Adapting Legal and Regulatory Aspects of Privacy and Security into Information Assurance Coursework

by

John W. Bagby
Professor of Information Sciences & Technology
Co-Director, Institute for Information Policy
The Pennsylvania State University

Abstract:

There is an emerging field of research and instruction in security and privacy law as applied to information assurance curricula in higher education. Of particular importance are various sources of institutional restrictions and opportunities from international law, federal and state laws and non-governmental organizations. This paper reviews this emerging field by exploring the interplay of constraints from criminal and civil law with emphasis on enforcement by regulatory agencies and self-regulatory organizations and with a view to enhancing liability risk management. Implications emerge on information assurance, information security and privacy that combine mandatory governmental standards, professional standards and best practices. This paper discusses the curricular development and its application to define this field for instructional and research purposes in the public policy realm.

I. Introduction: a Public Policy Imperative for Information Assurance (IA)

There is widespread ignorance and misunderstanding in higher education about liability risk exposure under privacy and security law. This is a particular concern for financial services and information technology (IT) professionals. The institutional, regulatory and public policy environment has grown highly complex further contributing to its strong intellectual merit. There is currently an undergraduate curriculum gap in many IT, engineering and business programs. To bridge this gap, a definition of the relevant field of privacy and security law is under development and with a view to further selection and arrangement as educational materials in support of coursework for delivery in higher education and in continuing professional education. This project’s objectives include: defining the field of security and privacy for higher education instruction in the
emerging field of information assurance (IA),\(^1\) the design of coursework and course materials for information assurance and the design of research agenda in the legal, regulatory and public policy aspects of IA.

Institutional constraints on security historically focused on traditional criminal enforcement and a slow but steady increase in civil remedies through the twentieth century. Professional security protection could satisfy reasonable assurance criteria by managing legal and regulatory risks based on commonly-held understandings of burglary, theft, conversion and widely-understood but related institutional constraints in the protection of physical property. This focus retained effectiveness so long as physical security over tangible property appeared successful, even extending to the maintenance of control over mainframe computers and their physical peripherals appeared sufficient. However, the proliferation of networked computers has made access and storage ubiquitous, vastly increasing the vulnerability of confidential data, private information and critical national security infrastructure. Security and privacy regulation compliance responsibility now falls much more harshly on both organizations and more broadly on individual personnel with access and responsibilities for computerized and networked information. These complex new duties constrain organizations in the data management industry as well as suppliers and users of data and all participants in the information supply chain, including consultants, software suppliers, applications service providers, maintenance outsources and communications services providers.

Other factors exacerbate these liability risk management difficulties. Advances in network computer storage and use, the broadening perception of heightened value\(^2\) of

---

\(^1\) A provisional definition of information assurance (IA) is needed. Throughout this paper additional nuance and clarification are presented to the broad concept of IA.

Information Assurance (IA) - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. See NSTISSI #4009 (August, 1997).

Closer analysis of this NSTISSI standard reveals it contains two broad, overarching, but general duties (i.e., protect, defend). It lists five, recurring IA vulnerabilities that obligate IA participants to more specific duties that are the subject of considerable research and professional practice (i.e., availability, integrity, authentication, confidentiality, nonrepudiation). Finally, the standard acknowledges that IA is imperfect and that IA due diligence includes an ongoing preparation for remediation through restoration using detection and reaction (the second appearance of “protection” in the standard’s final sentence is arguably redundant).
information and the pervasive availability of rich data warehousing increase the vulnerability of data management. Risks of information theft and integrity losses as well as the explosion of privacy rights and national security concerns now require fuller understanding of liability risk management principles/techniques among all managers and subordinates engaged in data management for both private sector and the public sector.

Information suppliers, handlers, owners and network service providers are increasingly exposed to civil litigation, regulatory oversight/compliance and criminal prosecution for various information-related wrongs. For example, confidentiality is compulsory for corporate trade secrets, privacy is required for personally identifiable information about individuals and secrecy is mandatory over matters of national security. All these seemingly diverse duties are related by the information assurance function. Effective execution of these functions require compliance with complex legal duties that are not widely nor uniformly understood. Some new legal duties are fundamentally driving the design of information handling processes.

This project is identifying legal and regulatory constraints on information security and privacy practices. A coherent body of knowledge is being assembled and effective delivery mechanisms are under development to help make information management become more effective. Anthologies of relevant instructional materials are assembled and the refinement of these into a manageable collection of materials into readings, exercises and evaluation materials is underway.

II. A Public Policy Component to IA Curricula

This project maps the relationship links among a growing plethora of local, state, federal and international laws/regulations by setting methodologies to assess and reduce the major risk points in information processing. An inversion in the relationship between law and technology is increasingly heard: regulation is beginning to drive technological development and deployment rather than the converse. For example, the healthcare

---

privacy rules issued by the Department of Health and Human Services (HHS) are driving technology changes as they stimulate compliance.\(^3\)

The legal environment of technology has seldom been more than vaguely related to undergraduate education in technology. Exposure to institutional environmental constraints, opportunities and prospects is largely delivered through general education coursework (e.g., political science, history, sociology). Such general education experiences are focused largely as breadth and seldom as depth nor as an integrating experience on the issues related to the matters directly confronting the technology disciplines. Undergraduate students in technology disciplines have limited curricular flexibility so that most of the general education exposure about the legal, regulatory, public policy and institutional environment is limited to breadth rather than in depth coursework that is predominantly delivered at lower division levels (e.g., freshman, sophomore). Such coursework is seldom competently targeted to the range of laws, regulations, regulatory agencies or public policy issues directly impacting the likely work life issues of technology or IA students.\(^4\)

A flood of new laws covering homeland security and privacy, in the United States, the EU, and other nations clearly signals the need for public policy participants to have balanced preparation in the underlying technology and the public policy aspects of that technology. An initial survey and analysis of various authoritative sources show sharp increases in legislation, litigation and regulations with significant impact on security and privacy. These include constitutional law, IP, commercial law, technology transfer, criminal law/procedure, computer forensics, torts/malpractice liability, cyberlaw, Internet regulation, and antitrust/trade regulation/consumer protection, among others.


\(^4\) There are a few notable exceptions to this scarcity of profession-relevant curricula about the institutional environment. For example, environmental law is increasingly available to baccalaureate students in earth and mineral sciences, civil engineering, chemical engineering, environmental engineering, chemistry and the biological sciences. A similar trend is noted with baccalaureate offerings in occupational safety and health regulation for industrial engineering and operations research programs. Finally, baccalaureate coursework in professional ethics and malpractice liability risk management are increasingly required for professional certification in many technology and IT fields, (e.g., architectural engineering, civil engineering). Such coursework was traditionally available or required as part of professional certification in some business professions (e.g., accounting, real estate).
A balanced range of topic coverage and integration is needed to equip undergraduates in IA programs. To complicate these matters, there is general recognition that many new regulatory agencies have overlapping, sometimes conflicting jurisdiction over individuals, private sector businesses, government programs and international trade.\(^5\) For example, some of the more powerful agencies include the Department of Homeland Security (DHS), the Department of Defense (DOD), the Department of Energy (DOE), the Department of State, the U.S. Justice Department (DOJ), and many state attorneys general, local police and public safety officials. There are challenges in navigating cooperation among these agencies and IA students’ general unfamiliarity with administrative process strongly suggests scholarly examination of these topics.

Exposure to this curriculum will benefit IA students’ professional work performance as they are exposed to the intellectual tools needed to participate in the public policy debate over the increasing public sector and private sector policies, contractual requirements and expected new laws from all levels of government with respect to privacy, security, IP, anti-terrorism and the attendant professional duties. There is a growing national recognition of the need for this coursework as evidenced in the recommendations from various authoritative task force reports in disciplines such as law, government, security, CSE, IT and business.\(^6\)

### A. Course Design for Information Assurance

Information assurance curricula are garnering widespread interest at universities. The national imperative for counter-terrorism, cyber-terrorism readiness and response effectiveness strongly implicates the need for capacity-building in information assurance coursework. Many universities are developing curricula and degree programs for certification by the Committee on National Security Systems (CNSS) and the National Security Agency (NSA) as compliant with National Training Standard for Information Systems Security (INFOSEC) Professionals.\(^7\) This educational standard is a required

---

\(^5\) See infra section III.


\(^7\) As of 2004 there were 50 colleges or universities with programs certified as compliant with NSTISSI Standard No. 4011. These programs are largely located in computer science, engineering or business schools and are supported by the National Colloquium for Information Systems Security Education (NCISSE). See [http://www.ncisse.org/CAE%20InfoSec%20Degree%20Comparison.pdf](http://www.ncisse.org/CAE%20InfoSec%20Degree%20Comparison.pdf)
component of certification\(^8\) by the NSA for higher education programs in IA such as the program at the Pennsylvania State University (Penn State).\(^9\) A theme track in IA is deployed at the School of Information Sciences and Technology at the Pennsylvania State University that is certified as compliant with National Training Standard for Information Systems Security (INFOSEC) Professionals and for Designated Approving Authority.

**B. Course Design: Legal/Regulatory Environment of IA**

This section describes an important component of that effort – the legal, regulatory and public policy aspects of information assurance. During 2003 and 2004, numbered IST 452 was developed and approved as one of several permanent courses at the Penn State. IST 452 has a purpose of exploring the “legal, regulatory, public policy and ethical issues related to security and privacy for information technology professionals in public institutions, private enterprise and IT services.”\(^10\) This required course is a component in the IA theme track that accompanies other coursework in security and privacy.\(^11\)

The legal and regulatory aspects of IA are mapped to IST 452 to ensure the exploration of legal, regulatory, public policy and ethical issues related to security and privacy for IT professionals in public institutions, private enterprise and IT consulting.

---

\(^8\) The NSA certifies Centers of Academic Excellence in Information Assurance (IA) Education (CAEs) with a view to promoting higher education in IA and producing a growing number of professionals with IA expertise in various disciplines. Candidate programs are assessed against published criteria intended to measure depth and maturity of programs in IA. The certification criteria are based on National Security Telecommunications and Information Systems Security Committee (NSTISSC) Training Standards. The NSTISSC is now known as the Committee on National Security Systems (CNSS). Certification compliance is required with NSTISSI-4011: National Training Standard For Information Systems Security Professionals (June 20, 1994, see [http://www.nstissc.gov/Assets/pdf/4011.pdf](http://www.nstissc.gov/Assets/pdf/4011.pdf)) and at least one other additional designated NSTISSC Training Standard, *inter alia*, NSTISSI-4012: National Training Standard For Designated Approving Authority (DAA) (August 1997); NSTISSI-4013: National Information Assurance Training Standard For System Administrators (SA) (March 20004); NSTISSI-4014: National Training Standard For Information Systems Security Officers (ISSO) (August 1997); NSTISSI-4015: National Training Standard For System Certifiers (December 2000) or a subsequently developed, but related standard.

\(^9\) A “theme track” in IA is deployed at the School of Information Sciences and Technology (IST) at the Pennsylvania State University that is certified as compliant with NSTISSI-4011 and NSTISSI-4012. See generally, [http://net1.ist.psu.edu/cica](http://net1.ist.psu.edu/cica).

\(^10\) See New Course Proposal, Supporting Documentation-Course Description, “IST 452: Legal & Regulatory Environment of Privacy and Security,” (approved by University Faculty Senate, Pennsylvania State University, April 2004).

\(^11\) Other coursework includes numerous existing and proposed courses in IT generally and more specifically in IA/security-related matters, including *inter alia*, Network Security; Wireless Network: Design and Security; Database and Web Security Information Systems Security; Security Management; Applied Cryptography. See [http://net1.ist.psu.edu/cica](http://net1.ist.psu.edu/cica)
services. IST 452 focuses on developing a working knowledge of the legal and regulatory constraints and opportunities for privacy and security of IT systems. The coursework is intended to prepare IT professionals to identify public policy constraints and opportunities, participate in the public policy debate over privacy and security issues, manage liability risks and appreciate when and how to summon legal counsel.\textsuperscript{12} Table 1 summarizes the topics and class contact exposure for those topics configured as a one semester, three credit-hour course.

**Table 1 - Topic Outline: IST 452**

<table>
<thead>
<tr>
<th>Security &amp; Privacy Topics</th>
<th>Class Contact Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Litigation &amp; liability risk management</td>
<td>1 class</td>
</tr>
<tr>
<td>Litigation &amp; forensics</td>
<td>1 class</td>
</tr>
<tr>
<td>Regulatory investigations</td>
<td>1 class</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>1 class</td>
</tr>
<tr>
<td>Constitutional protections</td>
<td>2 classes</td>
</tr>
<tr>
<td>Computer crimes</td>
<td>3 classes</td>
</tr>
<tr>
<td>Computer torts</td>
<td>2 classes</td>
</tr>
<tr>
<td>Professional malpractice &amp; industry self-regulation</td>
<td>2 classes</td>
</tr>
<tr>
<td>Infringement risk management</td>
<td>2 classes</td>
</tr>
<tr>
<td>Internal confidentiality controls</td>
<td>2 classes</td>
</tr>
<tr>
<td>Protection of databases</td>
<td>2 classes</td>
</tr>
<tr>
<td>Employment &amp; service provider contracting &amp; monitoring</td>
<td>2 classes</td>
</tr>
<tr>
<td>Conceptual privacy</td>
<td>1 class</td>
</tr>
<tr>
<td>Financial privacy</td>
<td>1 class</td>
</tr>
<tr>
<td>Healthcare privacy</td>
<td>1 class</td>
</tr>
<tr>
<td>Online privacy</td>
<td>1 class</td>
</tr>
<tr>
<td>Children’s &amp; telecommunications privacy</td>
<td>1 class</td>
</tr>
<tr>
<td>International privacy</td>
<td>1 class</td>
</tr>
<tr>
<td>Group presentations</td>
<td>3 classes</td>
</tr>
</tbody>
</table>

\textsuperscript{12} The key instructional, educational and course objectives for IST 452 include fostering skills to integrate the following perspectives: (1) gain understanding of public policies underlying regulation of privacy rights and security duties, (2) gain insight into how society accommodates transition of existing laws to the unique vulnerabilities of government and the information economy, (3) gain skills to manage employment and independent contractor relations for personnel involved in privacy and security, (4) gain familiarity with processes used in interacting with many government agencies newly authorized to regulate privacy and security, e.g., federal departments of Homeland Security, Defense, Energy, State & Justice, the Federal Trade Commission, and state attorneys general, local police & public safety officials, (5) understand the legal and regulatory constraints in preparedness and response for counter-terrorism, (6) gain skills in risk management for avoiding liability and infringement, (7) understand the role of security and privacy in business model innovation for emerging electronic commercial practice in both public and private sector applications.
C. IA Course Design Process

In the first phase of this course development, the course design team surveyed the field of privacy and security law to identify relevant topics for IA undergraduate students’ coursework through identification and classification of privacy and security issues relating to IA undergraduate education. This included a literature review enabling the analysis of U.S. law found in statutes, regulations, cases and legislative proposals at federal and state levels. Some international law (e.g., EU) was also examined where international law has clear impact on U.S. government units, multi-national businesses and on the activities of technology professionals.

In the second phase, the provisional curriculum was researched in greater depth using traditional doctrinal legal and public policy research methods. This activity identified, classified and synthesized legal research, including case law, regulations, legislative histories and public policy proposals. The emerging topics were prioritized and the mix of topics is under refinement using consultation with faculty, scholars and practitioners in computer science, information sciences and technology, business disciplines and technology law at various conferences and workshops that have substantial components in privacy and security-related matters. Appropriate pedagogies and supporting instructional materials have been pilot tested and are under refinement.

There are no existing published or traditional instructional materials in privacy and security law for IA students in higher education. In the third phase, the author is further refining and developing instructional materials in security and privacy with a view

---

13 A similar refinement process was successfully employed between 1997 and 2003 by this author in the related field of cyberlaw. That effort assisted in the deployment of curricula and courses, the dissemination of curricular findings through professional panels and presentations, the coauthoring of textbooks and the implementation of upper-division coursework in the Legal Environment of Information Sciences and Technology. See Bagby, John W., eCommerce Law: Issues for Business, (West Publishing Co. Mason OH) (©2003); Bagby John W. and F. William McCarty (Western Michigan University), Legal and Regulatory Environment of e-Business: Law for the Converging Economy, (West Publishing Co. Mason OH) (©2003); Bagby, John W., Cyberlaw Handbook for eCommerce, (West Publishing Co. Mason OH) (©2003). This work effort has also resulted in engagement of related research streams.

14 Traditional law pedagogy is adapted using instructional techniques consistent with: (1) a modified Socratic method using appellate and business-style case analysis, (2) team projects, (3) a considerable writing component and (4) the integration of public policy into IT education. The methods include mastery over readings, lecture, problem-based learning (PBL), technical search and retrieval of relevant documents and reports, group research projects, in-class student participation, in-class team presentations, homework problems and written examinations including both objective and essay questions.
to filling this void. A few professional treatises are emerging on these topics\(^{15}\) and there are considerable government documents and web-based materials. However, these are too voluminous, too highly fragmented and too poorly connected for convenient use as instructional materials. This project is compiling and interpreting these materials for assembly into a coherent set of instructional materials initially embodied as an anthology of course readings and supplemented with other related components, e.g., websites, visuals, exercises, projects, study guides, examinations.

III. Institutional Environment of Financial Information Assurance

The institutional structure of financial information assurance (IA) is complex. A plethora of public and private sector participants are authorized to: (1) advocate or mandate assurance controls, (2) monitor and enforce assurance control deployment, (3) monitor effectiveness of IA controls, (4) provide general IA guidelines, and/or (5) require specific types of IA controls. This institutional structure is an obscure composite. It exhibits multi-jurisdictional complexity that poses challenges similar to other instances of parallel regulatory diffusion. This complex structure is further complicated by the context in which the IA conditions arise. For example, some IA requirements are dictated by disclosure rules aimed at transparency to improve market functions. Some IA requirements are directed at counter-terrorism and money laundering-based regulations that recognize the financial system’s vulnerability as a critical infrastructure target for terrorism or means of terrorism financing. Some IA requirements are driven by individual privacy laws. Finally, many IA practices are the direct result of proprietary needs for confidentiality. This complexity suggests that the elaborate relationships in financial IA

can be analogized it to a supply chain along which there are multiple loci for addressing IA control.

The emerging complexity of the financial IA institutional framework poses several major challenges: consistency, efficiency and industry capture. There is potential for inconsistent, even conflicting yet binding requirements from different regulatory agencies discussed in this section. Indeed, the challenges imposed on national security by a proliferation of autonomous agencies is becoming well known\textsuperscript{16} and an emerging recognition that this situation may cause dysfunction has prompted efforts to achieve structural coherence, such as with passage of watershed legislation like the Homeland Security Act.\textsuperscript{17} Another difficulty with the ungainly, multi-jurisdictional structure is its potential inefficiency. Redundant security efforts are rife and it can be argued that process-improvements and consolidation of many key functions across various agencies could release resources for more deserving projects without compromising effectiveness. Finally, the proliferation of scores of potentially relevant agencies and other institutions is likely the result of two dynamics: (1) the widespread recognition of the international, national and state/local imperative for various institutions to address security vulnerabilities and (2) the traditional political economy phenomena of capture.

There may be three broad categories of institutions with important impact on financial IA: (1) regulatory agencies, mostly federal, with direct, sectoral authority over IA activities of particular industries,\textsuperscript{18} (2) U.S. federal agencies with broad, omnibus

\textsuperscript{16} See Comments of Joe D. Whitley, General Counsel of the Department of Homeland Security, luncheon speaker, November 20, 2003 at The Business Response to the New Cybersecurity Threats and Terrorism, (American Bar Association) Washington DC. Inter-agency relations may not be optimal in achieving security assurance as noted in 9-11 Commission testimony about interaction among the law enforcement and intelligence communities, see e.g., The Performance of the Intelligence Community, Staff Statement No. 11 and Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11, Staff Statement No. 9, National Commission on Terrorist Attacks Upon the United States (9-11 Commission), April 14, 2004.

\textsuperscript{17} See H.R. 5005, 107th Cong. 2d Sess. (2002). The Homeland Security Act draws together numerous agencies under one coordinating control structure, many with theretofore overlapping authority. Integrating these agencies is an ongoing and formidable challenge.

\textsuperscript{18} Since the New Deal, the delegation doctrine is interpreted to limit legislative power so that regulatory agencies are generally given relatively narrow authority to regulate particular industries or economic sectors, e.g., Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935). The Gramm/Leach/Bliley Act (G/L/B) Pub. Law 106-102, 15 U.S.C. § 6801, et seq. clearly recognizes sectoral regulation in financial services, fragmenting regulation of financial IA among designated “federal functional regulators” (i.e., Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, Secretary of the Treasury, National Credit Union Administration, Federal Trade Commission, Securities and Exchange Commission and the various
authority over IA activities of various industries, and (3) non-governmental (NGO) or self-regulatory organizations (SRO) with IA influence or authority over particular industries or the activities of particular professionals. Of course, collaboration among particular participants from among these groups may create ad hoc or even persistent new institutional frameworks (e.g., COSO). Additionally, there will likely be global influences from various international sources such as particular national governments, affiliated trading groups like the NAFTA or the EU and international standards setting bodies (e.g., ISO). The following focuses discussion on institutions with the most immediate and direct impact on financial IA.

A. Sectoral IA Regulation

Since the Great Depression, IA influences on financial services have been significant from sectoral federal agencies. Most fundamentally, a wide variety of financial IA foci are mandated by most federal securities laws. The Securities and state insurance regulators) for safeguarding the personally identifiable financial information (PIFI) of clients and customers in the various sub-sectors of financial services industry directly regulated by the aforementioned regulators.

While this structure appears straightforward for regulated entities engaged in few lines of business, such simplicity becomes lost in industries characterized by vertical integration or conglomerate-style diversification. The apparent simplicity of narrow sectoral regulation is further undermined by an active market for corporate control in which business combinations bring theretofore independent industry sectors under administrative control of consolidated corporate entities then required to interact with various independent regulators.

There is clearly some sectoral government regulation that is not federal, but instead state and local. First responders to the (largely) physical results of terrorism are decidedly state and local, many are governmental (e.g., police, fire, HazMat) while others are private sector participants (e.g., utilities), see, e.g., http://www.firstresponder.org/ State level regulatory agencies with significant financial IA impact generally include banking, insurance and public utility regulators although there are others and many of these are unique to particular states. See e.g., non-standards bodies are also influential, consider the Committee of Sponsoring Organisations of the Treadway Commission (COSO) - a collaboration from among five major financial professional associations in the United States, the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives Institute, the Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants). http://www.coso.org/index.htm

See infra text and accompanying notes 28 to 34.

See, e.g., The International Standards Organization (ISO) has developed basic IA standards such as ISO/IEC 17799:2000, Information technology - Code of practice for information security management, http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html. Also important are international consortia of financial IA standards setting bodies such as the International Accounting Standards Board (IASB), see http://www.iasb.org.uk.

See e.g., Securities Act of 1933 (1933 Act); Securities Exchange Act of 1934 (1934 Act); Congress passed the Public Utility Holding Company Act of 1935; Investment Advisors Act of 1940; Investment Company Act of 1940; Foreign Corrupt Practice Act of 1977 (FCPA); and the Gramm-Leach-Bliley Act of
Exchange Commission (SEC) is the predominant federal regulator of financial IA matters relating to the securities markets and investment banking. In addition, IA regulation can be expected from the several commercial banking regulators23 the Federal Trade Commissions’ (FTC) authority over the privacy of creditworthiness reports used to evaluate credit, bonding and employment applicants and more narrowly sectoral regulatory environments surrounding the commodities markets,24 regulation of the state, municipal and industrial revenue bond markets (munis)25 and credit unions.26

At least two additional federal regulators impact IA regulation. First, the Department of Justice (DOJ) is the only federal agency empowered to bring criminal prosecutions of violations impacting security and privacy.27 Criminal activities jeopardizing financial IA are only prosecuted nationally by the DOJ28 and not by any

---

1999. The securities litigation reform movement of the 1980s and 1990s has resulted in a mixed bag for the IA community as the scandal-induced political pendulum has oscillated between restrictions on private and regulator litigation and expansions in private rights of action and regulatory oversight. See e.g., Insider Trading Sanctions Act of 1984 (ITSA); Insider Trading and Securities Fraud Enforcement Act of 1988 (ITSEEA); Enforcement Remedies and Penny Stock Reform Act of 1990; Private Securities Litigation Reform Act of 1995 (PSLRA); Securities Litigation Uniform Standards Act of 1998; and Sarbanes-Oxley Act of 2002 (SOX) (complete citations omitted).

23 Consider the regulatory balkanization of commercial banking with diffuse oversight from the Federal Reserve Board (FRB), The Comptroller of the Currency, the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS) (consolidating regulatory powers from predecessors such as the Federal Home Loan Bank Board (FHLBB) and the Federal Deposit Insurance Corporation (FSLIC)) and state banking commissions.

24 The Commodities Exchange Act is enabling legislation for the Commodities Futures Trading Commission (CFTC) see generally 7 U.S.C. § 1, et seq.

25 The Securities Acts Amendments of 1975 created the Municipal Securities Rulemaking Board as an SRO under SEC supervision.

26 The Federal Credit Union Act enables credit union regulation through the National Credit Union Administration (NCUA) and member deposits enjoy deposit insurance under the National Credit Union Share Insurance Fund (NCUSIF), 12 U.S.C. §§1751-1795k.

27 State crimes related to security and privacy are enforced by state attorneys general (AG) and/or county-municipal prosecutors. A few federal statutes empower state AGs to bring civil enforcement actions. Military courts are empowered to bring criminal actions concerning security matters involving military personnel or on military installations.

28 At least one possible exception may be the activities of the National Association of Attorneys General (NAAG), an organization comprised of all 50 state attorneys general that “fosters interstate cooperation on legal and law enforcement issues, conducts policy research and analysis of issues, and facilitates communication between the states’ chief legal officers and all levels of government.” See generally http://www.naag.org/naag/about_naag.php NAAG has increasingly coordinated prosecutions of both civil and criminal investigations among [at least some] state attorneys general in several high profile cases, e.g., tobacco, antitrust, product liability, securities fraud. NAAG now claims expansion of their reach “[i]n many areas traditionally considered the exclusive responsibility of the federal government, the Attorneys General now share enforcement authority.” Id. Although many recent cooperative efforts primarily pursue civil enforcement remedies, the underlying acts are often also susceptible to prosecution as state crimes. Examples of NAAG activities broadly relevant to IA include NAAG’s ongoing projects addressing antitrust...
other federal agency acting alone. The DOJ’s cybercrime, computer crime, bank fraud and money laundering focci also clearly implicate the DOJ’s enforcement authority in financial IA matters.

Another important federal agency, the Department of Health and Human Services (HHS), has sectoral impact on the IA of healthcare information, including criminal penalties for certain violations of the detailed HIPPA healthcare privacy rules. However, the financial IA connection to private healthcare information is less direct—largely through the healthcare payment system generally applicable to benefits providers in the private insurance industry (e.g., HMO, PPO) and participants in government payment programs like Medicaid, Medicare and state and local health agencies.

Nevertheless, the HIPPA healthcare privacy rules promulgated by HHS are among the most detailed and pervasive, implement the HIPPA statute’s criminal sanctions for

---

29 Many federal agencies can provide enforcement leads/tips, investigation files and expert assistance to DOJ, effectively fostering criminal prosecutions. See generally, Bagby, John W., Administrative Investigations: Preserving a Reasonable Balance Between Agency Powers and Target Rights, 23 Am.Bus.L.J. 319-349 (Fall 1985) (arguing SEC and DOJ frequently and actively share investigatory files potentially leading to enforcement actions in cases of securities and disclosure fraud, market manipulation and insider trading).

30 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required HHS to promulgate privacy rules. Public Law 104-191, 104th Cong. (1996). Healthcare information includes personally identifiable information (PII) about various diagnostics and treatments that often reveals a subject individual’s former and present health condition (e.g., test results for blood pressure, HIV, biopsy). HHS rules designate personally identifiable healthcare information as protected health information (PHI). PHI is essential to effective diagnosis and treatment and to healthcare payments by insurers. These immediate uses of healthcare information for rendering of essential healthcare services are called uses and disclosures for treatment, payment and operations. Indirect or secondary uses of PHI are uses and disclosures other than for treatment, payment and operations are often challenged as less valid by privacy advocates. For example, secondary uses might include employment or underwriting decisions to minimize healthcare costs or. Secondary use of health care information is essential to medical research that identifies treatments, cures or otherwise alleviates suffering.

HIPPA permits freer movement of employees among the different health care plans of different employers, restricts disclosure of PHI by the medical profession, hospitals, health insurers, employers and healthcare intermediaries. PHI issues were so contentious that HHS delayed nearly four years after HIPPA’s passage before promulgation of the HIPPA privacy regulations in December 2000. HHS estimates for implementation costs ranged from $5 billion to $17 billion annually and its estimates for annual benefits ranged from $9 billion to $21 billion.

HIPPA privacy rules restrict the data management and disclosure activities concerning oral, written or electronic PHI when conducted by several covered entities: e.g., health care providers, plans, clearinghouses, HMOs, PPOs and their affiliates. Generally, patients must give prior written consent, an opt-in, before PHI can be used for treatment or before PHI can be disclosed for other uses. There are several forms of consent depending on the context, many have highly technical requirements. Arguably, the health care institutions can simply decline to provide healthcare-related services or payments without patient consent (except in emergencies). Patients have IA rights to notice, access and correction, they may demand an accounting of disclosures made (date, recipient, brief description of PHI).
privacy violations and include private data security rules. These may become a model for
guidelines and rules in other sectors, including more direct financial IA contexts.

Ironically, the sectoral nature of U.S. IA regulation is further reinforced by
international law, most importantly, the European Union’s (EU) 1995 privacy directive. The EU directive requires all member states (EU member nations) to legislate privacy
rights that are strong, national and omnibus - generally spanning all industries and all
EU nations. Member nations must prohibit any transfer of personal data to another nation
unless the destination provides an adequate level of protection for privacy. Data transfers to nations not certified are still possible on an, ad hoc, sectoral-regulation

---

protection of individuals with regard to the processing of personal data and on the free movement of

32 Under the EU Directive, PII or information relating to an identifiable person is personal data. The
Directive regulates the processing of personal data (e.g., operations performed on personal data either by
automated or manual means) and personal data that becomes part of a filing system. The flow of private
data is severely restricted across borders. Data managers and their clients, called data controllers, have
various duties:

1. **data controller identification**, a form of notice and awareness. The collector must be identified
and must disclose the purposes for data processing and how to assure fair and lawful processing, Id. at Articles 10 and 11;
2. **legitimacy of data processing**, a form of consent. Generally, personal information may be
processed only if there is unambiguous consent, essentially an opt-in, unless processing is
necessary in the following situations: (i) to perform a contract or protect the interests of the data
subject (subject individual), (ii) to comply with legal obligations of the subject or controller, (iii)
for the controller to exercise its legitimate rights so long as the data subject’s fundamental rights
are not violated, and (iv) for the public interest. There is an opt-out provision to avoid automated
processing that evaluates individual characteristics or would otherwise significantly affect on the
data subject (e.g., computer or electronic agent effected credit decision using defined
creditworthiness criteria), Id. at Article 7;
3. subject individual **access**, the right to confirm their data is being processed, i.e., the purpose,
categories of data, recipients of personal data reports, Id. at Articles 12 and 14;
4. **objection rights** to prevent use of data in direct marketing; and
5. the right to **rectify or correct** (erase or block processing) when data is incomplete or inaccurate.

The EU Directive has IA provisions addressing data integrity and security:

1. personal data must be accurate and current and retained no longer than necessary, Id. at Article 6;
2. the data collector must use technical and organizational security and integrity measures to avoid
data loss, unlawful destruction or unauthorized access, alternation or disclosure, Id. at Article 17;
3. PII may be used only for the use originally collected it must be adequate, relevant and not
excessive considering the authorized purpose for processing, Id. at Article 6;
4. there is a special class of PII, highly sensitive data, that includes ethnic or racial demographics,
opinions or beliefs based on political, religious or philosophical views, health or sex life
information and membership in unions, information that enjoys enhanced protections;
5. the national laws of the EU member nations are the primary source for enforcement and redress,
Id. at Articles 22, 23 and 24.

33 Id. at Article 25. Adequacy is under these criteria: (i) nature of the data, (ii) purpose and duration of the
proposed processing, (iii) nation where data originates, (iv) nation of final destination and (v) privacy laws,
professional rules and security measures in the final destination nation.
basis.\textsuperscript{34} That is, despite the omnibus nature of the EU Directive, there must be regulatory provisions authorizing enforcement by sectoral government regulators in the other data transferee nation. To take advantage of this exception in EU privacy rules, the U.S. Department of Commerce has negotiated a \textit{Safe Harbor} with the EU that recognizing when U.S. privacy protection satisfies the EU adequacy standard.\textsuperscript{35} The safe harbor requires IA - data handling methods and practices.\textsuperscript{36} Adequacy is generally demonstrated with self-certification showing compliance in the firm’s privacy policies with the safe harbor. A sectoral U.S. regulator must serve as a forum for appeals and have authority to remedy the U.S. firm’s compliance failure.\textsuperscript{37}

\textbf{B. Federal Omnibus IA Regulation}

Several federal agencies have broad IA authorities covering many or even most sectors of the economy. The Federal Trade Commission (FTC) has assumed an increasing role as the principal regulator of individual privacy. In addition to its traditional role in protecting the privacy of consumer financial information under the Fair Credit Reporting Act of 1970\textsuperscript{38} the FTC received residual regulatory powers over PII practices of financial institutions not directly regulated by other designated federal functional regulators.\textsuperscript{39} The Department of Defense (DOD, and its predecessor the War Department) may be one of the two\textsuperscript{40} longest-standing federal agencies regulating security matters. The National Institute of Standards and Technology (NIST) conducts research and analyzes studies in pursuit of its mission to set standards for the work of federal agencies. While many NIST standards are targeted to government computer

\begin{footnotesize}
\begin{itemize}
\item Factors relevant to a proposed PII transfer include: (i) whether the data transfer would involve highly sensitive data, (ii) the potential for financial loss (e.g., Internet credit card payment), (iii) personal safety risks (e.g., PII showing subject’s location), (iv) data is intended for decisionmaking significantly affecting a data subject, (v) repetitive transfers of mass volumes of data, and (vi) covert or clandestine practices to collect data (e.g., Internet browser cookies). It would be less likely that permission would be granted to transfer PII satisfying one or more of these factors.
\item See U.S. Department of Commerce Safe Harbor documents at \url{http://www.export.gov/safeharbor/}.
\item If carefully followed, the safe harbor should shield U.S. firms from EU legal action for privacy violations.
\item For example, the sectoral enforcement power might include the regulator bringing an enforcement action under federal or state law prohibiting unfair and deceptive acts.
\item 15 U.S.C. § 1681 et seq.
\item 12 U.S.C. §1813.
\item The Department of State is a traditional regulator in such areas of IA as national security, foreign policy, diplomacy and international development. See \url{http://www.state.gov/documents/organization/24299.pdf}.
\end{itemize}
\end{footnotesize}
operations and communications infrastructure,\textsuperscript{41} NIST regulations can ultimately impact the private sector through procurement (e.g., eCommerce) and the supporting financial services infrastructure. Indeed, NIST initiates emerging standards with broad potential in areas such as cryptography, network security, deployment of emerging technologies and general security management, more likely than not to become model standards.

\textbf{C. Non-Governmental and Self-Regulatory Organizations}

Much of the existing financial IS standards-setting work is non-governmental, largely promulgated by professional groups with a plurality of expertise in the subject areas. Several of these organizations and their processes are well-known to the financial services community. For example, the mission of the Financial Accounting Standards Board (FASB) is to “establish and improve standards of financial accounting and reporting for the guidance and education of the public, including issuers, auditors, and users of financial information.” FASB guidance takes many forms\textsuperscript{42} and generally underlies many of the generally accepted accounting principles (GAAP), a task generally delegated by the SEC to the authoritative accounting professional organizations. The American Institute of Certified Public Accountants (AICPA) licenses accounting professionals and its constituent groups set some GAAP standards as well as generally accepted auditing standards (GAAS). The securities exchanges and licensing organizations (e.g., National Association of Securities Dealers (NASD),\textsuperscript{43} state bar associations, state CPA societies\textsuperscript{44}) also have impact on financial IA through their discipline of licensed professionals.\textsuperscript{45}

Two other types of non-governmental organizations are also important in financial IA matters. First, the Sarbanes-Oxley Act (SOX), passed in the wake of the

\textsuperscript{41} The Computer Security Division (CSD) is one of eight divisions within NIST's Information Technology Laboratory that establish federal IA standards.

\textsuperscript{42} \textit{E.g.}, forms of FASB guidance include: FASB Pronouncements (i.e., Statements of Financial Accounting Standards, Statements of Financial Accounting Concepts, FASB Interpretations), Documents of the Emerging Issues Task Force (EITF) (EITF Consensus, EITF Issues), FASB Staff Positions (FSP), FASB Exposure Documents.

\textsuperscript{43} See \url{http://www.nasdr.com}.

\textsuperscript{44} \textit{See e.g.}, National Association of State Boards of Accountancy, \url{http://www.nasba.org}.

\textsuperscript{45} Numerous private and public-private organizations influence financial IA through their respective regulatory missions. For example, the Municipal Securities Rulemaking Board (MSRB) regulates broker/dealers, recordkeeping and customer account information in the markets for state, municipal and industrial-revenue bonds. See \url{http://www.msrb.org/}. 
Enron and WorldCom scandals, established a significant financial IA regime: it established the Public Companies Accounting Oversight Board (PCAOB) and it reinforces internal control in numerous ways. The PCAOB is a private-sector, non-profit corporation, with members appointed by the SEC, and a mission to replace the accounting industry’s previous self-regulation regime with the PCAOB’s oversight of “auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports.”⁴⁶ If further political difficulties are averted, the PCAOB is very likely to have a major impact on financial IA,⁴⁷ most directly for publicly-traded companies. The PCAOB financial IA influence will eventually go beyond publicly-traded issuers as its IA practices are imposed by publicly-traded firms on their non-public suppliers, customers, IT service providers, legal counsel and other consultants. As new financial IA standards applicable to publicly-traded companies emerge, these are likely to become practice of non-publics because the retain auditors, consultants and IT service providers accustomed to PCAOB financial IA standards.

A second non-governmental security regime is designed to quickly disseminate security-related vulnerabilities and responses applicable to critical infrastructures using Information Sharing and Analysis Centers (ISAC) keyed to particular industry sectors.⁴⁸ ISACs are government-industry partnerships with significant technical focus and expertise in various critical infrastructures, originally modeled on the Center for Disease Control and Prevention (CDC) for information sharing needs in healthcare. ISACs are intended to gather, analyze, and disseminate private sector information to both industry and government about information and physical security threats, vulnerabilities, incidents, and solutions. Several critical infrastructures directly impact the financial

⁴⁶ See http://www.pcaobus.org/default.asp.
⁴⁷ Many of the initial PCAOB rulemakings were stimulated by SOX and directly focus on financial IA matters, e.g., auditing standards, audit documentation, internal control, registration and discipline of the accounting profession, and GAAP/GAAS standards compliance. See generally, http://www.pcaobus.org/pcaob_rulemaking.asp.
services industry and financial IA in general. For example, ISACs have been established for the financial services industry, the telecommunications industry and the energy industry, all key infrastructures for banking and finance. An important incentive to private information submission of vulnerability or problem diagnosis information to ISACs is the self-evaluation privilege that promises the information will not (easily) become evidence in litigation or enforcement actions.

IV. Laws Applicable to Financial Information Assurance

There are numerous laws that govern financial IA and authorize the IA institutional framework discussed in the last section. This paper synthesizes statutes, caselaw and regulations directly applicable to financial IA with other laws not universally contemplated as clearly suitable for IA matters. Two major fields of law on security are examined here: (1) laws requiring data security practices for private information - personally identifiable information (PII), and (2) laws protecting trade secrets. Each area has a financial impact sometimes overlapping the others. The results of this comparison will become even more useful to financial IA as they are synthesized with traditional fields of accounting and administrative controls. The product would be useful in predicting the evolution of financial IA standards and in interpreting the impact of IA developments from analogous fields.

A. Regulating the Security of Individual Privacy

Although the need to protect confidentiality and secrecy of PII data is inherent in the concept of individual privacy, there is an emerging range of public policies that mandate this focus. A widely-recognized, contemporary origin for the IA framework of PII is the Fair Information Practice Principles (FIPP) first formulated by the U. S.

49 The Financial Services Information Sharing and Analysis Center is the ISAC for the financial services industry, [http://www.fsisac.com/](http://www.fsisac.com/)
50 The National Coordinating Center for Telecommunications is the ISAC for the Telecommunications industry, [http://www.ncs.gov/ncce/main.html](http://www.ncs.gov/ncce/main.html)
51 The Electricity Sector Information Sharing and Analysis Center is the ISAC for the electric utility and transmission industry, [http://www.esisac.com/](http://www.esisac.com/)
Department of Health, Education and Welfare in 1973.\textsuperscript{52} FIPP arguably underlies the primary approaches taken in many privacy laws and policies throughout the world.\textsuperscript{53} FIPP includes five “safeguard principles:”

\begin{enumerate}
\item Notice/Awareness\textsuperscript{54}
\item Choice/Consent\textsuperscript{55}
\item Access/Participation\textsuperscript{56}
\item Integrity/Security\textsuperscript{57}
\item Enforcement/Redress\textsuperscript{58}
\end{enumerate}

Each FIPP has impact on IA, four involve both the individual data subject and operators of the information system.\textsuperscript{59} For example, notice/awareness is needed to enable the subject individual’s choice, participation and redress - essential IA steps for the subject individual’s efforts and the subject individual has the clearest IA incentives to protect and defend. Choice/consent for the subject individual to be involved in PII data management triggers IA duties. Access/participation provides a monitoring incentive to the subject individual and broadens the opportunities for correction that sustain the accuracy of data. Enforcement/redress rights provide the subject individual with a retrospective IA incentive, legitimizing data practices as just. The IA obligations under the fourth principle, integrity/security, apply less to individual data subjects and more directly to operators of information systems.


\textsuperscript{54} Subject individuals should be given notice of an entity’s practices before any information is collected from them by identifying details about the data collection, security and uses.

\textsuperscript{55} Subject individual has choice on whether and how PII is collected. For example, consent might be manifest with an \textit{Opt-out} (an affirmative act preventing PII collection and/or use) or an \textit{Opt-in} (an affirmative act \textit{permitting} collection and/or use).

\textsuperscript{56} Subject individual can gain timely and inexpensive access to review PII about themselves. A simple and effective method should exist to contest and correct inaccurate data.

\textsuperscript{57} Collector takes reasonable steps to assure accuracy of PII as well as administrative and technical security measures to prevent unauthorized access or disclosure, destruction or misuse of PII.

\textsuperscript{58} Mechanism(s) exist to enforce privacy practices, including self-regulation, private rights of action and regulatory enforcement.

\textsuperscript{59} Information systems constitute “the entire infrastructure, organization, personnel, and components, for the collection, processing, storage, transmission, display, dissemination, and disposition of information.” NSTISSI 4009 (August, 1997).
1. The Privacy-Security Conundrum

Key to both privacy and security are their relationships between these concepts: some relationships are conflicting while other relationships are complementary. One line of reasoning holds that there are irreconcilable trade-offs between privacy and security. Under this conception, deploying effective public policies for each is impossible because they represent a zero-sum game: privacy gains diminish security while security gains come mainly at the expense of privacy losses. This conflict generally leads both camps, advocates of strong privacy rights and advocates of strong national security, to a similar set of public policy presumptions.\(^60\) The famed jurist, Learned Hand, developed a public policy balancing framework for the imposition of tort law duties.\(^61\) This framework is adapted by Judge Richard A. Posner to the limited privacy context of Fourth Amendment search and seizure,\(^62\) and is further adapted here to the privacy-security conundrum.\(^63\)

This model would dictate that privacy be protected or alternatively the model would dictate that security be enhanced depending on a balancing of: the usefulness to society of PII acquired from an intrusion against the repugnance of the intrusion. To adapt the Hand Formula to the privacy-security conundrum, assume the following:

\[
B = \text{intrusion costs} \\
P = \text{probability of discovering useful information} \\
L = \text{societal losses.}
\]

<table>
<thead>
<tr>
<th>Condition</th>
<th>Privacy vs. Security: The Impact on Legislation, Precedent or Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>B &gt; P * L</td>
<td>Privacy interests outweigh Security interests</td>
</tr>
<tr>
<td>B &lt; P * L</td>
<td>Security interests outweigh Privacy interests</td>
</tr>
</tbody>
</table>

The resulting relationship signals an optimal public policy balancing of privacy against security and/or security against privacy. Under the trade-off theory, a good society will "carefully balance individual rights and social responsibilities, autonomy and the

\(^{60}\) However, these presumptions typically lead these two camps to opposite public policy prescriptions.

\(^{61}\) See United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir.1947).


common good, privacy and...public safety.” Much of the public policy debate recognizes this as the fundamental trade-off that society addresses the privacy-security conundrum in such public policy decisions made in the post-9.11 efforts at counter-terrorism, cyber-security and critical infrastructure protections.

The privacy-security conundrum is based on several related propositions. First, the trade-off focuses on the externalities of strong privacy rights: privacy compromises security because intruders, terrorists enjoy increasing anonymity as privacy protections shield them from scrutiny. Second, the corollary is similar as the focus changes to conditions conducive to strong security: strong security requires limits on privacy rights because weak privacy better avails counter-terrorism forces of information potentially relevant to apprehending intruders or terrorists or circumventing their activities. Third, intrusion and attack are deterred by limited privacy because would-be intruders seeking to evade detection suspect that notoriety of their intentions or preparations would trigger counter-terrorism prevention. Fourth, security can be enhanced with limitations on the liberty of intruders and terrorists; weak privacy enhances the controls and disincentives that constrain their liberty.

2. The Privacy-Security Complement

The security-privacy conundrum is overly simplistic, it elevates law enforcement and institutional control above personal responsibility (and liberty) and it ignores the basic public policy underlying the function of IA to increase privacy as well as the security benefits of privacy. First, liberty can provide security such as when flight averts injury. Second, and related, is that the privacy concept of isolation is useful for the protection of prey, that is, self-imposed seclusion, and its related anonymity, can be an effective preemption to many threats. Third, applying isolation to PII, the benefits of privacy rights are diminished if PII is insecure because vulnerable physical and electronic collections of private data risk misuse. For example, insecure private and public databases have been used by predators to inform their stalking and identity theft.

---

activities - eventually prompting legislative, regulatory and judicial reaction. Finally, these propositions on complementarity are segue to the next section in which data security is essential to strong privacy, which in turn contributes greatly to individual security.

3. Security Component in Privacy Regulation

There is general recognition in the key financial privacy laws and regulations passed or promulgated in recent years that privacy rights are ineffective without an ongoing IA regime designed, evaluated and maintained to protect and defend PII and their supporting information systems. Modern financial assurance regulations can be traced to the Fair Credit Reporting Act (FCRA)\textsuperscript{67} as amended in Fair and Accurate Credit Transactions Act of 2003.\textsuperscript{68} The FCRA has IA rules that limit third party access to consumer credit reports for legitimate purposes, engages the subject individual with rights of access and redress, promote PII accuracy (e.g., revision/deletion of inaccurate or obsolete PII) and authorize both civil and criminal enforcement mechanisms.\textsuperscript{69}

The Gramm-Leach-Bliley Act of 1999\textsuperscript{70} (GLB) repealed the Glass-Steagall Act\textsuperscript{71} effectively eliminating the New Deal-era separations between the three major financial services sectors: commercial banking, investment banking and insurance. The inevitable consolidation of financial services signaled a consolidation of theretofore separate financial records into more conveniently useful databases, subsequently containing customers’ banking, brokerage and insurance PII. GLB required the major federal regulators of financial services to coordinate their promulgation of new privacy regulations that generally restrict the onward transfer of financial PII outside these affiliated firms, the initial and annual delivery of privacy notices, opt-out consent and IA data security measures.

---

\textsuperscript{67} 15 U.S.C. §1681 et seq.
\textsuperscript{69} FCRA enforcement is an incentive for financial PII security. Credit reporting agencies are subject to negligence liability for failure to install and maintain reasonable procedures to ensure accuracy reports.
The GLB security provisions most directly impacting financial PII establish legislative policy for every financial institution to have “an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.”72 This policy is initially implemented through sectoral financial regulators, each of which is directed to “establish appropriate standards … relating to administrative, technical, and physical safeguards to:

(1) to insure the security and confidentiality of customer records and information;
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.”73

During 2000, these “designated federal functional regulators”74 coordinated their G/L/B privacy rulemakings, resulting in cooperation and closely parallel G/L/B privacy rules.75 However, the detail and flexibility of the security rules varies widely, particularly when compared with HHS’s highly detailed healthcare privacy rules under HIPPA.76 A comprehensive and detailed comparison of G/L/B security rules is beyond the scope here. Nevertheless, a comparison of the SEC and FTC rules is instructive for financial IA given the move to multi-service financial firms (universal banking) precipitated by G/LB.

4. The SEC Security Rule

The SEC’s GLB privacy rule is Regulation S-P77 and this also contains the SEC privacy security rule,78 which is simple, straightforward and general, much more on the

---

74 See supra note 18.
75 See supra section III.A.
76 See supra text accompanying note 30.
78 17 C.F.R. §248.30. The complete text is as follows:

**Procedures to safeguard customer records and information.**

Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt policies and procedures that address administrative, technical, and physical
principles-based side of the standards continuum than is the HIPPA rule. It requires financial services firms under its authority to adopt policies and procedures that assure IA safeguards of customer records and information in three major areas: (1) administrative, (2) technical, and (3) physical. Firms must use evaluation techniques to achieve a “reasonable” design that insures security and confidentiality, protects against anticipated threats and hazards to the security or integrity of PII and protects against unauthorized access or use of PII if such could result in substantial harm or inconvenience to any customer.

The guidance provided in the SEC security rule is vague, principles-based and therefore allows considerable discretion on nearly every aspect of IA controls. A firm’s selection or development of particular controls, their implementation and monitoring and their evaluation are largely left to development by individual firms or as best practices safeguards for the protection of customer records and information. These policies and procedures must be reasonably designed to:

(a) Insure the security and confidentiality of customer records and information;
(b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
(c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The focus here is on financial IA of regulated entities under the SEC’s authority, not on the IA practices of the agencies themselves. However, increasingly and particularly since broader availability of the Electronic Data Gathering, Analysis and Retrieval (EDGAR) system in the 1990s, financial IA must also focus on the quality of the IT practices of government agencies (eGovernment). The SEC now also actively manages financial and eGovernment IA in recognition that the information it delivers has broad impact on markets, investors, regulated entities and beyond. Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility and Integrity of Information Disseminated by Federal Agencies; Notice; Republication, 67 Fed. Reg. 8452 (February 22, 2002). This SEC guidance was mandated by the Treasury and General Government Appropriations Act for Fiscal Year 2001, §515, Pub. Law 106-554; H.R. 5658. The Office of Management and Budget (OMB) requires federal agencies to: (i) publishing their own IA guidelines for ensuring and maximizing the quality of the information they disseminate and (ii) establish participation processes to facilitate the correction of information by persons affected if the agency is not in compliance with IA guidelines of OMB or the particular agency. All federal agencies subject to the Paperwork Reduction Act, 44 U.S.C. 3501 et seq., must publish data quality assurance guidelines on their websites.


This contrasts with some other, more detailed SEC security rules applicable in other contexts, see e.g., the SEC Data Security Rule for electronic customer records held by brokers and dealers, 17 CFR 240.17a-4. In 1997, the SEC amended paragraph (f) of Rule 17a-4 to enable broker-dealers to store records electronically (e.g., on optical disk or magnetic tape). That rule imposed significant requirements on IT details, e.g., media used to store records, storage, and indexing and retrieval of records.
from industry custom. It can be expected that some clarity and specificity may emerge as
enforcement actions or private litigation scrutinize (1) the particular policies adopted
pursuant to this rule, (2) the implementation of particular controls and (3) the
effectiveness of remediation response to intrusion incidents. An evaluation framework
and de facto standards may emerge, perhaps paralleling litigation over internal
accounting controls.\textsuperscript{81}

5. The FTC Security Rules

The FTC has taken a somewhat more detailed approach in its implementation of
the G/L/B security rules\textsuperscript{82} arguably anchored midway along the standards continuum
nearer to objectives-based standards.\textsuperscript{83} The FTC’s guidance is faithful to the G/L/B
security requirement\textsuperscript{84} yet is considerably more specific than the SEC security rule in
mandating an information security program, a risk assessment, the design and
implementation process for information safeguards and oversight of third party service
providers. In addition, the FTC security rule sets general, yet more detailed standards for
program evaluation than did the SEC.

The FTC’s basic requirement is for the initial development of a written
information security program\textsuperscript{85} and this is followed with a continuing duty of
execution through program implementation and maintenance.\textsuperscript{86} Several component
elements are required: coordination, risk assessment and deployment of information
safeguards. First, coordination responsibility for the information security program must
lie with a designated employee or employees.\textsuperscript{87} Second, a risk assessment must be
conducted to “identify reasonably foreseeable internal and external risks to the security,

\textsuperscript{81} See e.g., \textit{Ernst & Ernst v. Hochfelder}, 425 U.S. 185, 192, 193 n.10 (1976); \textit{SEC v. World-Wide Coin
v. Sporek}, 612 F.Supp. 1316 (N.D.Cal,1985); \textit{Monroe v. Hughes}, 31 F.3d 772 (9\textsuperscript{th} Cir.1994); and \textit{In re Ikon
Office Solutions, Inc}. 277 F.3d 658, 672 (3d Cir.2002).
\textsuperscript{83} See generally SEC-SOX Standards Study.
\textsuperscript{84} 16 C.F.R. §314.3 (b).
\textsuperscript{85} Information security program means the administrative, technical, or physical safeguards you use to
access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer
information, 16 C.F.R. §314.2 (c).
\textsuperscript{86} 16 C.F.R. §314.3 (a).
\textsuperscript{87} 16 C.F.R. §314.4 (a).
confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.” The risk assessment must focus on each relevant area of operations, including at a minimum, employee training and management, information systems, (e.g., network and software design, information processing, storage, transmission, disposal), and the development of appropriate safeguards - detection, preventing and responding to attacks, intrusions, or other systems failures.

Third, the results of the risk assessment are needed to inform a design and implementation process that deploys the information safeguards. Fourth, each regulated entity must exercise oversight of service provider (generally third parties) that may handle or supply software and hardware that processes customer PII. There are at least two aspects to third party oversight including reasonable selection and retention of competent service providers and further delegation of the safeguards obligations for implementation and maintenance, imposed under the service contract(s).

The FTC security rule envisions both an initial and recurring evaluation of the information security program. An initial and (likely) most comprehensive evaluation is needed in the conduct of the risk assessment. The evaluation rigor is measured against the regulated entity’s “size and complexity, the nature and scope of [its’] activities, and the sensitivity of any customer information at issue.” Evaluation must be conducted “in light of the results of the [risk assessment’s] testing and monitoring” and must inform the design and implementation of information safeguards that control the risks identified.

---

88 Customer information means any record containing nonpublic personal information as defined in [the FTC privacy rule], about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates, 16 C.F.R. §314.2(b).
89 16 C.F.R. §314.4 (b).
90 16 C.F.R. §314.4 (b)(1).
91 16 C.F.R. §314.4 (b)(2).
92 16 C.F.R. §314.4 (b)(3).
93 16 C.F.R. §314.4 (c).
94 Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part, 16 C.F.R. §314.2(d).
95 16 C.F.R. §314.4 (d).
96 16 C.F.R. §314.4 (d) (1).
97 16 C.F.R. §314.4 (d) (2).
98 16 C.F.R. §314.3 (a).
99 16 C.F.R. §314.4 (e).
Thereafter, and on an arguably regular basis, the effectiveness of the information safeguards’ key controls, systems, and procedures must be monitored and tested.\textsuperscript{100} Furthermore, additional evaluation may become necessary in light of the results of the testing and monitoring, to “any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.”\textsuperscript{101} In addition to the considerable detail in the FTC’s security rule, plain language guidance has been made available to sensitize regulated entities to other security resources throughout the public and private sectors.\textsuperscript{102}

\textbf{B. Analogies from Trade Secret Law}

Legal requirements for private sector IA are clearly not limited to the PII of customers or employees. IA activities are also derived from laws developed to protect critical infrastructures\textsuperscript{103} as well as confidential, proprietary information that can qualify as intellectual property (IP) under the rubric of traditional trade secret protections.\textsuperscript{104} The subject matter of trade secrets includes financial information. Trade secret law\textsuperscript{105} is unlike the federal schemes for copyrights, trademarks and patents.\textsuperscript{106} Trade secret law is

\begin{footnotesize}
\begin{enumerate}
\item[100] 16 C.F.R. §314.4 (c).
\item[101] 16 C.F.R. §314.4 (e).
\item[103] See supra notes 48 to 51.
\item[104] Trade secret law dates back to at least Roman law recognizing the wrongful corruption of another citizen’s slave: \textit{action servi corrupti}. Outsiders maliciously enticing another’s slave to divulge business secrets were liable to the owner in money damages. See Schiller, \textit{Trade Secrets and the Roman Law: The Actio Servi Corrupti}, 30 Colum.L.Rev. (1930).
\item[105] Forty-four states have adopted the Uniform Trade Secrets Act (UTSA). The original version of the UTSA was published in 1979 by the National Conference of Commissioners for Uniform State Laws (NCCUSL). Thirty-eight states have adopted the 1985 UTSA revision, \url{http://www.law.upenn.edu/bll/ulc/fnact99/1980s/utsa85.pdf} Trade secret law in the U.S. is traced to §757 of the 1939 Restatement of Torts (American Law Institute (ALI)), a syntheses of the common law to provide uniformity and predictability produced by judges, academics and prominent lawyers.
\item[106] See e.g., Kewanee Oil Co. \textit{v}. Bicron Corp., 416 U.S. 470 (1974) (holding patent and trade secret law are compatible, despite similarities in the subject matter: patents are strong property rights that require public disclosure of the invention while trade secrets require secrecy; owners and inventors may freely choose between these two schemes).
\end{enumerate}
\end{footnotesize}
rooted in confidentiality duties, implied from fiduciary principles, but now more typically expressed in employment contracts that impose IA or as criminal law.\footnote{Trade secret law can also be based on state criminal laws outlawing theft or possession of stolen computer information and prohibitions against the unlawful use of secret scientific material. The most significant criminal law is the federal Economic Espionage Act of 1996 (EEA), 18 U.S.C. §1831.} 

Trade secrets include confidential information with commercial value or that bestows commercial advantage— the owner derives independent economic value, actual or potential, from the information not being generally known. Under the UTSA, a trade secret can be:

“Information, including a formula, pattern, compilation, program device, method, technique or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”\footnote{UTSA §1(4).}

In the financial IA context it is important that trade secrets may exist in software or be available off servers accessed from the Internet and clearly include customer lists.\footnote{See e.g., Ed Nowogroski Ins. V. Rucker, 971 P.2d 936 (Wa.1999).}

\section{1. Implications of Trade Secrecy on IA}

Maintaining the economic benefits of trade secret ownership largely depends on IA. Confidentiality must be exercised over all persons exposed to the secrets. In addition, there are other types of control—physical, administrative and contractual—that must be exercised. Secrecy is the critical element— the owner must undertake reasonable measures to preserve the secrecy. Absolute privacy is not needed because the cost burden would too often overwhelm the secret’s economic value. Instead, an ad hoc, case-by-case analysis of the circumstances is made to determine whether the owner has “taken all proper and reasonable steps…considering the nature of the information sought to be protected as well as the conduct of the parties.”\footnote{USM Corp. v. Marson Fastner Corp., 393 N.E.2d 895 (Mass.1979).} Unfortunately secrecy is defined
negatively- when secrecy is lacking. For example, the Restatement denies trade secrecy to “matters of public knowledge or of general knowledge in an industry.” Secrecy can be lost even if the general public does not know the secret a competitor’s knowledge may be enough.¹¹¹

Relevant factors¹¹² in secrecy include the general knowledge of security in the industry and the offensiveness of the misappropriator’s conduct. Effective secrecy programs should examine past trade secret practices in the industry, conduct periodic IP audits,¹¹³ develop misappropriation scenarios and design protocols to avoid loss. Firms with substantial or key trade secret assets must develop and continually update their security protection programs.¹¹⁴ Deliberate evaluation of secrecy protections can employ various methodologies of risk-benefit analysis. Generally, the cost of each security control measure is balanced against the financial risk of the secret’s loss. Adjustments are usually needed to account for the probability that particular combinations of controls can prevent or impede misappropriation resulting in the net benefits.

2. Information-Centered Controls

An initial inquiry should focus on the information itself. Sensitive information is identified, employees and outsiders with access listed, need to know procedures established for future access, warning labels installed, logging of sensitive documents, files and facilities implemented, lock-out techniques deployed (e.g., vaults, restricted areas, computer/network passwords), data encrypted, document retention/destruction policies enforced, photocopying controlled, data segregated if more valuable when integrated, alarms installed, and video surveillance and electronic monitoring devices used. Network security techniques such as changing passwords, firewalls, hacker prevention and Internet-use policies are part of successful firm’s best practices. Logs should be kept showing when network information was accessed, downloaded, printed or saved and by who (IP address).

¹¹¹ UTSA §1 comment.
¹¹² The following discussion of secrecy under trade secret law is derived from
¹¹³ The audit team needs expertise in several areas, including: IP law, technical expertise in the invention field, computer security and business decisions (e.g., IT, MIS, finance and accounting).
¹¹⁴ Such programs are familiar to law enforcement, management accountants, auditors, security professionals and national security experts. See e.g., Epstein, M. and S. Levi, Protecting Trade Secret Information: Plan for Proactive Strategy, 43 Bus.Law. 887 (May 1988).
3. Employee-Centered Controls

To be effective, some aspects of trade secrets must be shared with employees, either because they invent/develop them or must implement them in the firm’s activities. Employee-centered controls strengthen confidentiality duties and control their misuse. Employee agreements often restrict the employee to confidentiality in using non-disclosure agreements (NDA), non-compete clauses (non-competes) or equitable remedies,¹¹⁵ bans on soliciting clients, customers and co-workers, they require sign-in to employer premises after hours, require strict use of identification cards while on site, employ special access codes for sensitive areas and reinforce secrecy with work rules prohibiting misappropriation and personal misuse of personal misuse of employer trade secrets. Many employers clearly inform their employees that phone records are retained, e-mail using the firm’s computers or networks belongs to the employer and workplace surveillance must be expected. Exit interviews and post-termination reminders can encourage compliance and permit graceful return of the employer’s documents, computers and files.

4. Outsider-Centered Controls

Outsiders must also be exposed to at least some trade secrets on occasion. Visitors, service and maintenance personnel, consultants or customers may respond to emergencies, use specifications and new product plans, provide expertise, assist in making strategies, develop products or production processes, but best only on a “need to know basis.” Best practices suggest NDAs, confidentiality for software containing trade secrets, prohibitions on de-compiling and reverse engineering. The professional duties of many consultants, accountants and lawyers prohibit disclosure of client confidences even without NDAs.

5. Misappropriation

Acquisition of trade secrets using improper means includes actions such as “theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy,

or espionage through electronic or other means.\textsuperscript{116} These are probably the most severe forms of trade secret misappropriation because they involve actions often unlawful under the criminal law. Figure 2 depicts the chain of misappropriation and depicts the four generally acts of misappropriation.

\textbf{Figure 2: Chain of Unlawful Forms of Misappropriation}

\begin{itemize}
  \item \textbf{Acquisition} by improper means: theft, bribery, espionage, breach of confidence, or misrepresentation
  \item \textbf{Disclosure} after improper means of acquisition, knowledge of misappropriation or breach of confidence
  \item \textbf{Receipt} after knowing disclosure made by source using improper means or in breach of confidence
  \item \textbf{Use} after improper means of acquisition, knowledge of misappropriation or breach of confidence
\end{itemize}

\textbf{V. Observations}

This research will assist in defining the field of public policy influences on IA in general, on the law and regulation relevant to privacy and security in particular. Many fields are working toward similar security goals and using similar means to achieve their IA goals. This strongly suggests more interdisciplinary approaches to financial IA practice and education. This similarity also suggests that research from other IA areas can be useful to guide the composition of research questions and the methodologies employed. For example, it would appear that current best practices and research findings in internal control for financial assets and liabilities is a rich source for analogy to other financial IA efforts mandated under privacy law, critical financial infrastructure protection requirements and financial market transparency.

\textsuperscript{116} UTSA §1(1).