



How a Framework for Information Security Law Could Improve Information Security

Aaron J. Burstein

Research Fellow

Samuelson Law, Technology & Public Policy Clinic

Berkeley Center for Law & Technology

University of California, Berkeley

School of Law (Boalt Hall)

Berkeley, CA 94720

aburstein@law.berkeley.edu

January, 2008

Acknowledgments:

This work was supported under grant number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology. The I3P is managed by Dartmouth College.

The author also thanks Deirdre Mulligan for several helpful discussions.

Copyright© 2008.Trustees of Dartmouth College.

Executive Summary	3
1. Introduction.....	4
2. What Is Information Security Law?.....	5
2.1. Defining the Core of Information Security Law	6
2.2. Defining the Periphery of Information Security Law	7
3. How Core Information Security Laws Work.....	7
3.1. Individual Prohibitions.....	8
3.2. Private-Sector Organizational Regulations.....	11
3.3. Public Sector Organizational Regulations	19
3.4. Summary	23
4. The Role of Information Security Law’s Periphery	23
4.1. Consumer Protection.....	24
4.2. Promoting Research.....	24
4.3. Promoting Government as Coordinator	26
5. Conclusion	27

Executive Summary

This paper defines a legal framework for protecting and improving information security. The basis for the framework is the definition of information security from the computer science literature: the ability of a system to maintain the confidentiality, integrity, and availability of information when the system is under attack. This definition provides a clear, consistent definition for identifying whether a law should be considered an “information security law.” (This often is not self-evident.) Applying this definition to statutes and regulations in the United States shows that there is a *core* and a *periphery* of information security law, a distinction that is helpful to maintain when evaluating information security policy.

The framework includes two other analytical dimensions. The first is whether a regulation is directed toward individuals or organizations. The second is whether a regulation works via deterrence or some other mechanism. Taking these distinctions into account helps to explain more fully the role of deterrence in improving information security, and points to the promise of mechanisms other than deterrence in this area. Analyzing information security policy along these dimensions will help guide assessments of a policy’s likely impact.

The principal findings of this paper are:

- **Many U.S. information security laws are cast explicitly in terms of the properties of confidentiality, integrity, and availability.** Duties to maintain these properties in information under an entity’s control, however, are rarely absolute. Instead, many of the laws prescribe taking “reasonable” or “appropriate” (or both) measures to protect information. Even where sector-specific regulations add detail to the kinds of mechanisms an entity must adopt, the ultimate substantive standards are rarely more specific.
- **The divide between laws regulating individual and organizational conduct is fundamental to information security law.** Information security law creates direct prohibitions against certain kinds of individual conduct. This system is simple to grasp, but is limited by the scope of conduct that can be prohibited, the probability of getting caught, and the penalties for violations. On the other hand, the responses of corporations and public agencies to deterrents are more far more complex and should be considered to be a separate problem from individual prohibitions.
- **Information security regulations that apply to the public and private sectors are sharply different, and the potential for bringing them closer is limited.** Ongoing oversight of public agencies is routine, but it is extraordinary where private organizations are concerned. Developing policies and practices to improve information security practices therefore presents different challenges in these contexts.
- **Laws appropriating money for information security research can play an important role in coordinating academic, government, and industry efforts on specific problems.**
- **Public-private partnerships may ease the difficulties of imposing substantive governance regulations on private organizations, but they create a heightened need for public oversight.** The Homeland Security Act delegated significant authority to the Department of Homeland Security to protect the information infrastructure. Understandably, the resulting strategy relies heavily on cooperation between the government and the private sector. Given the scope of the protection mission, however, and the diversity of data that is potentially subject to sharing through public-private partnerships, oversight on this topic is warranted.

1. Introduction

Regulating information security is a tricky business. Threats evolve constantly. Ownership of information infrastructure is highly dispersed and stretches across many different sectors of the economy. The compromise of one system can affect many other systems. Attacks can be difficult to detect. Attacks may also be difficult to differentiate from innocuous activity. Security is notoriously difficult to measure, making general standards difficult to formulate. Long-term improvements in information security depend heavily on how individual and organizational users respond to incentives to secure their systems; the different values that these actors place on security make incentives difficult to gauge. Moreover, security-enhancing policies can carry other costs, such as reducing functionality or making information technology more expensive. Thus, “information security” stands for many different policy objectives. All of these characteristics pose significant challenges to making laws that promote information security.

Still, there is widespread agreement that the law has a role to play in information security. Despite some successes of information security law, a prevailing sense from the technical community seems to be that law and policy are not doing all that they could to improve information security. As a recent report issued by the National Resource Council puts it, “the cybersecurity policy failure is not so much one of awareness as of action.”¹ An earlier Council report urged legislators to consider enacting legislation that would change the incentives of users to adopt secure technologies.²

A common view in these and other reports from the technical community is that the law should *deter* acts that compromise security; and deterrence, in one form or another, does play a central role in the law of information security. Federal laws prohibit intercepting electronic communications, for example, or breaking into a computer system that is connected to the Internet. These laws contain broad prohibitions, limited by specific exceptions, and apply to individual and organizational actors, irrespective of their identities.

But criminal prohibitions are just one form of deterrence. A variety of sector-specific laws impose duties of confidentiality, integrity, and availability with respect to some kinds of information. Under these laws, the focus of deterrence shifts from the ultimate bad acts, such as using a stolen Social Security number to commit identity theft, to the organizations that control data that might be used for these purposes.

Information security law also may go beyond deterrence. The law can enable the government to coordinate information security protection, implementation, and research. It can also direct government agencies and (occasionally) private-sector organizations to take account of information security in specific ways.

This paper provides a framework to relate these different legal approaches to the underlying technical problems in information security. The benefit of having a framework is that it allows one to identify gaps in the law and determine what effects filling those gaps would have on the existing legal structure. Part of this framework is descriptive; it defines “information security law” and provides a taxonomy of this body of law in the United States. The other part suggests directions for the law that might improve information security and fit into the overall structure of

¹ TOWARD A SAFER AND MORE SECURE CYBERSPACE 1-2 (Seymour E. Goodman and Herbert S. Lin, eds.) (draft released June 26, 2007).

² CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 15 (2002).

this area of law. This consideration is important, as it provides a basic check on expectations as to what kinds of action policymakers might be willing to take.

The overall argument developed in this paper is that regulating organizations' decisions about information security is central to the deterrence-based model of improving information security, but that such regulations are limited in how finely they can tune decisions within organizations. As a result, regulating information security by means other than deterrence should play an increased role in information security law.

The remainder of this paper proceeds in four parts. Part 2 sets forth a definition of information security law based on the definition of security from the computer science literature. This definition of the law in terms of the abstract properties of confidentiality, integrity, and availability suggests dividing information security law into a "core" and a "periphery."

Part 3 applies this definition to the core information security laws of the United States, both selecting information security laws and describing their contents.³ The laws described in this Part display a policy-level awareness of the information security's technical properties, but they also point to the difficulty of creating legislation that operates with these abstract definitions. This Part therefore expands the framework for information security law to account for how the law adds concreteness: by distinguishing between individuals, private sector organizations, and public sector agencies.

Part 4 explores the role of "peripheral" information security laws. All of these laws provide ways to escape some of the constraints of core information security law, either by taking advantage of very general regulatory authority or by getting around some of the constraints on regulating organizations discussed in Part 2.

Part 5 concludes with some suggestions for potentially fruitful directions in information security law.

2. What Is Information Security Law?

A legal framework should accomplish several things. First, it should provide a coherent description of the relationships among the topics included within the framework.⁴ Second, it should guide the development and enforcement of rights and obligations in order to achieve specific goals.⁵ This part starts that that framework by using the definition of information security found in the computer science literature to identify the goals of information security law. These ends then suggest a division in information security law—a *core* that creates express rights or obligations with respect to information security, and a *periphery* that less directly affects such rights and obligations.

³ A summary of all information security laws discussed in this paper is in the Appendix, beginning at page 28.

⁴ See, e.g., Jacqueline Lipton, *A Framework for Information Law and Policy*, 82 OR. L. REV. 695 (2003).

⁵ See Lawrence O. Gostin, *Meeting Basic Survival Needs of the World's Least Healthy People: Toward a Framework Convention on Global Health 2*, 96 GEO. L.J. (forthcoming Jan. 2008), available at <http://ssrn.com/abstract=1014082>.

2.1. Defining the Core of Information Security Law

To be descriptively useful, the definition of information security should avoid defining the area so narrowly that it leaves out related laws; and, conversely, it should not define the area so broadly that it encompasses everything. In addition, the definition should provide some hooks for linking the law to technical definitions of information security.⁶

Thus, the definition of “information security” found in the computer science literature provides a logical place to begin defining information security law. Though there is no single, authoritative definition of information security, several leading academic studies define information security to include the properties of *confidentiality*, *integrity*, and *availability*.⁷ These studies, in turn, define these properties as follows:

- *Confidentiality* means “keep[ing] protected information away from those who should not have access to it.”⁸
- *Integrity* means “produc[ing] the same results or information whether or not the system has been attacked.”⁹

⁶ A related semantic issue also requires some explanation. This paper deliberately refers to *information security*, rather than plausible alternatives such as “cybersecurity” or “computer and network security.” See Matt Bishop, *What Is Computer Security?*, 1 IEEE SECURITY & PRIVACY 67, 67 (2003) (equating “cybersecurity” with “computer and network security”). Including computer and network security within a single term makes sense, given the interdependence of security in the computer systems that hold data and the networks that connect them. See *id.* Taking account of laws that relate to the security of computers and networks is something that this paper seeks to achieve. At least some definitions of cybersecurity, however, limit the term to the security of *electronic* systems. For example, the U.S. Department of Homeland Security’s *National Infrastructure Protection Plan* (p. 103, for example, defines cybersecurity to mean:

The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

Requiring that a law refer exclusively to electronic information and computer systems would create severe limitations on the scope of this paper; many laws that relate to cybersecurity are concerned with rights and duties that apply to any information system, electronic or not. In addition, a significant subset of laws is concerned with *organizations* that control information, rather than with the information systems themselves. To avoid these limitations and potential sources of confusion, this paper uses the term “information security.”

⁷ See, e.g., NATIONAL RESEARCH COUNCIL, TOWARD A SAFER AND MORE SECURE CYBERSPACE 2-2 (Seymour E. Goodman and Herbert S. Lin, eds.) (draft released June 26, 2007); NATIONAL RESEARCH COUNCIL, CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 3 (2002); NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE 14 (ed. Fred B. Schneider) (1999).

⁸ NATIONAL RESEARCH COUNCIL, TOWARD A SAFER AND MORE SECURE CYBERSPACE, *supra* note , at 2-3.

⁹ *Id.*

- Finally, *availability* means that an information system is “usable or operational during a given time period, despite attacks or failures.”¹⁰

Moreover, a secure system maintains these properties in the face of attack; accidental compromises to a system’s confidentiality, integrity, or availability are beyond the scope of security.¹¹ Again, variations in these definitions exist within the computer science literature. It is beyond the scope of this paper (and perhaps any paper) to reconcile competing definitions.¹² The hope, however, is that explicit definitions will serve the purpose of clarity in the rest of this paper.

Using this definition of information security, this paper will define two senses of information security law. In the first sense, an information security law is a statute or regulation that creates an *obligation* to protect the confidentiality, integrity, or availability of information against a deliberate attack. In the second sense, an information security law is a statute or regulation that creates a *right* (or a person or an organization) to have certain information remain free from deliberate attacks against its confidentiality, integrity, or availability.

2.2. Defining the Periphery of Information Security Law

Restricting the analysis in this paper to statutes and regulations that fit the definition of core information security law would leave some important areas unexplored. Part 4 discusses three areas of law that have had, or are poised to have, a significant influence on information security through litigation, administrative rulemaking, or other means authorized by law. Recognizing that laws that do not meet the core definition is important to lending flexibility to the framework.

3. How Core Information Security Laws Work

A framework that consists entirely of the descriptions given in Part 2 is unsatisfactory because it articulates general goals but says little about how to achieve them. Indeed, recent studies by academics and government agencies have begun to specify more concrete—but still general—approaches to characterizing secure technologies. For example, the National Research Council’s 2007 report, *Trust in Cyberspace*, suggests four general approaches to improving information security: (1) secure design, development, and testing; (2) enabling accountability; (3) promoting deployment; and (4) deterring and punishing attackers. Similarly, a report from an NSF workshop on the next-generation secure Internet discussed viewing a security “design space” with the dimensions of prevention, detection and recovery, resilience and deterrence.¹³ And the *Federal Plan for Cyber Security and Information Assurance Research and Development* provides a

¹⁰ NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE, *supra* note , Appendix K (1999).

¹¹ Such accidents, however, are taken into account in the broader concept of trustworthiness. See NATIONAL RESEARCH COUNCIL, TOWARD A SAFER AND MORE SECURE CYBERSPACE at viii (explaining that “cybersecurity is only one element of trustworthiness, which can be defined as the property of a system whereby it does what is required and expected of it—despite environmental disruption, human user and operator errors, and attacks by hostile parties—â”and that it does not do other things”).

¹² For a concise guide to some of the variations, see ROSS ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 8-11 (2006).

¹³ Steven M. Bellovin et al., *A Clean-Slate Design for the Next-Generation Secure Internet* 5 (2005).

detailed taxonomy of areas for security research and development that includes many of these areas.¹⁴

On the policy side, the *National Infrastructure Protection Plan* sets forth a risk management framework for cybersecurity comprising six elements: setting security goals, identifying assets, assessing risks, prioritizing plans based on risk, implementing protective programs, and measuring effectiveness.¹⁵ Among the elements of the NIPP's protection implementation are deterrence, detection, mitigation, recovery, and preventative defense.¹⁶ Given the growing recognition of these approaches to secure technology, this Part makes an effort to point out whether a given law provides incentives to adopt any of these approaches.

A common theme in all of these documents is that the role for law and policy is most pronounced in the realm of deterrence. This observation is well-founded, as one of the principal justifications for legal sanctions, in the form of fines or imprisonment, is that they sufficiently raise the cost of undesirable conduct to make individuals forgo the expected benefit of engaging in the conduct.¹⁷ This Part finds that core information security laws do indeed work through the mechanism of deterrence, though there is significant variation in the strength of the laws' deterrents.¹⁸

3.1. Individual Prohibitions

The most severe legal means of regulating behavior is through a prohibition. Several core information security laws prohibit certain types of individual conduct. Before discussing specific statutes, however, a bit of background about prohibitions is warranted. One way to deter an activity is to make engaging in it a crime. Since running afoul of a criminal law can result in the loss of individual liberty, the law be clear as to what conduct is permitted and what is prohibited.¹⁹ The price for this clarity can be a lack of flexibility. If a criminal law is precise, but narrow, it might be easy to devise ways to skirt the law. The legislature that enacted the law, of course, can update it; but the amendment process can be slow or give way to other legislative priorities. Conversely, over time the definition of a crime can become so broad that it threatens socially beneficial conduct.²⁰

¹⁴ This report was written by the National Science and Technology Council and is available at http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf.

¹⁵ NIPP at 29-50. The framework also encompasses physical and human elements of security.

¹⁶ NIPP at 45.

¹⁷ See Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968).

¹⁸ A summary of all information security laws discussed in this paper is in the Appendix, beginning at page 28.

¹⁹ Criminal laws that do not provide adequate notice about which conduct is prohibited may be invalidated as “void for vagueness”—a conclusion that rests on the constitutional right to due process.

²⁰ The expansion of criminal laws through legislative amendment is by no means unheard of. The federal Computer Fraud and Abuse Act (CFAA), discussed above as a core information security prohibition, provides one example. The breadth versus narrowness debate also is playing out in the context of the CFAA. Certain offenses set a minimum threshold of \$5,000 in damage to a protected system. Some commentators have argued that this threshold is too low and criminalized conduct not worth prosecuting, while Congress has considered legislation that would eliminate

3.1.1. Computer Fraud and Abuse Act

The most sweeping set of prohibitions against individual conduct that harms information security comes from the Computer Fraud and Abuse Act (CFAA)²¹ Though the CFAA has been characterized by legal scholars as a “cybercrime” statute rather than an information security law,²² it squarely fits the definition developed in this paper.

The CFAA provides a set of confidentiality, integrity, and availability guarantees for essentially every computer in the United States connected to the Internet. The statute provides civil and criminal penalties that are intended to deter certain kinds of attacks against information systems.²³

The CFAA defines those attacks broadly. Targeted computer system break-ins, denial of service attacks, and spreading viruses and worms all generally fall within the Act’s prohibitions. The basic structure of the CFAA works is to prohibit individuals from accessing “protected computers”—which now means any computer connected to the Internet—in excess of their authorization to do so.²⁴ The CFAA defines offenses differently depending on the type of information system in question. For example, it is an offense merely to obtain without authorization a financial record from a financial institution’s computer²⁵ or to access without authorization a “nonpublic” U.S. government computer,²⁶ but an attacker must cause damage to other types of computers in order to have committed an offense.²⁷ Still, the generality of the CFAA is remarkable. Aside from exempting law enforcement and intelligence officials acting with legal authorization from its prohibitions,²⁸ the CFAA applies without exception.

the CFAA’s damage threshold. For the former view, see Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909 (2003). For the latter, see the Cyber-Security Enhancement and Consumer Data Protection Act of 2007 (H.R. 836, Feb. 6, 2007), which effectively eliminate the monetary damage threshold from the CFAA.

²¹ The CFAA was initially enacted in 1984 as Public Law 98-473 and codified at 18 U.S.C. § 1030, though the name CFAA comes from an amendment passed in 1986. *See* Pub. L. No. 99-474, 100 Stat. 1213 (1986). Many states have similar laws, but, given the similarities, only the federal statute is discussed here.

²² *See* Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1602-05 (2003) (explaining that “[c]rimes of computer misuse represent a new type of crime” in which computer systems themselves are the targets of a crime).

²³ *See* S. Rep. 99-432 (1986) (stating that the CFAA is “aimed at deterring and punishing certain ‘high-tech’ crimes”).

²⁴ *See* 18 U.S.C. §§ 1030(a)(1)-(a)(5). The use of “exceeding authorized access” and similar phrases to set a threshold for the acts that the CFAA prohibits has been the subject of intense criticism from legal scholars and courts on the grounds that the terms of use on a website, for example, could be taken to establish the boundaries of a user’s authorization. *See* Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

²⁵ 18 U.S.C. § 1030(a)(2)(A).

²⁶ 18 U.S.C. § 1030(a)(3).

²⁷ *See* 18 U.S.C. §§ 1030(a)(4)-(5).

²⁸ 18 U.S.C. § 1030(f).

3.1.2. Wiretap Act

A similarly broad prohibition is found in the Wiretap Act's ban on the interception of electronic communications; the Act creates a right to confidentiality in communications. Originally enacted in 1968 to prohibit interceptions of voice conversations (whether face-to-face or transmitted by telephone), Congress has since expanded the Wiretap Act to include electronic communications. (For simplicity, the discussion here will focus on electronic communications.)

Deterrence again works in a direct manner: Violations of the Wiretap Act are subject to criminal and civil punishment. In its present form, the Act prohibits any person from intentionally intercepting an electronic communication, or from disclosing or using any communication that was obtained through a prohibited interception.²⁹ This prohibition is quite general for actors other than law enforcement officials, the broadest exceptions being that one party to a communication may consent to an interception, 18 U.S.C. §§ 2511(c)-(d) and the provider of an electronic communications service (e.g., an Internet service provider) can intercept communications to protect its "rights or property."³⁰ Law enforcement officials must obtain from a court a warrant to intercept communications,³¹ unless they obtain the consent of one of the parties to the communication.

3.1.3. Discussion

Aside from providing legal redress for violations of the security of a computer system or communications, do these information security laws provide incentives to adopt more secure technologies? None of these prohibitions are contingent on the use by the party seeking protection of any particular type of technical security mechanisms. The CFAA does not depend, for example, on the use of any particular technical mechanism to control access to a computer. Indeed, it provides legal protection to owners of systems that contain software with known vulnerabilities. One civil case even went as far as to hold that a confidentiality agreement between a person and his former employer was sufficient to set the boundaries of "authorized access" to a computer.³²

Similarly, the protections of the Wiretap Act apply irrespective of the security properties of the systems used to transmit and store communications. For example, unencrypted communications generally receive the same level of protection under the Wiretap Act as encrypted messages.³³ Part of the explanation for rather weak role of the Wiretap Act and the

²⁹ 18 U.S.C. § 2511(1).

³⁰ 18 U.S.C. § 2511(2)(a)(i).

³¹ 18 U.S.C. § 2516. An application for a warrant authorizing a wiretap is subject to strict restrictions. The proposed warrant must involve an investigation of one of an enumerated list of crimes, 18 U.S.C. § 2516, authorization for the interception may be subject to court supervision and can last no longer than 30 days without re-authorization, and the interception must minimize the collection of communications not subject to the warrant, 18 U.S.C. § 2518.

³² See *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001).

³³ A slight qualification to this statement is due to 18 U.S.C. § 2511(4), which states that the interception of *unencrypted* satellite signals carrying radio or television content for rebroadcast on public channels is not an offense under the Wiretap Act.

A separate qualification is that there is a continuing debate over whether the use of encryption can trigger protection under the Fourth Amendment of the U.S. Constitution. See Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the*

SCA in promoting information security is that they are not pure information security statutes. They are, primarily, privacy statutes: they structure an information flow relationship among private parties and between citizens and the government. Viewed in this light, the lack of legislative attention to the role of security mechanisms in protecting privacy is understandable.

An alternative approach in both statutes would be to require anyone seeking to enforce his or rights to adopt certain security measures. A full evaluation of this approach is beyond the scope of this paper, but there are reasons to be cautious about it. In the case of the Wiretap Act, the individuals whose communications privacy rights are protected do not always have the ability to choose more secure technology. Though this problem may be less severe with electronic communications, for which encryption is widely available, than with voice communications, granting different levels of protection to these two types of communications has been a source of major confusion in the past.

As to whether the CFAA should set requirements for system security as a prerequisite to enforcement, there are arguments on both sides. On the one hand, computer owners who are sufficiently motivated to pursue civil or criminal cases under the CFAA might also be motivated to adopt secure technologies. The same logic applies to gathering the types of evidence that might be useful in criminal prosecutions; the availability of criminal law enforcement might encourage computer system owners to adopt mechanisms that promote auditing and accountability. On the other hand, many of the attacks that have been prosecuted under the CFAA exploited vulnerabilities in mass-market software—email clients, for example—about which most users were probably ignorant. Such information asymmetries between attackers and users show no sign of abating; until some combination of technological change, education, and usability improves general security awareness among users, setting a “security minimum” to invoke the CFAA might be unfair to many.

Still, without strong incentives to adopt secure technologies, the CFAA in particular places the focus rather late in the security game, namely after a successful attack. Laws that are better suited to directing attention to steps earlier in the information security development process require shifting the focus from individual bad actors to the organizations that produce, own, and operate the information infrastructure. As the remainder of this Part shows, this shift in focus requires laws with dramatically different structures than the prohibitions discussed here.

3.2. Private-Sector Organizational Regulations

The problem of getting organizations to do what policymakers want them to do - producing a product with certain characteristics, for example - has spawned a vast literature in law, economics, and sociology. Organizations might involve thousands of actors, making priority-setting and decision-making highly complex tasks whose outcomes are difficult to predict ex ante, and sometimes difficult to explain ex post. Even under a model that views an organization as a unified, rational actor that is assumed to act to maximize its own profit (or other measure of utility), some organizations are controlled by “bad apples” that decide violating the law is in the organization’s best interests.³⁴ Moreover, at the federal level in the United States, the general

Electronic Communications Privacy Act, 72 GEO. WASH. L. REV. 1557, 1596-97 and references cited in note 289 (2004).

³⁴ See Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 393-96 (2006) (describing “compliance models” of private firm behavior based on a view of firms as “amoral calculators”).

approach to regulating private firms has been to allow them wide berth to organize themselves internally.³⁵

It is against this background that one must consider the problem of changing organizational approaches to information security. The opportunities for directing investment, setting priorities, or requiring the adoption of specific technologies—whether relating to security or not—are extremely limited. Some firms that play an important role in information security, such as telecommunications companies, financial institutions, and healthcare providers, are subject to extensive, sector-specific regulations; whereas others, such as the software industry, are subject to virtually none. These firms place widely differing values on the information they control and differ tremendously in their incentives to protect their information systems. A “one-size-fits-all” approach to directing firms’ focus to information security in the contexts emphasized in this section—secure design, risk assessments, etc.—would have a hard time taking account of this highly varied terrain.

Accordingly, it is not surprising that there is no generally applicable set of information security regulations for private organizations in the United States. Instead, the primary means of regulating firms’ information security practices is through sector-specific statutes and regulations that prohibit disclosures of certain kinds of information. These laws operate under a general model of deterrence, but the deterrent applies to the organizations that control the information, rather than to the attackers that seek the data.

A further general observation about these laws is that they do not set highly specific requirements for the performance of security mechanisms or mandate specific technologies. Instead, many of the laws boil down to a standard of taking “reasonable and appropriate” precautions against known or anticipated threats. Sector-specificity helps to define such standards through regulatory oversight and industry practice.

3.2.1. Fair Credit Reporting Act

The earliest of these laws is the Fair Credit Reporting Act (FCRA),³⁶ which provides a set of confidentiality, integrity, and availability obligations with respect to information collected about individual consumers. The confidentiality protections in the FCRA consist mostly of regulations on the permissible purposes and recipients of information. The FCRA applies to “consumer reporting agencies” (CRAs) and limits the purposes for which a CRA may disclose a “consumer report.”³⁷ The FCRA also requires users of reports to identify themselves to a CRA before

³⁵ See Roberta Romano, *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance*, 114 YALE L.J. 1521, 1523 (2005) (noting that “[t]he federal regime [of corporate governance prior to the enactment of the Sarbanes-Oxley Act] had . . . consisted primarily of disclosure requirements rather than substantive corporate governance mandates, which were traditionally left to state corporate law”).

³⁶ Pub. L. No. 91-508 (Oct. 26, 1970) (codified at 15 U.S.C. § 1681 *et seq.*).

³⁷ 15 U.S.C. § 1681b. A CRA is defined under the Act as a person entity that “regularly engages . . . in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.” 15 U.S.C. § 1681a(f). A consumer report, in turn, is information about an individual’s credit worthiness, reputation, or “mode of living” that is used to grant or deny credit, insurance, or employment. 15 U.S.C. § 1681a(d). Violations of the FCRA are subject to civil and criminal penalties. 15 U.S.C. §§ 1681n-1681r.

obtaining reports and certify to the CRA that they will use a report only for permissible purposes.³⁸ CRAs and users are required to “properly dispose” of consumer information “by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.”³⁹ In addition, the FCRA requires CRAs to allow individuals to alert a CRA about potential identity theft and to correct information in their records—establishing, in effect, an availability requirement and integrity checks on the information in consumer records. A CRA must maintain “reasonable procedures” to prevent prohibited disclosures or uses and to assure the accuracy of reports.⁴⁰

3.2.2. Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)⁴¹ requires any educational agency or institution receiving federal funding to disclose education records only for certain purposes (such as audits, subpoenas, and school accreditation) or with the student’s (or guardian’s) consent.⁴² Thus, FERPA protects confidentiality. It does not impose any information security requirements on a covered entity;⁴³ the enforcement mechanism is the Secretary of Education’s authority to deny federal funds to any institution that has a “policy or practice” of disclosing student records or personally identifiable information in a manner not allowed by the Act.⁴⁴

3.2.3. Stored Communications Act

In 1986, as networked information systems were becoming more common, Congress enacted confidentiality protections for stored communications, i.e., communications that are not “in transit.” For example, an email stored on an ISP’s server after the recipient reads it is a stored communication. The law that regulates the disclosure of these communications is the Stored Communications Act (SCA). However, rather than applying to all actors, as is the case with the Wiretap Act, the SCA’s prohibitions apply only to providers of an electronic communications service—an ISP, for example—or a remote computing service, such as an email service.⁴⁵ As is the case with the Wiretap Act, law enforcement officials can obtain a court order—much more freely given than under the Wiretap Act—to compel the disclosure of protected communications.⁴⁶

The incentives present in the SCA to adopt secure technologies are subtle. The disclosure prohibitions under the SCA do not require service providers to protect their systems with even a

³⁸ 15 U.S.C. § 1681e(a).

³⁹ This “disposal rule” was recently issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions Act (FACT Act) of 2003. *See* 16 C.F.R. § 682.

⁴⁰ 15 U.S.C. § 1681e.

⁴¹ Pub. L. No. 93-380 (codified at 20 U.S.C. § 1232g); 34 C.F.R. § 99.

⁴² 20 U.S.C. § 1232g(b).

⁴³ But officials who receive records must protect them from disclosure “in a manner which will not permit the personal identification of students and their parents by other than those officials.” 20 U.S.C. § 1232g(b)(3)(C).

⁴⁴ Several courts have held that the Secretary of Education has the sole authority to enforce FERPA; there is no private right of action. *See, e.g.,* Frazier v. Fairhaven Sch. Comm., 276 F.3d 52, 67-69 (1st Cir. 2002); Girardier v. Webster College, 563 F.2d 1267, 1276-77 (8th Cir. 1977);

⁴⁵ 18 U.S.C. § 2702.

⁴⁶ 18 U.S.C. § 2703.

modicum of security. In fact, the mental state required for committing an offense under the SCA—a person or entity must *knowingly* divulge the contents of a protected communication—likely would not cover a service provider whose lax security measures allow attackers to penetrate the provider’s system, thereby exposing protected communications. (Such acts would, however, probably be offenses under the CFAA.) The SCA does not create liability for providers whose systems are compromised by malicious attack,⁴⁷ making the SCA somewhat anomalous in the group of laws considered in this section. The expectation among users that email service and other electronic communications providers will keep their communications confidential, however, is deeply seated and likely encourages providers to adopt secure technologies.

3.2.4. Gramm-Leach-Bliley Act

More recent federal information security legislation has continued the pattern of creating sector-specific duties to maintain the confidentiality (and, sometimes, the integrity and availability) of information. The security requirements have become more detailed, though the ultimate standard of “appropriateness” remains. The first example is the Gramm-Leach-Bliley Act (GLBA) of 1999.⁴⁸ The GLBA emphasizes the confidentiality property of information security. The basic obligation of financial institutions under the Act is to “protect the security and confidentiality of [their] customers’ nonpublic personal information.”⁴⁹ To add some specificity to this charge, the GLBA authorized federal financial oversight agencies and the Federal Trade Commission, to develop “appropriate standards” for financial institutions to follow to protect insure customer record “security and confidentiality” against “anticipated threats” and “unauthorized access” that “could result in substantial harm or inconvenience to any customer.”⁵⁰

In 2005 these agencies issued a regulation (the “Interagency Guidance”) that consists of two main elements: requirements for institutional breach response programs and requirements for customer notice following unauthorized access or use of customer information. The customer notice requirements of the Interagency Guidance squarely fit the deterrence model of promoting information security, with an emphasis on confidentiality:⁵¹ a firm that wishes to avoid damaging its reputation by disclosing a breach will take steps to avoid a breach in the first place.⁵² This regulation not only requires financial institutions to notify customers directly when a breach “could result in substantial harm or inconvenience to any customer,”⁵³ but also to notify the relevant regulator “when the institution becomes aware of an incident involving unauthorized

⁴⁷ Indeed, the SCA defines an offense quite similar in effect to the CFAA for individuals who obtain unauthorized access to a service provider’s facilities. 18 U.S.C. § 2701.

⁴⁸ Pub. L. No. 106-102 (Title V), 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801-6809 and 6821-6827).

⁴⁹ 15 U.S.C. § 6801(a).

⁵⁰ 15 U.S.C. § 6801(b) (setting forth the requirement to develop standards); 15 U.S.C. § 6805 (listing the agencies responsible for setting standards).

⁵¹ See 70 Fed. Reg. 15,736, 15,752 (“Financial institutions have an affirmative duty to protect their customers’ information against unauthorized access or use.”).

⁵² See 70 Fed. Reg. 15,736, 15,752 (“[A]n institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so.”).

⁵³ *Id.* at 15,752.

access to or use of ‘sensitive customer information’” a lower threshold than the customer notice provision.⁵⁴

The response program requirements set forth in the Interagency Guidance take a rather different approach. In contrast to the customer notice requirements’ ultimate reliance on reputational harm, the response program standards focus on the internal planning and decision-making processes within financial institutions. Moreover, they recognize that, while prevention is desirable, no prevention scheme is foolproof. Accordingly, the Guidance states that a “response program should be a key part of an institution’s information security program.”⁵⁵ Specifically, the Guidance requires (1) “notifying appropriate law enforcement authorities” and (2) “[t]aking appropriate steps to contain and control [an] incident” once it is detected.⁵⁶

Thus, a number of the response program provisions take a step back from deterrence to include approaches to security that are becoming prominent in the technical literature. For instance, the response program requires a plan to contain an intrusion, and the law enforcement reporting provision adds to the flow of information that could allow regulators and law enforcement officials to obtain a better picture of threats to the financial system. Still, the Interagency Guidance itself contains no specifics about how to accomplish these goals, though it points to existing security guidelines prepared by federal agencies. Moreover, response program provisions leverage the already extensive federal regulation of financial institutions. It is doubtful that this approach could be extended to sectors that are either lightly regulated or which have countervailing individual privacy protections for individuals.

3.2.5. Security Breach Notification Laws

A similar, but broader, approach is taken in security breach notification laws. California enacted the first such law in the United States in 2003; since then, at least 35 states have enacted similar laws.⁵⁷ Since California has served as a model in this area, and because there is currently no federal equivalent, this discussion focuses on California’s breach notification law. The California notification law requires any company that does business in California to disclose any security breach that the company reasonably resulted in the disclosure of unencrypted “personal information” to an unauthorized person.⁵⁸

The statute defines a security breach in terms of the technical properties of information security: the “unauthorized acquisition of computerized data that compromises the security,

⁵⁴ *Id.* at 15,741. As two legal scholars point out in a recent article, this “two-track system” leaves open the possibility that financial institutions, which are responsible for determining whether a breach has occurred and how severe it is, will report to regulators but not to customers because of the greater reputational risk involved in the latter. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 916 (2007).

⁵⁵ Interagency Guidance at 15,752.

⁵⁶ 70 Fed. Reg. 15,736, 15,752 (Mar. 28, 2005). Still, the guidance “does not detail the steps that an institution should take to contain and control a security incident to prevent further unauthorized access to or use of customer information.” *Id.*

⁵⁷ Samuelson Law, Technology & Public Policy Clinic, *Security Breach Notification Laws: Views from Chief Security Officers* 9 (Dec. 2007), available at http://www.law.berkeley.edu/clinics/samuelson/cso_study.pdf.

⁵⁸ Cal. Civ. Code § 1798.82(a).

confidentiality, or integrity of personal information.”⁵⁹ Thus, it is a core information security law. Like the GLBA, security breach notification laws work through deterrence: the threat of harming a company’s reputation due to disclosing a breach should encourage companies to adopt mechanisms to prevent breaches in the first place. But the differences between breach notification laws and the GLBA are significant.⁶⁰

The differences between breach notification laws and the GLBA highlight the importance of considering policy mechanisms that impose requirements within the boundaries of a firm. In California, at least, the duty to disclose a breach is not confined to a particular economic sector, nor does it set a minimum threshold of risk of harm to trigger the duty to disclose.⁶¹ The California law also does not create any duty to mitigate after a breach, nor does it follow the GLBA’s model of imposing substantive planning requirements within a firm.

3.2.6. Health Insurance Portability and Accountability Act Security Rule

The health care sector provides another example of regulating information security by defining the conditions under which information may be disclosed or accessed. The Health Insurance Portability and Accountability Act of 2002 (HIPAA)⁶² was intended to guard individuals’ privacy interests in “protected health information” (PHI). The Act applies only to PHI, and only to the extent that such information is handled by a “covered entity,” namely a health plan, health care clearinghouse, or a health care provider that conducts certain electronic transactions.⁶³ HIPAA was, in part, a response to the threats that interconnected electronic health record systems pose to individual privacy,⁶⁴ and the “Privacy Rule” that was issued by the U.S. Department of Health and Human Services (HHS) continues to direct a great deal of attention to privacy.⁶⁵

⁵⁹ *Id.* § 1798.82(d).

⁶⁰ For a detailed analysis of the differences among California’s breach notification law, the GLBA, and other disclosure laws, see Schwartz & Janger, *Notification of Data Security Breaches*, *supra* note 3.2.4.

⁶¹ For an analysis of the costs and benefits of a minimum-risk safe harbor, see Deirdre K. Mulligan & Chris Jay Hoofnagle, Testimony Before the Senate Judiciary Committee Subcommittee on Terrorism, Technology and Homeland Security (Mar. 21, 2007), at <http://judiciary.senate.gov/pdf/3-21-07HoofnagleTestimony.pdf>.

⁶² Pub. L. No. 104-191.

⁶³ 42 U.S.C. § 1172; 160 C.F.R. § 102.

⁶⁴ See Lawrence O. Gostin, James G. Hodge, Jr. & Mira S. Burghardt, *Balancing Communal Goods and Personal Privacy Under a National Health Informational Privacy Rule*, 46 ST. LOUIS L.J. 5, 8-9 (2002).

⁶⁵ HIPAA directed HHS to issue final regulations on the privacy of individually identifiable health information, in the event Congress failed to enact privacy legislation before within three years of HIPAA’s enactment. 42 U.S.C. § 1320d-2, HIPAA § 264. Congress failed to do so. The resulting regulation is widely known as the HIPAA Privacy Rule. See, e.g., Roberta B. Ness et al., *Influence of the HIPAA Privacy Rule on Health Research*, 298 JAMA 2164 (2007). The HIPAA Privacy Rule, 45 C.F.R. §§ 160 & 164, 65 Fed. Reg. 82,462 (Dec. 28, 2000), was implemented in April 2003.

But HIPAA also directed HHS to issue a Security Rule,⁶⁶ which went into effect in April 2005. With respect to security, the language of HIPAA itself tracks the language of the technical definition of information security. The Act requires covered entities to:

[M]aintain reasonable and appropriate administrative, technical, and physical safeguards—

- (A) to ensure the integrity and confidentiality of the information;
- (B) to protect against any reasonably anticipated—
 - (i) threats or hazards to the security or integrity of the information; and
 - (ii) unauthorized uses or disclosures of the information; and
- (C) otherwise to ensure compliance with this part by the officers and employees of such person.⁶⁷

The Security Rule implements these general goals in three categories of safeguards—administrative, physical, and technical.⁶⁸ The overall structure of the Security Rule also moves away from deterrence to a model of substantive regulation of covered entities. Each covered entity must conduct a risk analysis, develop a risk management plan and sanction policies, and audit activities in its information systems.⁶⁹ The Security Rule emphasizes that covered entities must protect against both internal and external security threats.⁷⁰ Covered entities must conduct security training for their employees. They must have security incident response (including mitigation) and disaster recovery plans.⁷¹ Finally, covered entities must obtain contractual guarantees from its business partners that the partner will abide by all of HIPAA’s requirements.⁷²

In addition, the technical safeguards move in the direction of requiring specific approaches that appear to be gaining favor within the technical security community. Specifically, the technical safeguards comprise five categories: access control, audit controls, integrity, person or entity authentication, and transmission security.⁷³ For each of these five categories, the Security Rule states a general standard, followed by one or more “implementation specifications.” For example, the integrity standard directs covered entities to “[i]mplement policies and procedures

⁶⁶ 68 Fed. Reg. 8334 (Feb. 20, 2003). The HIPAA Security Rule was issued separately from the Privacy Rule and has received much less attention. For an analysis that focuses on the Security Rule, see Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331 (2007).

Still, it is worth noting that the Privacy Rule states a security standard (45 C.F.R. § 164.530(c)(2)):

A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

⁶⁷ 42 U.S.C. § 1320d-2(d)(2).

⁶⁸ 68 Fed. Reg. 8345.

⁶⁹ 45 C.F.R. § 164.308(a).

⁷⁰ 68 Fed. Reg. 8338.

⁷¹ 45 C.F.R. § 164.308(a)(7), (8).

⁷² 45 C.F.R. § 164.308(b).

⁷³ 45 C.F.R. § 164.312.

to protect electronic protected health information from improper alteration or destruction;”⁷⁴ and the implementation specification states that there must be “mechanisms” to authenticate electronic PHI and to verify that such information has not been “altered or destroyed in an unauthorized manner.”

Despite providing these details, the HIPAA Security Rule does not tell covered entities how much security is “enough.” The technical safeguard standards, for example, tend to state what kinds of threats security mechanisms should guard against, but not how well they must do so.⁷⁵ Two factors help to explain this situation. First, HHS deliberately approached the Security Rule with an outlook of “technological neutrality”;⁷⁶ HHS stated that “it would be impossible to dictate a specific solution or set of solutions that would be usable by all covered entities.”⁷⁷ Second, Congress directed HHS to consider the costs and benefits of security measures and to recognize that the Security Rule would affect a highly diverse group of entities—small, rural, etc.—in the health care industry. Perhaps for this reason, many of the standards in the Security Rule boil down to covered entities’ discretion about what risks are “reasonable and appropriate” to consider, and hence which security measures are “reasonable and appropriate” to take.⁷⁸

3.2.7. Sarbanes-Oxley Act

A final example of a core information security law that regulates public-sector entities is the Sarbanes-Oxley act of 2002 (SOX).⁷⁹ Congress passed the Sarbanes-Oxley Act after corporate and accounting scandals at Enron, WorldCom, and several other major U.S. corporations led to their bankruptcies or even destruction. SOX effectively creates requirement to protect the integrity of information that goes into a publicly traded corporation’s financial reports. This mandate comes primarily from regulations implementing section 404 of the Act, which require publicly traded companies (all others are exempt from SOX) to implement “an adequate internal control structure and procedures for financial reporting.”⁸⁰ This mandate is backed up by a reporting requirement—the top managers of a corporation (usually the CEO and CFO) must issue a report containing their assessment, with attestation from the firm’s accountant, of the firm’s internal controls⁸¹—and criminal penalties for filing a fraudulent report.

The connection between Sarbanes-Oxley and information security is a bit tenuous. Though the internal control mandate was developed against the background of corporate fraud that spurred Congress to pass SOX, it is not limited to fraud.⁸² Instead, a Securities and Exchange

⁷⁴ 45 C.F.R. § 164.312(c)(1).

⁷⁵ An exception is the access control standards, which states that an information system must grant access “only to those persons or software programs” that have been properly granted access rights. 45 C.F.R. § 164.312(a)(1).

⁷⁶ Hoffman & Podgurski, *supra* note 3.2.6, at 338.

⁷⁷ 68 Fed. Reg. at 8335.

⁷⁸ See 45 C.F.R. § 164.308(a)(ii)(B) (stating the implementation standard for risk management).

⁷⁹ Pub. L. No. 107-204 (codified in scattered sections of 15 U.S.C.).

⁸⁰ 15 U.S.C. § 7262(a).

⁸¹ SOX § 404(b).

⁸² In this regard, SOX is similar to the Foreign Corrupt Practices Act, which requires publicly traded companies “maintain a system of internal controls” to assure the integrity of financial reporting information. Pub. L. No. 95-213 § 102 (1977) (codified at 15 U.S.C. § 78m(b)). See also Romano, *Quack Corporate Governance*, *supra* note , at 1541 & n.56.

Commission (SEC) regulation issued pursuant to section 404 states that a company's internal controls must "provide reasonable assurance regarding the reliability of financial reporting."⁸³ One of the requirements for such controls is that they provide "reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements."⁸⁴ Thus, to the extent that information is a corporate asset, SOX could be interpreted to require corporations to make preventing and detecting unauthorized access to information systems, at least if such access could have a "material effect" on the company's financial position.⁸⁵

Sarbanes-Oxley, however, has rather severe limitations as an information security law. First, it applies only to publicly traded corporations. Many of the corporations that play a critical role in information infrastructure security are organized differently. Many hospitals, for example, are organized as nonprofit corporations, while many IT companies do not have publicly traded stocks. Thus, even if its internal control mandates promote the development of integrity-enhancing mechanisms in SOX-regulated companies, the vast majority of U.S. businesses are under no obligation to follow suit.⁸⁶ Second, the purpose of the law is to punish and deter fraud by corporate managers, board members, and auditors; weak information security policies and practices within a company, without more, are unlikely to interest the Securities and Exchange Commission or Department of Justice, which have the authority to enforce SOX. Finally, the backlash against SOX in business, academic, and government circles has been intense.⁸⁷ Aside from imposing compliance costs and arguably chasing some corporations out of U.S. securities exchanges, SOX has been criticized for imposing *substantive* corporate governance mandates at the national level. That is, the internal control requirements (among others) impose specific duties on managers and board members.⁸⁸ This style of regulation is strongly at odds with the other organization-based information security laws discussed here, and the momentum seems to building to reduce, rather than expand, this approach.

3.3. Public Sector Organizational Regulations

Imposing substantive duties on officials within government agencies is quite a different story from defining duties within corporations and other private organizations. The need to oversee how agencies use public funds and how they are using (or abusing) their legal authority lead to

⁸³ 17 C.F.R. § 240.13a-15(f), available at <http://www.sec.gov/rules/final/33-8238.htm>.

⁸⁴ 17 C.F.R. § 240.13a-15(f)(3).

⁸⁵ This argument is made by Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 139-40 (2005).

⁸⁶ See Stephen Bainbridge, THE COMPLETE GUIDE TO SARBANES-OXLEY: UNDERSTANDING HOW SARBANES-OXLEY AFFECTS YOUR BUSINESS, Ch. 1 (2007), AVAILABLE AT <http://ssrn.com/abstract=1028033> (stating that SOX directly affects 13,000 of the more than 4 million corporations in the United States).

⁸⁷ See, e.g., Erik F. Gerding, *The Next Epidemic: Bubbles and the Growth and Decay of Securities Regulation*, 38 CONN. L. REV. 393, 393 (2006) (stating that "[t]he backlash against the Sarbanes-Oxley Act has begun in earnest" and quoting President George W. Bush and SEC Chairman Christopher Cox); *id.* n.160 (citing articles calling for reform of Sarbanes-Oxley).

⁸⁸ See Romano, *The Making of Quack Corporate Governance*, *supra* note , at 1540-43.

extensive intra-agency accountability mechanisms being imposed by Congress as well as within the hierarchy of an agency. Congress also plays an active role in overseeing executive branch agencies. This combination of approaches is evident in the first information security laws discussed in this section, the Federal Information Security Management Act of 2002 (FISMA). FISMA combines some of the sector-specific approaches discussed above with direct regulation of federal agencies' hierarchy, resulting in a general information security law that has no counterpart for private-sector organizations. The second law discussed in this section is the Privacy Act of 1974, which creates a security standard for databases maintained by federal agencies. Like FISMA, the Privacy Act's information security standard applies to nearly all federal agencies. Unlike FISMA, however, it contains few mechanisms for monitoring the agencies' information security performance.

3.3.1. Federal Information Security Management Act

FISMA⁸⁹ exemplifies the definition of a core information security law. Its purpose is to “provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.”⁹⁰ Moreover, FISMA adopts a definition of “information security” that closely tracks the technical definition reviewed earlier in this paper.⁹¹ Thus, FISMA states a conception of information security that comports with both technical notions of security as well as with the other information security laws reviewed in this paper. FISMA also sets a substantive standard for the performance of each agency's information security that tracks the risk-based compliance standards set forth in HIPAA and the Gramm-Leach Bliley Act: each agency must “provid[e] information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction” of information that the agency or its contractors collect, use, or maintain.⁹²

It is FISMA's significantly different means for achieving information security that is of interest here. The Act makes use of three policy levers that are rarely, if ever, used in regulating

⁸⁹ Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002) (codified at 44 U.S.C. §§ 3541-3549).

⁹⁰ 44 U.S.C. § 3541(1).

⁹¹ The definition is stated in 44 U.S.C. § 3542(b)(1):

The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provideâ”

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

⁹² 44 U.S.C. § 3544. FISMA's definition of information security, in turn, closely tracks the one given in Part 2. *See* 44 U.S.C. § 3541.

information security in the private sector. First, FISMA leverages and amplifies the hierarchy within the federal government to establish standards and oversee compliance with them. The Director of the Office of Management and Budget (OMB) is responsible for coordinating information security within the covered agencies.⁹³ Federal agencies are required to name a chief information officer, who must develop an agency information security program, in conjunction with the Director of OMB, based on federal standards.⁹⁴ These standards, in turn, have been developed by NIST;⁹⁵ the resulting documents provide a risk management framework that includes standards for categorizing information, selecting security mechanisms, and documenting and evaluating their effectiveness.⁹⁶ This approach of assigning substantive duties to government officials—and administrative mandate—contrasts sharply with the regulation of private-sector organizations, where SOX provides the sole example of a law that directs how an organization must approach information security. A further point of contrast is that there may be no way to enforce an agency’s FISMA duties in court, a remedy that might be useful if a federal agency exposes sensitive personal information through a security breach.⁹⁷

Second, FISMA relies heavily on ongoing monitoring to enforce compliance. Monitoring takes place at two levels. The first level is the Director of OMB, who has the authority to “enforce accountability” through means that may include cut agency budget requests, though OMB does not appear to have taken such drastic action.⁹⁸ The second layer of oversight is Congress itself. Each federal agency covered by the Act must send an annual report to Congress specifically on the “adequacy and effectiveness” of its information security management policies and programs.⁹⁹ After receiving the reports, a Congressional committee hands out grades for each agency.¹⁰⁰ In addition, each year since FISMA went into effect, Congress has held hearings that provide opportunities to grill CIOs from agencies with failing grades and praise those from highly rated agencies. Congress has also directed the Government Accountability Office to study

⁹³ 44 U.S.C. § 3543.

⁹⁴ 44 U.S.C. § 3506.

⁹⁵ Under authority granted by 40 U.S.C. § 11331.

⁹⁶ All of these guidelines and standards are available at

<http://csrc.nist.gov/groups/SMA/fisma/index.html>.

⁹⁷ The sole Court of Appeals to consider FISMA enforcement considered a situation that fits this description: in *Cobell v. Kempthorne*, beneficiaries of an Indian trust fund sued the Secretary of the Interior, in part to compel Interior to comply with FISMA, alleging that the Department had not adequately secured trust fund data. 455 F.3d 301 (D.C. Cir. 2006). Regarding judicial enforcement of FISMA, the court stated: “Notably absent from FISMA is a role for the judicial branch. We are far from certain that courts would ever be able to review the choices an agency makes in carrying out its FISMA obligations.” *Id.* at 314.

⁹⁸ The Director of OMB’s budget authority is provided through 44 U.S.C. § 3543(a)(4) and 40 U.S.C. § 11303(b)(5). One critic of FISMA has called the budget-reduction penalty a “stick . . . so draconian and counterproductive to agency effectiveness that it is hard to imagine OMB ever fully imposing it.” Robert Silvers, *Rethinking FISMA and Federal Information Security Policy*, 81 N.Y.U. L. REV. 1844, 1862 (2006).

⁹⁹ 44 U.S.C. § 3544(c).

¹⁰⁰ See William Jackson, *Cyber eye: Cybersecurity report cards don’t make the grade*, GCN.COM (May 16, 2005), at http://www.gcn.com/print/24_11/35774-1.html.

ways to make OMB's role more effective.¹⁰¹ Despite this coordinated and continuing oversight, the security of most federal information systems appears to be rather poor.¹⁰² Some FISMA critics have argued that the law's requirements place too heavy an emphasis on process and compliance, rather than performance.¹⁰³

This point, however, begs the question of how to measure security performance. As the National Research Council's report *Toward a Safer and More Secure Cyberspace* cautions:

Researchers have sought good metrics for many years, and though many benefits would flow from the invention of good metrics, the challenge in this cybersecurity research area is particularly great and some very new ideas will be needed if cybersecurity metricians are to make more progress.¹⁰⁴

Moreover, even if meaningful metrics were available, the question of how to set priorities and enforce certain levels of performance, short of mandating specific mechanisms, would remain. Such detailed mandates are nowhere to be found in FISMA or anywhere else in the body of information security law that this paper has discussed.

3.3.2. Privacy Act

Finally, the model of continuing oversight is prominent in the federal Privacy Act of 1974.¹⁰⁵ Much of the Privacy Act is concerned with "requiring governmental agencies to maintain accurate records and providing individuals with more control over the gathering, dissemination, and accuracy of agency information about themselves."¹⁰⁶ The Privacy Act is limited to certain kinds of government-held data, specifically federal agency records "from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" are covered.¹⁰⁷ As part of the privacy framework for these records, the Act imposes an explicit information security mandate:¹⁰⁸

Each agency that maintains a system of records shall . . . establish appropriate administrative, technical, and physical safeguards to insure the security and

¹⁰¹ See U.S. Gov't Accountability Office, *Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses* 46-47 (July 27, 2007) (recommending that OMB require reporting of agency patch management).

¹⁰² See Brian Krebs, *DHS Gets Another F in Computer Security*, WASH. POST (Mar. 15, 2006), at <http://www.washingtonpost.com/wp-dyn/content/article/2006/03/15/AR2006031501589.html>.

¹⁰³ See, e.g., James A. Lewis, *Testimony before the House Committee on Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement and the Subcommittee on Information Policy, Census, and National Archives* (June 7, 2007), at <http://www.csis.org/media/csis/congress/ts070607lewis.pdf>.

¹⁰⁴ NATIONAL RESEARCH COUNCIL, *TOWARD A SAFER AND MORE SECURE CYBERSPACE* at 6-20.

¹⁰⁵ Pub. L. No. 93-579 (Dec. 31, 1974) (codified at 5 U.S.C. § 552a).

¹⁰⁶ *Devine v. United States*, 202 F.3d 547, 550 (2d Cir. 2000). For a helpful overview of the Privacy Act's history and substance, see Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 360-62.

¹⁰⁷ 5 U.S.C. § 552a(a)(5); see also *McCready v. Nicholson*, 465 F.3d 1, 9 (D.C. Cir. 2006).

¹⁰⁸ 5 U.S.C. § 552a(e)(10).

confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Given the explicit focus on protecting the confidentiality of information against attacks, the Privacy Act fits the definition of a core information security law.

The Privacy Act, however, has provided little impetus to increase information security within federal agencies. Individuals may sue an agency for violating the Privacy Act.¹⁰⁹ In this regard, the Privacy Act follows the model of the statutes described above, which use the threat of liability for improper disclosure to encourage organizations—federal agencies, in this case—to adopt mechanisms to prevent such disclosures. Though a few civil cases allege violations of the Act’s security requirement, none of these claims reached final adjudication. As a result, judicial interpretations have not given further content to the standard of “appropriate” security for databases covered by the Privacy Act.

Unlike FISMA, the Privacy Act does not provide any mechanism for ongoing oversight that focuses on information security. Though a large majority of federal agencies report assessing threats to the systems containing records covered by the Act,¹¹⁰ little information is available about what results those assessments brought. Nor does the biennial report that the president must submit to Congress have any statutory requirement to discuss information security.¹¹¹ Moreover, given the limited amount of information that the Privacy Act protects, security requirement thus falls short of a generally applicable security requirement for federal information systems.

3.4. Summary

To summarize the findings from this Part, the technical definition of information security, with its focus on the properties of confidentiality, integrity, and availability, provides a useful heuristic: one can identify and group together statutes that create rights or duties with respect to information confidentiality, integrity, or availability. Part 3 has argued, however, that this definition, on its own, proves unilluminating. The ends of confidentiality, integrity, and availability are abstract and leave the means for achieving them unspecified. As a result, without more explanation, basing the information security law framework solely on the technical definition does not provide a means for analyzing how specific policies help (or hurt) information security. Organizing core information security laws according to whom (or what kinds of entities) they regulate, and what the laws require or prohibit, proves to be more insightful.

4. The Role of Information Security Law’s Periphery

This Part argues that three areas of law that fall outside the definition of core information security law—consumer protection, setting research priorities through legislation, and government

¹⁰⁹ 5 U.S.C. § 552g.

¹¹⁰ U.S. General Accounting Office, *Privacy Act: OMB Leadership Needed to Improve Agency Compliance* 20 (June 2003) (stating that 82% of agencies report assessing “threats, vulnerabilities, and effectiveness of current or proposed safeguards” for systems that contain Privacy Act records).

¹¹¹ 5 U.S.C. § 552a(s).

coordination under the Homeland Security Act—have constructive roles to play in improving information security.¹¹²

4.1. Consumer Protection

In recent years, the Federal Trade Commission (FTC) has used its authority to fight “unfair or deceptive” trade practices¹¹³ to sue companies that sold products containing software with security vulnerabilities. Most notably, in 2005, the FTC sued the record label Sony BMG for selling CDs that installed a rootkit on users’ PCs (to prevent copying the CD), leaving those PCs vulnerable to local and remote attacks.¹¹⁴ The FTC has also sued companies that failed to take adequate measures to protect customers’ personally identifiable information.¹¹⁵ Like many core information security laws, the standard for security policies, practices, and mechanisms that emerges from many of the FTC’s enforcement actions is that of reasonableness.¹¹⁶ Accordingly, the potential to use FTC enforcement actions to give clear guidance to information technology firms may be limited, just as the sector-specific laws discussed in Part 3 tend to leave individual firms with wide discretion to choose specific technologies to meet general performance goals.¹¹⁷

4.2. Promoting Research

Congress can also continue to use research spending as a means to improve information security. Appropriations for research funding do not create rights or duties with respect to information

¹¹² One area that this Part does not address is the use of tort or defective products liability for insecure software, hardware, or information good or services. For an early analysis, see Pamela Samuelson, *Liability for Defective Electronic Information*, 36 COMM. ACM 21 (1993). Making vendors liable for producing insecure technology is an idea that has long been proposed as a way to make entities internalize the costs that their technologies currently impose on others. Nonetheless, neither statutes nor case law has developed to impose this kind of liability. Since the focus of this paper is on formally enacted laws and statutes, tort liability (and related doctrines) is beyond the scope of this paper.

¹¹³ 15 U.S.C. § 45. The FTC’s mandate says nothing in particular about enforcing a right or duty relating to information security, so it does not fit the definition of a core information security law.

¹¹⁴ See Agreement Containing Consent Order, *In re Sony BMG Music Entm’t*, FTC File No. 062 3019 (Jan. 30, 2007), available at

<http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf>. For a detailed discussion of the Sony BMG episode and a thoughtful proposal to use the FTC’s consumer protection to set standards for user notice and consent in the context of information security and privacy, see Deirdre K. Mulligan and Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Incident*, 22 BERKELEY TECH. L.J. 1157 (2007) [hereinafter Mulligan & Perzanowski, *Magnificence of the Disaster*].

¹¹⁵ See Mulligan & Perzanowski, *Magnificence of the Disaster*, *supra* note , at 1211-18 and accompanying footnotes.

¹¹⁶ See *id.* at 1212; see also *In re Sony BMG Music Entertainment*, FTC File No. 062-3019, Agreement Containing Consent Order § VII.A (Jan. 30, 2007) (requiring Sony BMG to provide “a reasonable and effective means for consumers to uninstall” software).

¹¹⁷ But, as Mulligan and Perzanowski point out, the FTC could coordinate more technical, detailed discussions among industry, academic, and government findings to develop clearer guidance. Mulligan & Perzanowski, *Magnificence of the Disaster*, *supra* note , at 1224-31.

confidentiality, integrity, or availability, except to the extent that they direct a funding agency to spend money on security-related research. Indeed, some of Congress' uses of research policy to address information security as a very broad goal, to the point of expressing nothing more specific than an aspiration of improved security.

For example, the High-Performance Computing Act of 1991 (HPCA),¹¹⁸ sought to make the provision of "security requirements, policies, and standards" part of a national program to develop the Internet (which was, at that time, controlled by the federal government).¹¹⁹ A revision to the HPCA, the Next-Generation Internet Research Act of 1998,¹²⁰ declared that "[i]nformation security is an important part of computing" and that "research into security architectures is a critical aspect of computing, information, and communications research programs."¹²¹ As a whole, this act emphasized the development of Internet functionality but left unchanged the HPCA's general aspiration of making security part of the Internet's development. By contrast, the Cyber Security Research and Development Act of 2002¹²² appropriated money for the National Science Foundation to award in "grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security."¹²³ Finally, granting agencies themselves generally have some discretion under their legislative or regulatory missions to fund information security research.¹²⁴

Research funding complements the other approaches reviewed in this paper, in several ways. Most significantly, it allows information security investments to be targeted in ways that the other legal approaches discussed in this paper have difficulty achieving. For instance, the Cyber Security Research and Development Act identified several areas in which additional work is likely to lead to improvements in information security. Some of these topics overlap with security mechanisms that the laws discussed above require firms or government agencies to implement, including authentication, intrusion detection, emerging threats, and vulnerability assessments.¹²⁵ By contrast, as the discussions of the Sarbanes-Oxley Act and FISMA pointed out, legislation is not a viable way to directing corporate and federal agency budgeting with this level of precision. Research funding also allows at least some coordination in setting priorities for the development of new technologies, creating room for research into long-term solutions. Research funding also makes technology transfer a priority.¹²⁶

¹¹⁸ Pub. L. No. 102-194 (Dec. 9, 1991) (codified at 15 U.S.C. § 5501 *et seq.*)

¹¹⁹ HCPA § 101(a)(2)(I), 15 U.S.C. § 5511(a)(2)(I).

¹²⁰ Pub. L. 105-305 (Oct. 28, 1998)

¹²¹ Next-Generation Internet Research Act of 1998, Pub. L. No. 105-305, § 2(b)(2) (adding 15 U.S.C. § 5501(9)).

¹²² Pub. L. No. 107-305 (Nov. 27, 2002) (codified at 15 U.S.C. §§ 7401 *et seq.*).

¹²³ 15 U.S.C. § 7403(a).

¹²⁴ For a historical review of the role that funding agencies have played in information security research, see Chapter 6 of NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE. A more recent look at research funding priorities that are not tied to particular legislative mandates is in National Science and Technology Council, *Federal Plan for Cyber Security and Information Assurance Research and Development* (April 2006). [hereinafter NSTC, *Federal Plan*]

¹²⁵ 15 U.S.C. § 7403(a)(1).

¹²⁶ See, e.g., NSTC, *Federal Plan*, *supra* note , at 111 (noting that the Department of Energy "promotes the transfer of the results of its basic research to a broad set of application fields").

It is worth pointing out here that funding is not the only way that the law affects the development of information security research. A variety of laws, from copyright laws to electronic communications privacy laws, also constrain researchers' activities. Creating security research exemptions, or expanding existing ones, therefore could provide important assistance for information security researchers.¹²⁷

4.3. Promoting Government as Coordinator

This Part examines the use of law to establish the role of government as a coordinator of information security activities within the public and private sectors. The most extensive and sustained effort in this direction is taking place under the auspices of the Homeland Security Act of 2002,¹²⁸ which gave DHS authority to develop a plan to secure U.S. critical infrastructure, including the information infrastructure.¹²⁹

The Act's characterization of security closely tracks the technical definition that underlies core information security law this paper.¹³⁰ As was the case with research funding, does not create specific obligations with respect to information security. The law also works through means other than deterrence; it delegates to DHS broad authority to protect information security.

Extensive coordination with sector-specific agencies as well as the private sector is central to of DHS's approach to its responsibility of protecting the information infrastructure on a national scale. The NIPP details the ways in which DHS is creating public-private partnerships focused on information security: there are partnerships (actual or planned) for objectives ranging from education and training to information sharing and analysis.¹³¹ Information security experts have long made the case for public-private partnerships, arguing that the proliferation of firms that provide information technology to the government and the private sector undermined the effectiveness of government mandates and purchasing power as means of controlling technology.¹³²

¹²⁷ Privacy issues arising from security research are discussed in Aaron J. Burstein, *Toward a Culture of Cybersecurity Research* (in preparation). Copyright-related issues are examined by Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L. J. 501 (2003).

¹²⁸ Pub. L. No. 107-296.

¹²⁹ See Homeland Security Act § 201(a)(5). See also NIPP at 17-18; Homeland Security Presidential Directive 7; and the *National Strategy for Homeland Security* (stating that DHS would "forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructures and key assets from terrorist attack").

¹³⁰ Homeland Security Act § 212(5)(A) (referring to the goal of ensuring the "availability, integrity, and reliability" of critical infrastructure).

¹³¹ See NIPP at 107-22.

¹³² See NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE, *supra* note , at 219-21; Marjory S. Blumenthal, *The Politics and Policies of Enhancing Trustworthiness for Information Systems*, 4 COMM. L. & POL'Y 513, 537-43 (1999) ("A call for public-private partnership is the central theme in trustworthiness policy making, most notably in the information security and critical infrastructure arenas.").

As the National Research Council report *Trust in Cyberspace* noted however, “the meaning of ‘partnership’ must be developed and translated into action.”¹³³ This remains true, though an additional caveat applies. The statutory authority for DHS’s role as coordinator gives the department extremely broad discretion as to how to fulfill its mission. A lesson from the discussion of core information security laws that regulate private organizations is that oversight is necessary to define standards and to ensure that the regulated entities are meeting them. The same is true in this context; overseeing the delegation of information security authority to DHS requires not only cooperation between DHS and the private sector, but also attention (from Congress and others) to how this cooperation is being managed. This presents difficult questions about how to balance the needs of oversight with the sensitivity of information that might be shared in public-private partnerships. Answering them is beyond the scope of this paper, but, to conclude, public trust in DHS and private sector partners is important to the effectiveness of all of them in improving information security.

5. Conclusion

The goal of this paper has been to create a framework for information security law that (to paraphrase *Toward a Safer and More Secure Cyberspace*) better translates policymakers’ attention to information security into action. This concluding section points to a few ways in which the framework could serve as the basis for action.

First, the two different modes of deterrence explored in this paper—deterrence of individual actions and deterrence of organizational actions—suggest a need to pay greater attention to this distinction in developing information security policy. The principal law to deter information security violations by individuals, the Computer Fraud and Abuse Act, prohibits an extremely broad range of conduct. Initiatives to broaden this range should be closely examined and weighed against the costs and benefits of increasing penalties for existing offenses and devoting greater resources to enforcement.

Second, the structure of individual deterrents in current information security law does little, if anything, to encourage the adoption of more secure technologies. Thus, within the deterrence framework, the more important lever for adopting (and producing) secure technologies is to regulate private organizations and public agencies. As discussed in Part 3.2, creating substantive corporate governance duties within private organizations through federal legislation is rare for any purpose. Security is no exception. Thus, working within the models of sector-specific performance regulations and security breach notifications might hold the most promise. Collecting data about information security practices and expenditures in regulated industries could help provide more meaningful guidance than the existing regulations, without imposing technology mandates.

Third, implementing information security policy by means other than deterrence is a well-established approach. Funding research allows policymakers to direct spending on specific problems in a way that they generally cannot when regulating private sector organizations or overseeing public agencies. As pointed out in Part 4.2, however, security researchers would greatly benefit from exemptions to, or clarifications of, laws that expose them to liability in the course of conducting their research.

¹³³ NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE, *supra* note , at 220.

A final suggestion arises from the framework's identification of using public-private partnerships to protect information security. As pointed out in Part 4.3, the legal framework in this area is nebulous. Oversight of these partnerships is important not only to maintain fidelity with the goal of information infrastructure protection, but also to ensure public trust in the public and private organizations that join these partnerships. A place to begin this oversight is with a comprehensive listing of the composition, goals, and structures of all public-private partnerships that play a role in information infrastructure protection.

Law	Citation	Summary	Properties
“CORE” INFORMATION SECURITY LAWS			
INDIVIDUAL PROHIBITIONS			
Computer Fraud & Abuse Act (CFAA)	18 U.S.C. § 1030 (1984)	Prohibits transmitting “a program, information, code, or command” and thereby causing damage to a computer connected to the Internet. Prohibits “intentionally access[ing] a protected computer without authorization” and thereby causing damage. Certain types of computers—U.S. government computers and those of financial institutions and consumer reporting agencies—are protected against any access exceeding authorization that results in obtaining information; no damage to the computer is required.	Confidentiality Integrity Availability
Wiretap Act	18 U.S.C. § 2510 <i>et seq.</i>	Prohibits interception of electronic, wire, and oral communications	Confidentiality
PRIVATE SECTOR ORGANIZATIONAL REGULATIONS			
Fair Credit Reporting Act (FCRA)	15 U.S.C. § 1681 (1970)	Requires financial institutions and credit reporting agencies	Confidentiality Integrity
Family Educational Rights & Privacy Act (FERPA)	20 U.S.C. § 1232g	Requires federally funded educational institutions to disclose student records only under specific circumstances	Confidentiality
Stored Communications Act (SCA)	18 U.S.C. § 2701-2711	Prohibits certain communications service providers from disclosing communications contents and customer records	Confidentiality
Gramm-Leach-Bliley Act (GLBA)	15 U.S.C. §§ 6801-6805 (1999); 69 Fed. Reg. 77,610 (Dec. 28, 2004) (“Security	GLBA requires development of federal standards for ensuring the security and confidentiality financial institutions’ customers’ information against “anticipated threats or hazards” and against “unauthorized access or use.” The Security	Confidentiality

	Guidelines”); 70 Fed. Reg.15,736 (Mar. 29, 2005) (“Response Guidelines”)	Guidelines require financial institutions to dispose of customer records “properly.” The Response Guidelines require financial institutions to conduct risk assessments, to “consider” security measures that are appropriate,” report suspicious activities to the relevant federal regulator, report criminal activity, take “appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information,” and “[n]otif[y] customers when warranted.”	
Security Breach Notification Laws	State-by-state; <i>see, e.g.</i> , Cal. Civ. Code §1798.82	Require public disclosure of information system security breaches that expose personal information	Confidentiality
Health Insurance Portability & Accountability Act (HIPAA) Security Rule	45 C.F.R. parts 160-64 (2003)	Prohibits covered entities (healthcare providers, healthcare facilities, and health insurers) from disclosing protected health information. Requires covered entities to maintain “reasonable and appropriate” security safeguards.	Confidentiality Integrity
Sarbanes-Oxley Act	Pub. L. No. 107-204 (codified in scattered sections of Title 15 U.S.C.) and SEC regulations	Implementing regulations require public corporations to adopt internal controls over financial information to assure its reliability and that it reflects “timely detection of unauthorized acquisition, use or disposition” of the corporation’s assets that “could have a material effect” on its finances.	Integrity
PUBLIC SECTOR AGENCY REGULATIONS			
Federal Information Security Management Act (FISMA)	Title III of Pub. L. No. 107-347 (codified at 44 U.S.C. §§ 3541-3549) (2002)	Makes Director of OMB responsible for coordinating information security standards and compliance in the federal government. Requires covered federal agencies to name chief information officers. Requires annual evaluations and reports to Congress.	Confidentiality Integrity Availability
Privacy Act	5 U.S.C. § 552a (1974)	Requires federal agencies to protect certain records about individuals against “anticipated threats or	Confidentiality Integrity

		hazards to their security or integrity” and cause harm to the individual identified in the record.	
“PERIPHERAL” INFORMATION SECURITY LAWS			
Federal Trade Commission Act	15 U.S.C. § 41 <i>et seq.</i>	Authorizes FTC to enforce ban on “unfair or deceptive” practices	
Cyber Security Research and Development Act of 2002	15 U.S.C. § 7401	Directs NSF to fund grants pertaining to basic research in information security	
Homeland Security Act of 2002	Pub. L. No. 107-296	Gives Dept. of Homeland Security authority to protect U.S. information infrastructure	