personal Information Definition

All of the data breach laws include a section that specifies the type of data that is subject to the breach law. All state laws cover a common set of data types. This includes an individual's first name or first initial and last name in combination with another identifying element, such as: (1) SSN; (2) DL number; (3) state ID number; (4) financial account number in combination with an access code, security code, or password; (5) credit card number in combination with an access code, security code, or password; or (6) debit card number in combination with an access code, security code, or password. However, this is where the commonality ends. Other data types covered in some states include checking account number, savings account number, personal identification number, electronic identification number, employer identification number, government issued ID number, routing code, digital signature, biometric data, fingerprints, account passwords (not in combination with other data), mother's maiden name, address, date of birth, medical information, DOT Photo Identification number, and telecommunications device. While there is consistency among states on six of the data items, there is variation on 17 other types of personal information that could be used to commit identity theft or other types of fraud.

Notification Requirements

Each data breach law includes a notification requirement that specifies the conditions under which covered entities[v] are required to disclose the breach; however, the details vary. Eighty percent of the laws require covered entities to provide a safe harbor for encrypted data. Safe harbor means that covered entities are exempt from having to disclose breaches when the data are encrypted. To make the situation even murkier, encryption standards are specified in some state laws (e.g., Maine, North Dakota, and Indiana), but not in other states (e.g., California, Arkansas, Louisiana, and Illinois). For those states where an encryption standard is specified, covered entities are expected to disclose if their encryption method does not meet the standard. In states that do not specify an encryption standard, covered entities are able to choose their own encryption method, which may or may not be "good enough". Some states (New York, North Carolina, and Pennsylvania) require that covered entities notify victims when encrypted data are breached and the encryption key has also been acquired.

In all 45 laws, the notification requirements describe the categories of covered entities. There are two broad categories: 1) entities that own or license computerized data, and 2) entities that maintain computerized data. Whereas all state laws apply to entities that own or license personal information, just over 50% of the state laws also apply to entities that maintain personal data. In general, covered entities are persons, agencies, and/or businesses that are required to provide notification; though in some states the law does not apply to state and local government agencies. For the most part, the state disclosure laws apply only to computerized data; however, the North Carolina and Wisconsin laws apply to paper records as well.

In all of the state data breach laws, the notification requirements define the trigger for notification. From this perspective, there are basically two types of laws: acquisition-based and risk-based. Acquisition-based laws require disclosure anytime the covered personal information has been acquired by an unauthorized person. Risk-based laws require notification only if there is "reasonable likelihood" of harm, injury, loss, or risk. It should be noted that "reasonable likelihood" is subject to interpretation. Twenty-two of the state laws are risk-based laws.

Notification Procedures and Timelines

All of the laws include a section that specifies the method of notification and the circumstances under which affected individuals are to be notified. The laws spell out the methods for notification, i.e., written notice, electronic notice, or telephone notice. All states allow for written notice; almost all allow for electronic notice, with the exception of North Dakota. Another anomaly is Indiana's provision for notification via facsimile.

Many state laws include a provision for substitute notice. Essentially this provision allows for email notification, website posting notification, or notification through statewide media based on a threshold. The threshold for when substitute notification is allowable is the cost of notification or the size of the affected class of residents. For example, a state may allow for substitute notification when the cost is expected to exceed $50,000 or the affected class of residents to be notified exceeds 100,000. There is considerable variation in the provision for substitute notification (some states do not provide for substitution), as well as variation in the threshold levels ranging from $25,000 to $250,000 for notification cost and 5,000 to 500,000 for persons affected.

A minority of states specify a time limit for notification. More state laws address the timeline vaguely as the "most expedient time possible" and "without unreasonable delay", where notification time can be affected by allowing the covered entity the opportunity to (a) determine the scope of the breach, and/or (b) restore system integrity, and/or (c) notify law enforcement.

Law enforcement officials can then delay notification further if it is deemed that notification would impede an investigation or jeopardize national or homeland security.

Several states require notification of other parties besides the individuals directly affected by the breach. For example, in some states covered entities must notify consumer reporting agencies and state agencies such as the Attorney General, the State Police, the Department of Justice, the Consumer Protection Board, the Cyber Security and Critical Infrastructure Coordination Office, and so on. Most state laws require notification to consumer reporting agencies. The three national consumer reporting agencies are Equifax Credit Information Services, Inc.; Trans Union LLC; and Experian Information Solutions, Inc. However, there is variation among the states regarding the threshold at which notification beyond the consumer is required. For example, in Minnesota the covered entity must notify the consumer reporting agencies if the breach exceeds 500 state residents; in Georgia the threshold is 10,000.

Other

A minority of the state data breach notification laws include requirements for data protection and secure data destruction and disposal. When information security provisions are included, the law is transformed from being just a data breach disclosure law into also being an information security law. Many would contend that improving information security is perhaps the most essential part of reducing identity theft.

The state data breach disclosure laws vary with regard to penalties. Fewer than half of the states include stipulations for monetary penalties, and the amount of the penalty varies widely. Some states allow for private right of action against companies for breached data while other states rely solely on the State Attorney General's office for enforcement. For example, West Virginia specifies that no civil penalty shall exceed $150,000 per breach or series of breaches discovered in a single investigation. Alaska violators are liable to the state for a civil penalty of up to $500 for each state resident who was not notified, but the total civil penalty may not exceed $50,000. Rhode Island delimits the penalty to no more than $100 per occurrence and no more than $25,000 adjudged against a defendant.

State laws also vary in their protections to consumers. Fewer than 20% of the state laws include a provision for a security credit freeze, which prohibits credit agencies from releasing consumer credit information without the express authorization of the consumer. This provision shows that some states believe that part of the solution is to provide consumers with more ability to take action to protect themselves and information on how to do so. The disparity among states reflects, in part, differences in the perceived importance of consumer rights and education.

The patchwork of 45 state data breach notification laws presents challenges. Interstate businesses say that their firms have difficulty complying with dozens of state laws. Critics also contend that the potential volume of notifications is a concern. As notifications increase we risk consumer desensitization and could lead to consumers' inattention to the risk, which would be counterproductive.

Need for Change

The clarion call is that we are drowning under a myriad of different state data breach notification laws, thereby making a federal data breach notification law imperative. In response, a number of federal data breach notification bills have been introduced in the past four years. These include the following from the 109th Congress (GovTrack.us), which spanned 2005-06:

- S. 115 - Notification of Risk to Personal Data Act

- S. 116 - Privacy Act
- S. 500 - Information Protection and Security Act
- S. 751 - Notification of Risk to Personal Data Act
- S. 768 - Comprehensive Identity Theft Prevention Act
- S. 1216 - Financial Privacy Breach Notification Act
- S. 1336 - Consumer Identity Protection and Security Act
- S. 1408 - Identity Theft Protection Act
- S. 1789 - Personal Data Privacy and Security Act
- H.R. 1069 - Notification of Risk to Personal Data Act
- H.R. 1080 - Information Protection and Security Act
- H.R. 3140 - Consumer Data Security and Notification Act
- H.R. 3997 - Data Accountability and Trust Act
- H.R. 4129 - Data Accountability and Trust Act
- H.R. 5318 - Cyber-Security Enhancement and Consumer Data Protection Act

While all of these bills are dead, the discussion of preemptive federal law continues. The Senate Judiciary Committee of 111th Congress is trying to move forward a cybersecurity bill (the Personal Data Security and Privacy Act of 2009) that includes data breach notification.

The debate continues as to the needs of business versus consumer groups. As business vies for a high threshold for notification due to notification costs time, money, and reputation, consumer groups contend that higher thresholds don't grant enough notice to consumers. Questions of what *should be* with regard to identity theft, privacy, and security remain salient.

POLICY ANALYSIS

We now turn to a discussion of the policy analysis. The discussion is divided into three parts. First we look at the analytic framework used in this chapter, Ostrom's Institutional Analysis and Development (IAD) framework, and its general principles. Then, in a retrospective analysis, we use the model to consider why and how we arrived at the development of the 45 existing data breach laws. The state of information assurance and security is shaped by historical and institutional factors and it behooves us to consider these factors. Finally, we explore the anticipated effects of these laws in a prospective analysis.

IAD Framework

The IAD framework is associated with the social theory of new institutionalism, which grew out of institutionalism. Institutionalism studies formal institutions, such as organizations, norms, laws, and markets. New institutionalism adds to this the study of how institutions operate in a context. In new institutionalism, institutions are abstractly defined as "shared concepts used by humans in repetitive situations organized by rules, norms and strategies" (Ostrom, 1999, p. 37). New institutionalism considers topics such as how individuals and groups construct institutions, how institutions function in practice, how institutions interact and affect each other, the effect that the sociological environment has on these interactions, and the effects of institutions on society. Institutions are both the entities themselves, as well as things (rules, norms, strategies) that shape the patterns of interaction across entities.

Interestingly, while these rules and norms are powerful, they are largely invisible, which makes identifying and measuring them hard to do (Ostrom, 1999). They can be described, but not precisely. This is relevant as readers will clearly see that this chapter uses qualitative descriptions to depict institutions in action, but we offer no quantitative measures. Readers should also keep in mind that all description of this type, by nature includes connotation, which cannot be avoided.

After all, norms exist in us, not apart from us. Therefore, this chapter is subject to the author's bias. It is left to the readers to improve upon this work. It is incumbent on all who are interested in such research to be aware of, and guard against, personal biases where they may limit findings.

We begin discussion of the IAD framework (shown in Figure 1) with the action arena in the middle. The action arena includes the action situations and the actors. In describing the action situation(s), the analyst attempts to identify the relevant structures, i.e., those affecting the process of interest. This can include participants, allowable actions and linkages to outcomes, the level of control participants have over choice, information available to participants, and costs and benefits assigned to actions and outcomes. The analyst also identifies the pertinent actors. Actors are individuals and groups (entities) who take action, i.e., they behave in a manner to which they attach meaning, either subjective or instrumental. Moving to the right in figure 1, the IAD model includes outcomes. Outcomes are observed, inferred, and/or expected behaviors or results.

Figure1. Institutional analysis and development framework. Adapted from P. Sabatier, 1999.

Action arenas can also be viewed as dependent variables. In this way, the analyst looks at how rules-in-use, attributes of community, and physical/material conditions influence the action arena. Rules-in-use are shared understandings about what is expected, required, and allowed in ordering relationships. Physical/material conditions refer to the characteristics of the states of the world as they shape action arenas. Clearly, what is expected or allowed may be conditioned by what is physically or materially possible. Likewise, rules-in-use might be shaped by physical conditions and vice versa. Attributes of community are nonphysical conditions that provide structure to the community. Attributes of community may or may not be shaped by physical conditions and can serve to influence rules-in-use and the utilization of physical conditions. Using the IAD model, one can also study how outcomes influence physical conditions, attributes of community, and rules-in-use. The IAD model assumes that social systems are continually constituted and reconstituted; in this way, both the systems and the models to analyze them are organic in their worldview.

The IAD model includes four levels of analysis: operational, collective, constitutional, and metaconstitutional. Any of the units (action situation, actors, patterns of interaction, outcomes, rules-in-use, attributes of community, and physical/materials conditions) could be identified at any, some, or all of the four levels of analysis. The analyst can, for example, consider the nested structure of rules within rules, i.e., how do the structures and rules of a constitutional government shape constitutional choice, and then how does that shape collective choice and operational rules and how do these influence the action arena? Or how does the action arena at a collective level interact in such a way as to influence attributes of community at the constitutional level, and what does this suggest for patterns of interaction or outcomes? The power of the model is in its general nature; any one use of the model (including this one) is not likely to include all units of analysis or all levels.

Readers should note that the IAD model does not prescribe how analysis is performed. The arrows are not meant to suggest that the analyst needs to work through the model in full, or from left to right. So, for example, an analyst can work from 1) the action arena to 2) outcomes in an effort to discern or predict patterns of interaction. Another alternative would be to work from 1) observed outcomes to 2) effects thereof on rules-in-use or attributes of community. Or the analyst can work across levels, e.g., investigating how do collective choice rules-in-use such as excludability and the free-rider problem influence what type of operational policy can be enacted? This is the power of this model, which is partly why it was chosen for this analysis.

The IAD model is especially useful for analyzing self-governing entities. The defining characteristic of a self-governing entity is that individuals influence the rules that structure their lives. More specifically, the members (or their representatives) of a self-governing entity participate in the development of the collective-choice and constitutional rules-in-use. Self-governing entities are complex, adaptive systems in that they are comprised of a large number of elements interacting in multiple ways; the interactions change the system, which shapes future interactions such that outcomes are hard to predict, and thus, considered emergent. Self-governing entities are polycentric where citizens organize multiple governing authorities and private arrangements at different scales. A constitutional government is a self-governing entity; the author contends that the Internet is also a self-governing socio-technical entity. Public policy in information assurance and security then is about how a polycentric system governs a polycentric system, which is the second reason why the IAD framework was selected for this research.

Retrospective Analysis

In the retrospective analysis, we consider the rules-in-use, attributes of community, and physical and material conditions that served to shape the policy actions we have seen until now. To date, public policy in information security and privacy in the United States has been largely incremental in nature. We can see from the patchwork of laws discussed earlier in this chapter that we have, thus far, resisted a coordinated, federal law that preempts existing legislation. Incrementalism is common in self-governing, polycentric entities. In policy analysis, incrementalism assumes 1) that the effects of seriality enhance outcomes by reducing uncertainty, and 2) enhanced consideration of context enhances outcomes. That the information age has introduced a number of uncertainties makes incrementalism especially relevant.

Stated more directly, and in connection to the IAD model, one of the rules-in-use is incrementalism. When there is a high degree of uncertainty, policy will be enacted incrementally. Thus, the plethora of laws we have is to be expected. While identity theft is nothing new, the magnitude of identity theft that we have experienced in the past decade is new. The global information infrastructure is in its infancy – we are still learning what people will and will not do in the electronic frontier. The Internet was never designed to serve the myriad of purposes for which it is being used, nor was it designed for billions of users. Through trial and error we are learning how laws that were crafted for the industrial era do, and do not, apply in the information age. We have yet to learn what new laws are needed as a result of information technologies. We have yet to learn how effective these laws will be.

During this period of transition, new communities are being formed and existing communities are being reshaped; as a result, behavioral norms are being renegotiated. Given the global nature of the Internet, it is reasonable to view these communities as more heterogeneous or, at a minimum, heterogeneous in new ways. Therefore, norms probably cannot be easily transported from based on existing communities; they will have to be established from the ground up, which is bound to take time. Additionally, because the technology is still new, scientists and engineers are still determining what actions are physically possible. Talented individuals around the world are working on technologies to help anonymize data, enhance privacy-preserving computation, and provide improved intrusion detection, but this takes time as well. Experience in all of these areas – rules-in-use, attributes of community, and physical/material conditions – will be gained through observation, involvement, and exposure.

Though we don't have much experience, there has been the need to take action. Identity theft is on the rise and citizens are concerned. Two of the core imperatives of the state are domestic order and legitimacy (Dryzek, Downes, Hunold, Schlosberg and Hernes, 2003). Yet, the existing

federal and private sector laws are not sufficient to address the rising identity theft problem threatening domestic order, thereby forcing lawmakers to take action to ensure their perceived legitimacy. In response, federal laws have been amended, private sector laws are being tweaked, and a flurry of state laws have been enacted. To what can we attribute the incremental changes we have observed? Why do we have these laws as opposed to something else? To answer these questions, we turn to a discussion of openness and transparency, informational regulation, the infancy of the information industry, and federalism; and we further examine how rules-in-use, attributes of community, and physical/material conditions have intersected in each of these areas to produce the policies we have today.

Openness and Transparency

A democracy is founded on principles of openness and transparency. In 1933, Justice Louis D. Brandeis coined the powerful phrase "sunlight as disinfectant" in support of increasing openness and transparency in public policy. While laws that aim to ensure openness and transparency in government operations existed before 1933, Brandeis is responsible for the term 'Sunshine Laws'. The impetus behind sunshine laws is twofold. First, a thriving, open democracy depends on open access and citizen participation, thus the right-to-know is a constitutional and inherent right of American citizens. Second, a government that is of the people, for the people, and by the people asserts government subservience to the individual, which predicates freedom of information.

The Freedom of Information Act (FOIA), signed into law on July 4, 1966 by President Lyndon B. Johnson, is a sunshine law. FOIA allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States government. The concept of "freedom of information" conveys a philosophy that values the advantages of increasing our ability to gather and send information, and clearly does not connote privacy as a positive right. This acts as a rule-in-use.

The Privacy Act of 1974 arrived eight years later as an amendment to the FOIA in response to Watergate and the abuse of privacy during the Nixon administration. The Privacy Act of 1974 was passed not to promote privacy, but to establish a code of fair information practice. It was also an attempt to limit the powers of government and was passed hastily during the final week of the 93rd Congress, which was in session from 1973-74. According to the U.S. Department of Justice,

> no conference committee was convened to reconcile differences in the bills passed by the House and Senate. Instead, staffs of the respective committees -- led by Senators Ervin and Percy, and Congressmen Moorhead and Erlenborn -- prepared a final version of the bill that was ultimately enacted…the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply. (U.S. Department of Justice, 2008).

Moreover, even after more than twenty-five years of administrative and judicial analysis, numerous Privacy Act issues remain unresolved or unexplored. Adding to these interpretational difficulties is the fact that many Privacy Act cases are unpublished district court decisions.

This offers important insight into the historical context with regard to how information and privacy are embedded in the past and offers food for thought on how this norm has shaped our ongoing collective treatment of it coming forward. Through the enactment of FOIA in 1966, we see the push to enable information sharing as a result of mistrust in government. Eight years later we see The Privacy Act, which is reactive in nature and also reflective of distrust of government.

Through these pieces of legislation we find two noteworthy threads. First is the value of freedom of information, wherein information belongs to and exists for the advancement of citizens and the common good. This is coupled with an interesting distrust of government powers, wherein stewardship cannot be entrusted to the polity. Privacy in the Privacy Act is not a positive right, but rather is a necessary provision subservient to limiting government powers.

Earlier it was noted that HIPAA was passed to enable job mobility and GLBA was passed to modernize the financial services industry. Again, we see in the context of these laws that privacy is secondary to another purpose. In HIPAA and GLBA, privacy is cast as a means to an end; in other words, privacy plays a functional or instrumental role. We need privacy because we need job mobility; we need privacy because we need to modernize financial services. Implicit is the message that if we did not need job mobility or financial services modernization, we would not need to concern ourselves with privacy. Even though privacy was cast as a functional need in both HIPAA and GLBA, the similarity ends there. These industry sectors have significantly different regulatory frameworks (Congressional Research Service, 2008). What we see in the security and privacy provisions in these laws is more reflective of the larger regulatory framework for these industries. The regulatory framework for these industries served as additional rules-in-use, shaping these laws.

Informational Regulation

Another phenomenon that is essential to understanding the U.S. data breach laws is informational regulation. Informational regulation has become a striking development in American law (Sunstein, 2006). To date, informational regulation has been applied in the environmental and health policy arenas. The fact that informational regulation has been applied to environmental and health policy is noteworthy. In the case of environmental policy, informational regulations has been used to protect aspects of the environment that are *common (or public) good* in nature, which by definition means that the private sector will not attend to them. A similar situation occurs in public health where the health of all citizens is both good for the individual as well as for the collective as a means and an end, i.e., it is a common or public good.

Informational regulation has two functions. First, it serves to inform people of potential risk exposure (Volokh, 2002) and serves as "sunlight", which we already discussed as the value of transparency. Second, it aims to change the behavior of risk creators (Volokh, 2002) and aims to exert pressure on entities to care for the common good. Informational regulation is useful in a polycentric policy arena where the problems that the policy is meant to address are attributable to multiple sources, the solutions require participation from multiple parties, and the nature of problems and solutions is dynamic; all of which necessitate that the policy must allow for adaptability. Clearly caring for the environment or health are polycentric policy areas. Environmental and health problems stem from multiple sources and ameliorating these types of problems takes ongoing involvement from multiple parties. The same is true for data security, identity protection, and privacy. Improved data security is possible only under conditions that shape the practices of numerous individuals and covered entities; therefore, policy that provides incentives for such change is, in theory, necessary. How does informational regulation work in practice?

Figure 2 shows the mechanistic view of informational regulation for data breach. We start with consumers. Informational regulation intends to provide warning information to consumers. In theory, by enhancing the knowledge level, consumers can perform a personalized risk assessment and make purchase decisions based on that assessment. The market decisions made by consumers intend to drive the less secure entities out of the market, thereby improving the state of security overtime. In addition, the enhanced knowledge levels will propel consumers to engage in other

protective actions, such as active credit monitoring or a credit freeze. Consumer credit monitoring typically includes alerting the bank and credit card merchant, notifying the FTC, and/or contacting law enforcement. A credit freeze allows the consumer to lock their consumer credit report and scores. Once a consumer has locked their credit information, the lender or merchant cannot access it, which significantly lowers the likelihood that the merchant will issue credit. The benefit is that the thief is not likely to get credit in the consumers' name (so the law prevents a false positive, also called a Type II error). The downside is that this also impedes consumers from quickly getting credit in their name (a false negative or Type I error); note, that consumers can release the freeze, but it takes a few days and may jeopardize quick access to special loans and other purchase incentives. These proactive consumer measures will in theory also lead to improved security over time.

Informational regulation also aims to change the actions of producers. By engaging producers in providing information, informational regulation, in theory, reveals an entity's practices. This sends a signal to society that perhaps this entity cannot be trusted. The premise is that covered entities value their reputation. As such, they will act to improve their security in order to preserve their reputation and minimize associated costs, which could include the costs of the notification itself, as well as downtime costs, costs of remediation and recovery due to the breach, and the costs of lost business. Ideally, these two streams combine to improve data security, which in turn mitigates identity theft and enhanced privacy.

Figure 2: Informational regulation premise for data breach disclosure laws.

The premise of informational regulation is that (1) market mechanisms can be used to shape risk behavior, thereby reducing the need for command-and-control regulation, and (2) it enhances democratic processes and promotes individual autonomy. By providing data breach information to victims, individuals are empowered to make decisions based on quality (i.e., they can elect to purchase goods/services from a provider who offers enhanced information security and privacy), and market mechanisms will be fortified. A failure to provide complete and accurate market information can impede the efficient allocation of goods and services and result in market failure, which is the driver for changing producers' behavior.

In theory, informational regulation allows more public monitoring of decisions, a norm already discussed. By forcing disclosure, more people are informed; and by informing more people, the quality and the quantity of public deliberation will improve, thereby enhancing the democratic processes that are vital for openness and transparency. In general, information disclosure rests on the normative belief that citizens have a right to know the risks to which they are exposed. This information promotes choice and autonomy, both of which are foundational to what some may consider the penultimate norm in American society: liberty (Renshaw, 2002).

In contrast to command-and-control regulation where the government sets and enforces standards, informational regulation is often less expensive. In the United States, we value efficient government and recent decades have seen an increased emphasis on downsizing the federal government. While it is not clear that command and control legislation would be effective in mitigating data breaches or in making data breach disclosure more effective, it is clear that a command and control approach is not politically efficacious at this point in time.

In summary, informational regulation has grown in areas where consumer protection, private sector practices, and risk converge. Examples include warning labels regarding mercury levels, nutrition labels disclosing fat contents, and notifications about the side effects of a given medication. That data security shares these same material features – consumer protection, private

sector practices, and risk – has clearly contributed to adopting informational regulation as the model for data breach disclosure laws.

Infancy of the Information Industry and Federalism

Here we pick up a thread that was started earlier, namely our relative inexperience with the information age, and add a few contours. The information industry includes 1) industries that buy and sell information as a good or service, 2) certain service sectors that are especially information intensive, such as banking and legal services, 3) information dissemination sectors, such as telecommunications and broadcasting, and 4) producers of information processing devices, such as computers and software. The information industry is seen as a boon to the economy as information amplifies growth in more traditional industry sectors and the demand for information goods and services increases markedly. Because of this ends and means nature of information goods and services, the market is quite large and still emerging.

An example of emergence is the following relatively recent cascade of events: the Internet explosion; September 11, 2001; and the subsequent war on terror. These events converged to boost the data brokerage industry. Data brokerages are companies that collect and sell billions of private and public records containing individuals' personal information. Many of these companies also provide products and services, including identity verification, background screening, risk assessments, individual digital dossiers, and tools for analyzing data. Most data brokers sell data that they collect from public records (e.g., driver's license records, vehicle registration records, criminal records, voter registration records, property records, and occupational licensing records) or from warranty cards, credit applications, etc. In addition, data brokers purchase so-called "credit headers" from credit reporting agencies. Information on a credit header generally includes a person's Social Security number, address, phone numbers, and birth date (Congressional Research Service, 2007). Although some of the products and services provided by data brokers are currently subject to privacy and security protections aimed at credit reporting agencies and the financial industry under the Fair Credit Reporting Act (1971) and Gramm-Leach-Bliley Act (1999), many are not. Because the industry is relatively young, there is no history of oversight or self-regulation of the industry's practices, including the accuracy and handling of sensitive data, by an industry-sanctioned body.

Data brokerages are not the only unregulated entities. There are many other organizations that process, store, and transmit personal information: state and local agencies, public hospitals, departments of revenue and motor vehicles, courts at the state and local level, agencies that oversee elections, K-12 schools, school districts, post-secondary institutions, and business entities engaging in inter- and intrastate commerce. Most of these entities are not covered by HIPAA and GLBA (Congressional Budget Office, 2006) and have traditionally been governed through state law; hence the 45 state data breach laws discussed earlier. The suite of laws we have is in part a result of our lack of experience with information markets and partly a function of our need for legislation that spans the numerous and varied types of entities that process, store, and transmit personal information. A broad and amorphous social challenge such as information security and privacy is not only diffuse, it is emergent. Research has shown that in cases of open-access, common good resources (such as security and privacy), collective choice action arenas, i.e., those that improve opportunities for communication and public deliberation, result in better joint outcomes (Ostrom, 1999). The patchwork of data breach laws we have fit this profile – they aim to increase the communication and public deliberation.

In a federalist system, such as the United States, sovereignty is constitutionally divided between the federal government and the constituent states. The powers granted to the federal government in the United States are limited to the right to levy taxes, declare war, and regulate interstate and

foreign commerce. The powers traditionally reserved by the states include public safety, public education, public health, transportation, and infrastructure. Of course, information security and privacy challenges permeate these state governed organizations too. While a federal, preemptive law might span all organizations and individuals, there is the possibility that it would erode state sovereignty and in the process alter the federal-state balance of power in unprecedented ways. The patchwork suite of laws we have can be partially attributed to a collective belief that this would be wrong.

In summary, this retrospective analysis provides nuanced insight into the present. Federal laws were enacted to delimit government powers and privacy was seen as necessary for that. Private industry sector laws were passed to innovate the private sector, and data security and privacy were included as functional means to that end. These federal and private sector laws reflect a general cultural norm in the United States of distrusting government while trusting in the private sector and market forces. Informational regulation was established as a form of legislation considered effective for issues that spanned consumer protection and risk, and where market mechanisms would/could work effectively, which is further evidence of pervasive trust in the private sector. Social and economic factors coupled with technological advancements are changing the landscape considerably. The problem is highly polycentric and emergent, and these conditions favor polycentric and incremental policy approaches. The resulting set of data breach laws put data security into the hands of citizens and organizations. In a society pillared by equity and freedom as ideals, and where there is no constitutional provision for privacy, the constant for deliberating the common good is through an open and representative process. This myriad of data security laws aims to serve the purpose of making explicit these individual preferences in a manner that allows all to translate these preferences into collective choice – the future of data security is contingent on us all.

Prospective Analysis

Because the data breach disclosure laws are so new, many of the interactions and outcomes are yet to be realized. Hence, this discussion is prospective in nature. First, we explore alternative policy configurations as a type of outcome. Then, we consider possible interactions and outcomes if these laws remain as they are today.

Alternative Policy Configurations

Alternative policies are not policy outcomes in the truest sense. Public policies don't intend to make more public policy. Rather, public policies intend to ameliorate a social problem or advance a social good. However, policy modifications frequently are the intermediate (incremental) outcome of policy making, especially in nascent issue areas embedded in self-governing action arenas. And so it is here that we begin.

The policy alternatives being considered vary according to how problems with the current policies are perceived. Embedded, either implicitly or explicitly, in the different criticisms are expectations for what outcomes the data breach disclosure policies aim to achieve and how. For sake of simplicity, the alternatives can be classified into two categories: 1) variations of existing laws using incremental approaches to 'fine-tune' the efficacy of the laws, and 2) introduce new laws, which could include comprehensive and preemptive federal legislation that is regulatory in nature and/or the application of tort liability to redress problems of negligent security. Some proposed alternatives are hybrid in that they include tweaking existing laws as well as the introduction of preemptive federal legislation with the caveat that when a state or industry sector law has higher requirements than the federal legislation, it shall prevail.

The first proposed alternative assumes that the premise of current laws is, for the most part,

sound, but suggests that there are some minor flaws. However, there is considerable disagreement regarding how the existing laws are flawed. Some critics note that the outcome of data breach disclosure should be to motivate large-scale reporting so that data breaches and trends can be aggregated, which allows a more purposeful and defensive use of incident data. Those who advocate for large-scale data collection view the existing laws as "disclosure disincentives". This stems from two sources. First, breached entities view themselves as victims of attack and not deserving of reputational repercussions. Second, existing laws offer covered entities considerable discretion as to whether to disclose. Together, these factors result in underreporting of data breaches, which in turn constrains large-scale data collection regarding breaches.

The proposed policy solution is to modify the laws to make breach notification completely anonymous where breached entities report to an intermediary and not to consumers. Advocates of this approach contend that disclosing the locus of the breach to consumers is practically worthless; because consumers at this time generally either cannot, or choose not to, use this information for discriminatory purchasing, which is a premise of the legislation. Another benefit cited by advocates of anonymous disclosure is that it removes the requirement to postpone disclosure until law enforcement assures it will not conflict with an investigation, which enhances timely response to the breach. In summary, the net outcome gain of this alternative is viewed as increased and timelier disclosure. While advocates of this approach purport that we do not lose anything with this approach, for those who agree that data security is a polycentric problem needing polycentric solutions, omitting the consumer from participation may be viewed as undesirable at best and opaque and unparticipatory at worst.

The second incremental alternative is a coordinated response architecture, also called CRA (Schwartz and Janger, 2007). Advocates of this alternative agree that large-scale data collection on data breaches is needed, but contend that consumer notification needs to be amended, not eliminated. Their main concerns with the existing consumer notification practices are that 1) there are too many notifications, leading to consumer desensitization and 2) the information provided to consumers is unhelpful at best and befuddling at worst. In response, this group advocates for amendments to the data breach laws to include a CRA. The CRA is an intermediary agency with responsibility for 1) supervised delegation of the decision whether to give notice, 2) coordination and targeting of notices to other institutions and to customers, and 3) tailoring of notice content. Regarding notification to consumers, this policy alternative calls for a bifurcated notification scheme that includes notification to consumers based upon a *reasonable likelihood of harm or risk* and notification to the intermediary based upon a *reasonable likelihood of unauthorized access*. Under this policy alternative, the threshold for notification to the intermediary would be lower than the threshold for notification to the consumer; therefore breach information will be provided to the central intermediary while at the same time mitigating the concern of over-notification to consumers. The third policy change is that the CRA will play a role in mandating the inclusion (e.g., specific steps to take to place a credit freeze) or omission (e.g., marketing of security services that the breached entity is selling) of certain content in notification letters, so as to minimize consumer confusion and cynicism. Because the intermediary could potentially have tomes of personally identifiable information making it an attractive target, the policy would also call for establishment and implementation of data minimization principles for the CRA. Last, a recommended policy change would provide incentives for disclosure by offering companies a chance to avoid consumer notice through early reporting and cooperation, and a disincentive through a statutory fine of $500 for each failure to notify.

In contrast to tweaking existing laws, new laws are still being debated. For example, the discussion of a preemptive and uniform federal data security law continues. Proponents of this approach say that omnibus legislation provides for greater certainty in courts, reduces confusion

and cost for entities that need to comply, and could provide for enhanced enforcement through private right to action. The difficulty in the uniform preemptive federal law is what it should include. Companies like the risk-based provision for notification, which reduces the burden on them, while consumer groups prefer the acquisition-based approach. Some companies, especially the smaller ones, prefer fewer information security requirements because they are costly and therefore more onerous for the smaller entities to incur. Small business advocates weigh in by noting that hefty information security requirements could be so costly as to disadvantage small companies from entering the market. Larger companies are generally less concerned with the information security requirements and more concerned with how to control for reputational damages from a massive data breach. Generally speaking, companies prefer less enforcement, while consumer groups advocate for more enforcement to include private action. The ultimate question for the policy makers is which action(s) to target given that no one law can strive toward them all.

Given that government regulations may not be enough, another alternative is tort liability. The reasoning is that applying common law rules to redress problems of negligent information security will motivate businesses to enact better policies and procedures, and comply with industry standards in a more effective manner than a one-size-fits-all government regulation could (Picanso, 2006). While not insurmountable, the following challenges would need to be addressed in order for tort law to protect personal data: determination of whether such a duty exists, defining a standard of care (no small feat given that emergent nature of security vulnerabilities), and accounting for intervening acts of third parties that would break the chain of causation.

Others support a mix and match set of alternatives. One example is a preemptive federal law in conjunction with tort laws and existing state laws, where the scope of preemption is fairly narrow. The justification is that such a policy mix would allow greater stringency, and therein sovereignty, in state laws as desired by states, but provide for certain requirements in a federal law in areas that are considered crucial to improving security. A few of the suggested requirements for a federal law are as follows. A federal law should specify an encryption standard and allow an exemption from disclosure when breached data are encrypted and standard compliant. According to advocates, this would entice more companies to use encryption and deter companies from purchasing inexpensive, ineffective encryption just for the sake of compliance. A federal law should mandate that all thresholds for disclosure be based on risk as opposed to acquisition, which would reduce over-notification and consequent desensitization.

Each of the alternatives offers a critique of the existing suite of laws. Each critique is grounded in a premise of what outcomes matter and each alternative offers a view on how policy can/should target actions in pursuit of these outcomes. However, another option is to make no policy change at this juncture. Here we turn to a discussion of anticipated interactions and outcomes of existing laws.

Interactions and Outcomes of Existing Data Breach Disclosure Laws

As previously mentioned, the IAD framework includes four nested levels of analysis: operational, collective, constitutional, and metaconstituional. Policy analysis at the operational level considers rules that affect day-to-day decisions made by participants. Policy processes at the operational level address issues of appropriation, provision, monitoring, and enforcement. The policy alternatives discussed above are at the operational level; for example, inserting an intermediary to allow large-scale collection of data breach information and trends to enhance monitoring. The collective-choice level is where decision-makers create rules to impact operational level activities and outcomes. Policy processes at the collective-choice level focus on

policy-making and management. For, example, a group of farmers changing the way they share a water resource for irrigating their crops is a collective choice. The utilization of market forces for data breach and information security was a collective choice. The constitutional level includes rules to be used in crafting the set of collective-choice rules that in turn affect the set of operational rules. Policy processes at the constitutional level focus on policy formulation, governance, adjudication, and modification. For example, voting rules that specify how collective-choice members will be selected. The metaconstitutional level includes basic principles from which constitutional situations derive and affect all of the other levels. The metaconstitutional outcomes affect constitutional decision-making, which, in turn, shapes collective-choice decision-making, which, in turn, shapes operational decision-making. Here we consider possible interactions and outcomes of the existing data breach disclosure laws, first at the collective-choice level and then at the constitutional level.

Collective-Choice

The overriding collective-choice premise of the data breach disclosure laws is the use of market forces to stem the tide of data breach, which has implications for identity theft, information security, and privacy. Therefore, the significant question is whether informational regulation is the right model for regulation for this problem space. Will market forces work effectively or will citizens perceive that covered entities are victims too, and in that regard choose to not punish them by purchasing elsewhere? The dependencies presented in figure 2 make many assumptions. The data breach laws assume that: consumers are notified, become knowledge and then take action; covered entities are exposed, suffer reputational loss, and incur costs, which motivate them to invest in information security; market forces drive entities that don't improve security out of the market; and the combined forces raise the tide of security. And as a result identity theft is mitigated and privacy improved. Is this the case?

As we know, policy in polycentric problem arenas is meant to address how multiple sources contribute to a dynamic problem. Thus, policy solutions require participation from multiple parties and must allow for adaptability. What do we know about the polycentric problem space? Data breach notification and data security are not the same thing. Data security and privacy are not the same thing. Privacy and identity theft are not the same thing. Identity theft and data breach are not the same thing. However, together they appear to constellate a polycentric problem arena.

While the premise that data breach is correlated to identity theft is plausible, a 2009 report by the American National Standards Institute (ANSI, 2009) looked at 166 studies investigating identity theft, data breach, identity theft protection, and information security. The ANSI report found several notable gaps in research. The research gaps range as follows: a lack of empirical research correlating data breach and identity theft; a lack of research investigating data traders' activities to consumers victimized by identity theft; a lack of studies on the efficacy of existing laws; and a lack of studies investigating whether and how information security solutions prevent identity theft. We need to know more about the relationship between data breach and identity theft if we want to evaluate data breach laws by their ability to reduce identity theft. If, on the other hand, there is little relationship between the data breach and identity theft, then it is not useful to evaluate the laws according to their impact on identity theft. If on the other hand there is a notable relationship, yet the laws do not seem to be mitigating identity theft, then we can be more certain that the laws are ineffective. The data breach disclosure laws assume that through the use of market forces the state of security will ultimately improve. The recent ANSI (2009) report notes that, as of now, there is no empirical basis to suggest the effectiveness of information security solutions correlate to identity theft and data breach. Again, knowing more about the interrelationships of the problem can inform policy analysis and future policy making.

Addressing questions such as these, however, is not easy. There are some existing studies that we can use. For example, the Javelin Strategy and Research Identity Fraud Survey Report (2008) includes measures such as consumer trust, intention to purchase in the future, and consumer credit monitoring. The Ponemon Institute study (2008) includes measures such as total cost, cost in different categories (e.g., cost of notification, cost of lost business, and cost by breach type). The concern is that while such sources exist, differences in terminology and research methodology have led to contradictory results. In response, a new cross-sectoral initiative called the Identity Management Standards Panel (IDSP) has been formed, the purpose of which is to reconcile disparities and create voluntary standards and guidelines, so that in the future we are better able to assess how well the marketplace is doing controlling identity crimes (American National Standards Institute, 2009). Progress in this regard is positive.

As we progress, a number of questions may be useful as we attempt to answer whether the marketplace is useful for fortifying information security and privacy and combating data breach and identity crimes. The data breach laws provide for notification exceptions, e.g., the notification thresholds and the fact that 50% of the laws do not pertain to covered entities that maintain data (both of which were discussed earlier). Therefore, the set of consumers who are notified is a subset of consumers whose data were breached. What is the size of this subset and what is the significance relative to utilizing a consumer market to drive change? The model assumes that once consumers are notified, they will be knowledgeable and this knowledge will lead to consumption choices based on quality. This assumes that consumers have complete information, can utilize this information effectively, and have well-ordered preferences. How complete is the information provided to consumers? What are the knowledge gain and the sufficiency of this knowledge gain? It is not clear that consumers have well-ordered preferences for data security over, for example, convenience and necessity. A citizen may receive notification from a retail store that his data were breached in a recent attack. However, the individual may value shopping at the store for its low prices and proximity more than it values changing retailers. Parents may receive notification that their child's school health records were breached. Clearly they cannot make a decision to "purchase schooling elsewhere". To what degree do citizens have well-ordered preferences? Can they, and do they, order their preferences thereby catalyzing market forces? Why or why not?

The data breach laws apply to a wide variety of covered entities, some of which are not in the private sector. How will the utilization of market forces to stimulate change impact entities such as local election boards, K-12 schools, non-profits and universities? What proportion of total data breaches occur in these types of covered entities? Can these types of entities find resources to invest in upgrading their information security? What repercussions are there if they do not upgrade their security?

Addressing collective action problems can be time consuming and costly. Given the dependencies, in order for collective choice problems to be meaningfully addressed, it is usually necessary to have a parallel effort to adapt constitutional institutions (Ostrom, Gardner, and Walker, 1994). We turn next to consider of interactions and outcomes at the constitutional level. Readers may wonder why this level not discussed first, given that it shapes the collective-choice and operational level interactions and outcomes. The reason is that this level is the most abstract. Often abstract ideas makes the most sense when viewed in relation to the more concrete as it is in the more concrete that the implications of the abstract become manifest and perceivable.

Constitutional

The United State is rooted in principles of democratic social order, distributed power, and active

citizen participation. The citizens influence the rules that structure their lives and in this way the United States can be considered self-governing. A self-governing entity is one whose members participate in the development of many of the constitutional or collective-choice rules as they are expected to accept the legitimacy and appropriateness of these rules (Ostrom, 1990). Self-governing entities are complex, adaptive systems comprised of a large number of elements that interact in multiple ways, adapt in response to interaction, and emerge in sometimes unpredictable ways.

So far we talked about changes such as improving data breach laws to achieve outcomes such as reduction of consumer desensitization, large scale collection information about of data breaches, timely collection of data about breach incidents, and security for large companies, while exempting small entities. That all of these outcomes are of practical importance and worthy of deliberation seems undisputable. But it is the view of this author that privacy, security, identity theft, and data breaches disclosure are inherently good only in relation to citizens' lives and livelihood. The Internet is a complex socio-technical system with multiple actors, countless interactions, and myriad effects, many of which will never be truly "knowable". It seems doubtful that we will be able to "govern" the Internet and information systems. Still, that we need some form of governance that aims toward collective interests and common good is obvious. So we may ask ourselves questions about self-governance. How should we engage citizens in the constitution and reconstitution of establishing collective-choice and operational rules in this arena? How can we engage the myriad of organizations (covered entities) that own, license, or maintain computerized data?

Social issues we seek to improve range from efficient and effective healthcare to financial reform, privacy, and national security. Information pervades them all. It is here that we clearly see the tensions as we attempt to reconcile multiple competing interests. Information is the raw material of knowledge. Knowing enables national security. Knowing enables economic growth. Knowing can improve healthcare. Knowing is foundational to social welfare and domestic law and order. In this regard, information is "sunlight". In a society founded on principles of distributed power and active citizen participation, government accountability is paramount. Public officials in such systems are accountable for how their decisions are made and in whose interests. In order to achieve accountability, the preferences of citizens have to be available to decision makers. Seen in this light, the data breach disclosure laws may not be about using market forces to force covered entities to enhance their security. Instead, these laws are a mechanism for us to make our preferences regarding the myriad uses of information as ends and means more apparent to decision-makers. The data breach laws are an opportunity to raise our collective conscience about data breach, data security, information security, identity theft, and privacy so that we may use our human insight, reason, and vigilance to transform our structures in a way that: preserves self-governance first and foremost; advances the state of information security and privacy in support of other social goods like improved healthcare, economic growth, and national security; and contributes to a better understanding of the changing and elusive role of privacy in our lives.

In 2006, Bonner (p. 21) noted, "a sharp divide has been inserted between the potential meanings of privacy and its actual meaning in practice. Its potential has been left behind". Is privacy something more than an aggregation of other types of rights, e.g. property rights and trespass? Do we need privacy for reasons other than job mobility, improved healthcare, and restricting government power? Is privacy inextricably linked to other desirable human conditions such as human dignity, intimacy, social relationships, and personhood? How much do we value these conditions? How do we value these relative to improved healthcare, national security, economic growth, etc? Perhaps we should evaluate the outcomes of the data breach disclosure laws in

regard to helping us more clearly see the costs and benefits of the freedom of information.

Recently the author was discussing privacy with a colleague where the statement was made that "privacy is dead". The logical malleability (Moor, 1985) of the computer enables a market of one – entities can and do offer personalized goods and services based on our individual preferences. As consumers, we seem to like this. For all intents and purposes, privacy, as we knew it, is dead. Privacy today is based on the principle of one. My privacy will be different from yours. There is no given level of privacy that each of us should expect; instead the amount of privacy each of us has is what we claim for ourselves in short bursts of time. Privacy is a series of microstates subject to rapid change, so that privacy is something that we have to continuously reclaim. Getting a populous to recognize this and continually practice it is a notable scaling up problem. Perhaps we should evaluate the outcomes of the data breach disclosure laws with regard to their impact on changing our collective conscience regarding this.

Finally, if principles of openness and transparency are vital for self-governance, should we even have an expectation of privacy, regardless of its merit for personhood? Is there an inherent contradiction? Ostrom notes that self-governance is always only a possibility and not a given (1990). Self-governance relies on a common understanding of the physical world we face and the trust and reciprocity of participants backed by their own willingness to monitor and enforce interpersonal commitments. Self-organization relies on smaller enclave to be productive in monitoring and enforcing. If, in the long run, the data breach disclosure laws amplify citizen participation in reconstitution of the macrostructure in a manner that support and encourages this self-organization, then they will have been highly effective.

In these more open, less-constrained situations, analysis is difficult. Interrelationships among institutions such as markets, legal systems, and social norms are highly complex and the effects are often unknowable. However, given the stakes, evaluation of the effect of the data breach disclosure laws on amplifying citizen participation and implications for self-governance seems to be the ultimate measure of the success of these policies.

CONCLUSIONS and FUTURE RESEARCH

Information assurance and security is inherently normative, dealing with complex social and ethical issues such as data breach, identity theft, privacy, access, and ownership. Information assurance and security questions such as "How secure is *secure enough*?", "What *ought* this system do in order to preserve privacy?" and "To whom *should* access be granted?" are more than technical questions – necessitating that IAS professionals consider how technological, sociological, ideological, and ecological systems interrelate. We are becoming more organically interdependent on technology. As technology becomes more intimately a part of us, deliberation of the social control of technology grows in importance. If citizens are to influence their own future, they must know enough about technology to fulfill their role as citizens; they must be in a position to speak from knowledge because speaking from ignorance is a position of subservience; subservient individuals can never expect to control their own destiny (DeVore, 1984). Participatory control of this participatory technology is necessary. Therefore, IAS professionals need to work meaningfully toward educating users on the limitations of information technology systems and the complexities of this powerful, potentially benevolent, yet imperfect technology.

While individuals comprise the collective, the sum total of individual decisions is not necessarily the equivalent of a social decision. Information assurance and security professionals need to be aware of "social goals", how they are formed, and how social systems and human purpose are arrived at through the collective involvement of all citizens. And, this understanding needs to be

brought to bear on the design, development, and control of technical systems. It was the intent of this chapter to analyze the policy landscape so that IAS students have a better understanding of the social context of information availability, information security, identity theft, data breach, and privacy. Enlightenment and knowledge regarding technology, society, and the relationship thereof to self-determination and self-governance is more important than ever before.

REFERENCES

American National Standards Institute (ANSI). (2009). *IDSP workshop report: Measuring identity theft.* Available at: http://webstore.ansi.org/identitytheft/

Bonner, B. (2006). The difficulty in establishing privacy rights in the face of public policy from nowhere. Saskatchewan Institute of Public Policy, *SIPP Public Policy Paper Number 43.* ISBN #: 0-7731-0566-2. Retrieved from http://www.uregina.ca/sipp/documents/pdf/PPP%2043%20-%20Bonner.pdf

Congressional Budget Office, (2006). *CBO S. 1789 Personal data privacy and security act of 2005 cost estimate.* Retrieved July 20, 2009 from http://www.cbo.gov/doc.cfm?index=7161

Congressional Research Service, (2007). Data brokers: Background and industry overview, *CRS Report for Congress RS22137-070112*. Retrieved June 15, 2009 from http://opencrs.com/

Congressional Research Service, (2008). Federal information security and data breach notification laws, *CRS Report for Congress RS33199.* Retrieved June 15, 2009 from http://opencrs.com/

DeVore, P. (1984). *Technology: An introduction.* Worcester, MA: Davis Publication.

Dryzek, J., Downes, D., Hunold, C., Schlosberg, D., & Hernes, H. (2003). *Green states and social movements.* Oxford University Press, NY.

Electronic Privacy Information Center (EPIC), (2008). *The Graham-Leach-Bliley act.* Retrieved May 30, 2009 from http://epic.org/privacy/glba/.

Fair Credit Reporting Act, at 15 U.S.C. § 1681 (1971).

Federal Trade Commission Act, 15 U.S.C. § 41-58 (1914).

GovTrack.us . Retrieved http://www.govtrack.us/congress/bill

Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320 (1996).

Hinde, S. (2003). Privacy legislation: a comparison of the US and European approaches. *Computers and Security, 22*(5), 378-387.

Identity Theft Resource Center, (2008). Retrieved May 25, 2009 from www.idtheftcenter.org

Javelin Research. (2008). *Identity fraud survey report: 2008.* Javelin Strategy & Research. Retrieved May 8, 2009 from http://www.idsafety.net/803.R_2008%20Identity%20Fraud%20Survey%20Report_Consumer%2

0Version.pdf

Javelin Research. (2007). *Identity fraud survey report: 2007*. Javelin Strategy & Research. Retrieved May 8, 2009 from http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf

Javelin Research. (2006). *Identity fraud survey report: 2006.* Javelin Strategy & Research. Retrieved May 8, 2009 from http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf

Lenard, T., & Rubin, P. (2005). An economic analysis of notification requirements for data security breaches. *Emory Law and Economics Research Paper No. 05-12*. Available at SSRN: http://ssrn.com/abstract=765845

Moor, J. (1985). What is computer ethics? *Metaphilosophy, 16*(4), 266-275.

Ostrom, E. (1999). Institutional rational choice. An assessment of the institutional analysis and development framework. In P. Sabatier (Ed.), *Theories of the policy process* (pp. 35-67). Boulder, CO: Westview Press.

Ostrom, E., Gardner, R., & Walker, J. (1994). *Rules, games, and common pool resources*. Ann Arbor, MI: The University of Michigan Press.

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action.* New York, NY: Cambridge University Press.

Personal Data Security and Privacy Act of 2009, S. 1490, 111th Congress (2009).

Picanso, K. (2006). Protecting information security under a uniform data breach notification law. *75 Fordham Law Review,* 355.

Ponemon Institute, (2008). *Consumers' report card on data breach notification.* Ponemon Institute Research Report. Retrieved May 15, 2009 from http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Consumer%20Report%20Card%20Data%20Breach%20Noti%20Apr08.pdf

Ponemon Institute (2008). *Fourth annual US cost of data breach study*. Ponemon Institute Research Report. Retrieved May 15, 2009 from http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf

Privacy Rights Clearinghouse (2008). *A chronology of data breaches*. Retrieved May 1, 2009 from http://www.privacyrights.org/ar/ChronDataBreaches.htm#1

Renshaw, K. (2002). Sounding alarms: Does informational regulation help or hinder environmentalism? *Environmental Law, 14*(3), 654-697.

Schoeman, F. (Ed). (1984). *Philosophical dimensions of privacy: An anthology,* Cambridge, MA: Cambridge University Press.

Schwarz, P., & Janger, E. (2007). Notification of data breaches. *Michigan Law Review, vol. 105,*

p. 913.

Sunstein, C. (1999). Informational regulation and information standing: Atkins and beyond. *University of Pennsylvania Law Review, 147*(3). 613-675.

U.S. Department of Justice, (2008). Available at: http://www.usdoj.gov/oip/04_7_1.html

Veterans Affairs Information Security Act, 38 U.S.C. § 5722 (2006).

Volokh, A. (2002). The pitfalls of the environmental right-to-know, *2002 Utah Law Review*, 805-841.

Westin, A. (1967). *Privacy and freedom*, New York, NY: Atheneum.

[i] The U.S. Virgin Islands, Puerto Rico and the District of Columbia have also enacted data breach disclosure laws.

[ii] It should be noted that in many reported breaches, the number of records breached is unknown. Thus the actual number is undisputedly higher.

[iii] Elinor Ostrom, an American Political Scientist, was awarded the Nobel Memorial Prize in Economic Science in 2009. She shares the award with Oliver Williamson.

[iv] This chapter provides a brief description of the Institutional Analysis and Development model (IAD). For a more complete discussion of the IAD model, readers can turn to Elinor Ostrom books, two of which are – Governing the Commons: The Evolution of Institutions for Collective Action (New York: Cambridge University Press, 1990) or Institutional Incentives and Sustainable Development: Infrastructure Policies in Perspective (Boulder: Westview Press, 1993).

[v] Covered entities are persons, agencies, and/or businesses that are required to provide notification and can include, for example, state and local agencies, public hospitals, departments of revenues and motor vehicles, courts at the state and local level, agencies that oversee elections, K-12 school districts, post-secondary institutions, and business entities engaging in inter and intrastate commerce not already covered by HIPAA and GLBA.