CHAPTER 1

Information Technology

Chapter Contents

"Information security" is a term used to describe the technological and procedural measures[1] organizations take to protect data from unauthorized access,[2] use,[3] disclosure,[4] disruption,[5] modification[6] or destruction.[7] Information security is necessary to control digital assets and ensure:

(1) *Integrity:* protection against improper information modification or destruction, which prevents data repudiation[8] and ensures authenticity;[9]

---

[1] See Ch. 3 *infra* for a discussion of the policies and procedures organizations must implement to secure computer systems.

[2] See: § 9.01[2] *infra* for a discussion of liability for unauthorized access to protected computers under the Computer Fraud and Abuse Act (CFAA) pursuant to 18 U.S.C. § 1030(a)(1)-(a)(5) and a discussion of the definition of "exceeds authorized access" under the CFAA pursuant to 18 U.S.C. § 1030(a)(1)-(e)(6); § 11.01[3] *infra* for a discussion of the Digital Millennium Copyright Act (DMCA) (17 U.S.C. §§ 1201 *et seq.*) and how "access" has become a focal point in statutes addressing digital works and computer systems; § 10.03[1] *infra* for a discussion of unauthorized access under the Stored Communications Act pursuant to 18 U.S.C. § 2701(a); § 5.06 *infra* for a discussion of the Gramm-Leach-Bliley Act Safeguards Rule and financial institution duties to prevent unauthorized access pursuant to 15 U.S.C. § 6801(b)(3); § 7.02[4] *infra* for a discussion of the definition of "access" under the Health Insurance Portability and Accountability Act (HIPAA) pursuant to 45 C.F.R. § 164.304 (July 22, 2004); § 9.05[5][o] *infra* for a discussion of the FTC's implementation of the Fair and Accurate Credit Transactions Act's (FACTA's) provisions that relate to financial institution's disposal of consumer information pursuant to 16 C.F.R. § 682.3(a); § 8.07[1] *infra* for a discussion of government agency responsibility to prevent unauthorized access to government systems under the Federal Information Security Management Act (FISMA) pursuant to Pub. L. No. 107-347, 116 Stat. 2899, 2946-2948 § 301(b)(1) (Dec. 17, 2002).

[3] See § 3.04 *infra* for a discussion of the contractual provisions organizations create to establish "authorized use."

[4] See § 7.02[4] *infra* for a discussion of HIPAA's health data security standards pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [c]onfidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes").

[5] See: § 3.01 *infra* for a discussion of the importance of continuity plans in the event of a network breach; § 8.07[2][a] *infra* for a discussion of FISMA's information security program requirements pursuant to Pub. L. No. 107-347, 116 Stat. 2899, 2946-2951 § 301(b)(1) (Dec. 17, 2002) (codified in 44 U.S.C. § 3544); § 7.03[2][a] *infra* for a discussion of HIPAA's security safeguards requirements pursuant to 45 C.F.R. § 164.308(a)(7)(i) (July 22, 2004) .

[6] See: § 7.02[4] *infra* for a discussion of HIPAA's security safeguards requirements pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [i]ntegrity means the property that data or information have not been altered or destroyed in an unauthorized manner"); § 2.04[2] *infra* for a discussion of the importance of financial record accuracy under the Sarbanes-Oxley Act pursuant to Pub. L. No. 107-204, § 1, 116 Stat. 745 (2002) (codified in 15 U.S.C. § 7202) (stating that the Sarbanes-Oxley Act is "[a]n Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes").

[7] See: § 3.06 *infra* for a discussion of those policies that an organization must adopt to address retention and destruction of data and documents; § 3.01 *infra* for a discussion of organizations' duty to address disaster recovery.

[8] For example, non-repudiation ensures data integrity and prevents network users from denying authorship of a given communication. See *Black's Law Dictionary* (5th ed. 2003) (defining "repudiate" as "[t]o put away, reject, disclaim, or renounce a right, duty, obligation, or privilege").

[9] See: § 8.01 *infra* for a discussion of the definition of "integrity" under the E-Government Act pursuant to Pub. L. No. 107-347, 116 Stat. 2899, 2946-2947, § 301(b)(1) (Dec. 17, 2002) (codified in 44 U.S.C. § 101 note) (stating that "[c]hapter 35 of title 44, United States Code, is

(2) *Confidentiality:* preservation of authorized restrictions on access and disclosure, which protects personal privacy and proprietary rights to information;[10] and

(3) *Availability:* timely and reliable access to and use of information.[11]

Organizations are increasingly dependent upon interconnected computer systems to facilitate business operations and manage important information. Moreover, the global computer system known as the "Internet" is recognized as a strategic national asset and a national security priority.[12] Various groups threaten these systems by exploiting the weaknesses intrinsic to information technology. The extent of security measures organizations take to prevent such threats is governed by the value assigned to data residing within a network, regulation of specific data classes, risk of loss of such assets, and the

---

amended by adding at the end the following new subchapter . . . Sec. 3542. Definitions. (a) In General. Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter. (b) Additional Definitions. As used in this subchapter: (1) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity . . ."); § 7.02[4] *infra* for a discussion of HIPAA's security standards pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [s]ecurity or Security measures encompass all of the administrative, physical, and technical safeguards in an information system." and ". . . [i]ntegrity means the property that data or information have not been altered or destroyed in an unauthorized manner."). Also see: § 3.06 *infra* for a discussion of those policies an organization must adopt to address retention and destruction of data and documents; § 4.02[4] *infra* for a discussion of the Fair Information Practice Principle's (FIPP's) integrity principle; § 2.04[2] *infra* for a discussion of the Sarbanes-Oxley Act's (SOX's) corporate responsibility provisions that relate to financial report certification pursuant to Pub. L. No. 107-204, § 1, 116 Stat. 745 (2002) (codified in 15 U.S.C. § 7202) (stating that the Sarbanes-Oxley Act is "[a]n Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes").

[10] See § 8.01 *infra* for a discussion of the definition of "confidentiality" under the E-Government Act pursuant to Pub. L. No. 107-347, 116 Stat. 2899, 2946-2947, § 301(b)(1) (Dec. 17, 2002) (codified in 44 U.S.C. § 101 note) (stating that "[c]hapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter . . . Sec. 3542. Definitions. (a) In General. Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter. (b) Additional Definitions. As used in this subchapter: (1) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide . . . (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. . . .").

[11] See, e.g., § 8.01 *infra* for a discussion of the definition of "availability" under the E-Government Act pursuant to Pub. L. No. 107-347, 116 Stat. 2899, 2946-2947, § 301(b)(1) (Dec. 17, 2002) (codified in 44 U.S.C. § 101 note) (stating that "[c]hapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter . . . Sec. 3542. Definitions. (a) In General. Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter. (b) Additional Definitions. As used in this subchapter: (1) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide . . . (C) availability, which means ensuring timely and reliable access to and use of information.").

[12] National Security Strategy (Dec. 2010), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (last visited April 14, 2011).

potential costs associated with remedying a network breach.[13] As a general matter, more valuable data and more costly remedial measures will require greater levels of protection.[14] Proper information security measures, therefore, constitute "best practices" for businesses that rely on networked computer systems[15] and are mandatory for certain organizations that collect, disseminate and use "sensitive" classes of data.[16]

---

[13] It should be borne in mind that security breaches result in both direct costs (e.g., lost productivity and overtime pay for remedial measures) and indirect costs (e.g., loss of customer confidence, lost sales and legal liabilities). Many groups have attempted to quantify these damages in order to determine an appropriate amount of technology spending. See, e.g.: CSI/FBI Computer Crime and Security Survey, Computer Security Institute (2005) (finding that total financial losses from computer attacks have declined dramatically in 2005), available at http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf (last visited April 12, 2006); § 5.06[1][c] *infra* for a discussion of the Gramm-Leach-Bliley Act's (GLBA's) FTC Safeguards Rule's flexible standards pursuant to 67 Fed. Regs. 36484, 36488 (stating that "[t]his standard is highly flexible, consistent with the comments, the Banking Agency Guidelines, and the Advisory Committee's Report, which concluded that a business should develop 'a program that has a continuous life cycle designed to meet the needs of a particular organization or industry'").

[14] See, e.g.: § 5.06[1][c] *infra* for a discussion of the GLBA's FTC Safeguards Rule pursuant to 67 Fed. Regs. 36484, 36489 (stating that "[t]he Commission notes the importance of providing guidance to financial institutions, particularly small businesses, on how to comply with this and other aspects of the Rule. The Commission therefore intends to issue educational materials to help businesses identify risks and comply with the various other provisions of the Rule. Because of the ever-changing nature of the relevant risks, however, the Commission does not find it appropriate to delineate risks more specifically within the Rule. In addition, to retain appropriate flexibility, the Commission will rely on its discretion in enforcing the Rule, and not describe any particular schedule or methods for enforcement."); § 7.02[4] *infra* for a discussion of HIPAA's security standards pursuant to 45 C.F.R. § 164.306(b)(2)(iv) (July 22, 2004) (stating that "[i]n deciding which security measures to use, a covered entity must take into account the following factors . . . [t]he probability and criticality of potential risks to electronic protected health information."); § 7.03[2][a] *infra* for a discussion of: 45 C.F.R. § 164.308(a)(1)(i) (July 22, 2004) (stating that "[a] covered entity must, in accordance with § 164.306 . . . Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations."); and 45 C.F.R. § 164.308(a)(1)(ii)(A) (July 22, 2004) (stating that "Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."); § 8.07[2][a] *infra* for a discussion of FISMA's federal agency information security program requirements pursuant to Pub. L. No. 107-347, 116 Stat. 2899, 2946-2949, § 301(b)(1) (Dec. 17, 2002) (codified in 44 U.S.C. § 3544) (stating that "[c]hapter 35 of title 44, United States Code, is amended by adding at the end the following . . . 'Sec. 3544. Federal agency responsibilities. . . . (b) Agency Program. Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source that includes (1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. . . .'").

[15] "Best Practices" are techniques or methods that have proven to lead reliably to a desired result. This term is frequently used in fields such as health care, government administration, project management, and software development. For example, a best practice in software development is a well-defined method that contributes to successful product development (e.g., iterative development processes, requirements management, quality control, and change control). In the context of information security, however, best practices are still evolving and require a commitment to the implementation of both legal and technical measures that ensure control over

§ 1.01 Networks

A "network" may be defined as an intricately connected system of things or people. The concept of a network has been applied in many contexts, such as the social contacts a person makes to further his or her career (e.g., "vocational networking"), the nervous systems of living creatures (e.g., "neural networks"), and the structural arrangements used in information technology (e.g., "networked computing").[17] Regardless of its function, a network is said to follow certain "laws" that are intrinsic to its structure and composition. For instance, a network's efficiency and resilience from disruption will be dependent on its architecture, which can be divided into at least three types or topologies:

(1) *Chain:* The chain or line network, where data move along a line of separated contacts, and where end-to-end communication must travel through intermediate nodes.

(2) *Hub:* The hub, star, or wheel network, where a set of data points is tied to a central (but not hierarchical) node, and the points must go through that central node to communicate and coordinate with one another.

(3) *Full Matrix:* The all-channel or full-matrix network, in which every node is connected to every other node.[18]

---

proprietary information. See, e.g.: § 8.01 *infra* for a discussion of the E-Government Act's purpose as stated in Pub. L. No. 107-347, 116 Stat. 2899, 2900-2901 § 2(b)(10) (Dec. 17, 2002) (codified in 44 U.S.C. § 3601 note) (stating that "[t]he purposes of this Act are the following . . . [t]o transform agency operations by utilizing, where appropriate, best practices from public and private sector organizations . . ."); GAO, Information Security Management: Learning from Leading Organizations, GAO/AIMD-98-68 (Washington, D.C. May 1998), available at http://www.gao.gov/archive/1998/ai98068.pdf (last visited April 14, 2006).

[16] See: § 1.02[3] *infra* for a discussion of the different laws that apply to: (1) consumer data, (2) financial data, (3) credit data, (4) health data, and (5) government data; Chs. 4-8 *infra* for a discussion of the various laws that protect the privacy of such data; § 5.06[1][c] *infra* for a discussion of the GLBA's FTC Safeguard Rule's information security program requirements pursuant to 67 Fed. Regs. 36484, 36488 at n.46 (May 23, 2002) (stating that "[t]he adaptability of the standard according to 'the sensitivity of information' mirrors the Advisory Committee's finding that 'different types of data warrant different levels of protection'").

[17] In the context of information technology, computer networks facilitate communications via the transfer of data along various configurations of connection points within a system called "nodes." A computer network, therefore, is a series of points or nodes interconnected by communications paths.

[18] See Arquilla and Ronfeldt, Networks and Netwars: the Future of Terror, Crime, and Military, pp. 7-8 (2001) (displaying graphical representations of these networks), available at http://www.rand.org/publications/MR/MR1382/MR1382.ch1.pdf (last visited April 14, 2006). See, e.g., § 11.01[2][g][v][B] *infra* for a discussion of decentralized peer-to-peer file-sharing networks' effects on intellectual property holders' rights, where each network user maintains an index of only those files that the user wishes to make available to other network users. Under this model, the software broadcasts a search request to all the computers on the network and a search of the individual index files is conducted, with the collective results routed back to the requesting computer. For a more in-depth description of P2P networks, see, e.g.: Feder, "Is Betamax Obsolete?: *Sony Corp. of America v. Universal City Studios, Inc.* in the Age of Napster," 37 Creighton L. Rev. 859, 862-868 (2004); Benkler, "Coase's Penguin, or, Linux and The Nature of the Firm," 112 Yale L.J. 369, 396-400 (2002).

[1]—Cyberspace

Many computer networks are interconnected through what has come to be called the "Internet" or "cyberspace."[19] In essence, "cyberspace" is an international network of private and public computer systems[20] that use various protocols to exchange data.[21] In terms of topology, cyberspace is currently

---

[19] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.

The "Internet" is defined in a variety of statutory texts. For instance, the Communications Act of 1934 defines the Internet twice. One definition was from the Communications Decency Act (passed as a part of the Telecommunications Act of 1996) and the other from the Children's Online Protection Act. The two definitions, though right next to each other, are not the same. 47 U.S.C. § 230(f)(1) states that "[t]he term 'Internet' means the international computer network of both Federal and non-Federal interoperable packet switched data networks." 47 U.S.C. § 231(e)(3), on the other hand, states that "[t]he term 'Internet' means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit the information." See § 4.03 *infra* for a discussion of the definition of "Internet" under the Children's Online Privacy Protection Act (COPPA) pursuant to 15 U.S.C. § 6501 (stating that "[i]n this chapter . . . [t]he term 'Internet' means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio"). See § 12.01[1][i] *infra* for a discussion of the Department of Defense's (DOD's) Defense Advanced Research Projects Agency (DARPA) Internet Project that resulted in the computer network that eventually grew into what is now referred to as "cyberspace."

[20] See, e.g., § 9.01[1] *infra* for a discussion of the Computer Fraud and Abuse Act's definition of "protected computer" pursuant to 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as one "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States").

[21] On the Internet, two primary protocols exist: (1) Transmission Control Protocol (TCP), which uses a set of rules to exchange messages with other Internet points at the information packet level (Internet Protocol (IP), on the other hand, uses a set of rules to send and receive messages at the Internet address level. Additional protocols that are usually packaged with a TCP/IP suite, including the Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP), each with defined sets of rules to use with corresponding programs elsewhere on the Internet); and (2) Internet Protocol (IP), which is the method by which data are sent from one computer to another on the Internet. Each computer on the Internet (known as a "host") has at least one IP address that uniquely identifies it from all other computers on the Internet. When data are sent or received over the Internet, the message gets divided into little chunks called "packets." Each of these packets contains both the sender's IP address and the receiver's IP address. See § 10.04[3] *infra* for a discussion of court orders to install monitoring devices pursuant to the Pen Register and Trap and Trace Devices Act under 18 U.S.C. § 3122. The Pen/Trap statute permits law enforcement to obtain the addressing information of Internet e-mails (with the exception of the subject line, which can contain content) using a court order, in the same manner that court orders permit government agents to obtain addressing information for phone calls and individual Internet "packets" using a court order. Conversely, the interception of e-mail contents, including the subject line, requires careful compliance with Title III. See § 12.01[1][i] *infra* for a discussion of the Department of Defense's (DOD's) role in securing Internet Protocol version 6 (IPv6).

the largest existing full-matrix network—every computer that transfers information is effectively connected to every other computer.[22] The protection of cyberspace, while safeguarding privacy and civil liberties, is recognized as a national security priority and an economic necessity.[23] Organizations must be mindful of the security issues that arise when connecting networks to cyberspace. This will be especially important for establishing best practices[24] and implementing security policies.[25] In order to avoid liability when protecting their networks and software, technicians should have some grasp of the legal theories pertaining to information security.[26]

[2]—National Infrastructure

The national infrastructure is composed of "critical systems" that facilitate the core functions of modern society.[27] Without a secure national infrastructure, telecommunications, power, transportation, banking, water supply, and emergency services would cease to operate. These systems share one common element: each is dependent on computer networks to organize, coordinate, and execute functions. Each system, therefore, is susceptible to the weaknesses intrinsic in the architecture of computer networks.[28]

The Critical Infrastructure Information Act of 2002 (CIIA), subtitle B of Title II of the Homeland Security Act,[29] regulates the use and disclosure of information submitted to the Department of Homeland Security (DHS) about vulnerabilities and threats to critical infrastructure. The CIIA was enacted, in part, to respond to the need for the federal government and operators of the nation's critical infrastructures to share information on vulnerabilities and threats, and to promote information sharing between the private and public

---

[22] Cyberspace presents unique issues that apply specifically to *computer* networks. For instance, the value of cyberspace as both a communications and commercial medium increases proportionately with the storage capacity of individual nodes (i.e., computers) and the number of interconnections between such nodes. These technological principals become increasingly significant as systems become more dependent on the pervasive, full-matrix network of powerful computing machines called "cyberspace."

[23] See National Strategy for Trusted Identities in Cyberspace (April 2011), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (last visited July 20, 2011).

[24] See N. 15 *supra*.

[25] See § 3.01 *infra* for a discussion of the policies that facilitate information security.

[26] See, e.g.: Ch. 9 *infra* for a discussion of various network activities that may lead to criminal liability; § 10.02[2][c][i] *infra* for a discussion exceptions to the Wiretap Act pursuant to 18 U.S.C. § 2511(2)(a)(i); § 9.03[4] *infra* for a discussion of official immunity.

[27] See § 1.04[7] *infra* for a discussion of the Comprehensive National Cybersecurity Initiative (CNCI) and national cybersecurity policy.

[28] See § 1.03 *infra* for a discussion of the various methods used to breach computer networks. See § 9.01[2][c] *infra* for a discussion of liability under the CFAA for unauthorized computer access pursuant to 18 U.S.C. § 1030(a)(5)(B)(v) (imposing liability for unauthorized access to a computer resulting in "damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security").

[29] Pub. L. No. 107-296, 116 Stat. 2135, §§ 211-215 (Nov. 25, 2002) (codified in 6 U.S.C. §§ 131-134).

sectors in order to protect critical assets. Courts continue to balance the government's need to protect sensitive infrastructure data with the public's right to access this information. For instance, it has been determined that the CIIA will shield infrastructure information received *by* local governments from the DHS, but not information that local governments provide to the DHS.[30] Protections for key resources that support critical infrastructure will become increasingly important as public-private partnerships emerge to secure these assets.[31]

Smart Grid technologies are an example of the national infrastructures that require extensive cyber security analysis and built-in privacy protections. Smart grids will introduce millions of new intelligent components to the electric grid that communicate in much more advanced ways than in the past. The Smart Grid Interoperability Panel Cyber Security Working Group (SGIP-CSWG) is led by the National Institute of Standards and Technology (NIST)[32] and has more than 350 participants from the private sector. The group is addressing cyber security via a process that will result in a comprehensive set of cyber security requirements using a high-level risk assessment process that is defined in the cyber security strategy for the Smart Grid.[33] Cyber security requirements are discussed in the NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (NIST Special Publication 1108).[34]

[3]—Network "Laws"

The proliferation and increased power of information technology, as well as the increased importance of information security, can be ascribed to certain technological "laws" that computer systems follow. For instance, computer networks follow rules intrinsic to their architecture. Moreover, these rules affect government's attempt to regulate such technology.[35]

[a]—Moore's Law

Gordon Moore, co-founder of Intel Corporation, has been credited with the observation that the amount of information that a microchip can store

---

[30] See, e.g., County of Santa Clara v. Superior Court of Santa Clara County, 70 Cal. App.4th 1301 (Cal. App. 2009) (holding that a California county's electronic geographic information map must be disclosed to a public interest group despite the county's objection that releasing the map would reveal sensitive infrastructure data).

[31] See: § 9.03[4] *supra* for a discussion of official immunity; Murray v. Northrop Grumman Information Technology, 444 F.3d 169, 174 (2d Cir. 2006) (granting absolute immunity to a government contractor from suit for state tort actions arising from sharing of information with federal agencies and dismissing appellants' claims of negligent misrepresentation and defamation).

[32] See http://www.nist.gov/smartgrid/ (last visited April 27, 2010).

[33] See Smart Grid Cyber Security Strategy and Requirements, available at http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628_2nd-public-draft.pdf (last visited April 27, 2010).

[34] See NIST Framework and Roadmap for Smart Grid Interoperability Standards, available at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf (last visited April 27, 2010).

[35] See Ch. 12 *infra* for a discussion of the various government and industry bodies that attempt to regulate information security.

doubles approximately every eighteen months. It should be noted, however, that researchers have predicted that "Moore's Law" will cease to be viable around 2025.[36] From a practical standpoint, information security and the privacy issues that arise in connection with a network breach[37] become increasingly important as vast amounts of data reside in isolated locations.[38] For

---

[36] See Zhirnov, Cavin III, Hutchby, and Bourianoff, "Limits to Binary Logic Switch Scaling—A Gedanken Model," Intel (Nov. 2003), available at http://www.intel.com/research/documents/Bourianoff-Proc-IEEE-Limits.pdf (last visited April 12, 2006).

[37] See, e.g.: § 5.06[3][b] *infra* for a discussion of the GLBA Bank Safeguard Rule's discussion of identity theft pursuant to Response Guidance § II (stating that "[m]illions of Americans, throughout the country, have been victims of identity theft. Identity thieves misuse personal information they obtain from a number of sources, including financial institutions, to perpetrate identity theft. Therefore, financial institutions should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information."); Federal Trade Commission, Identity Theft Survey Report (Sept. 2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited May 25, 2006) (estimating that nearly 10 million Americans discovered they were victims of some form of identity theft in 2002); § 9.05 *infra* for a discussion of the various laws that apply to identity theft; § 9.05[5] *infra* for a discussion of the definition of "identity theft" under the Fair and Accurate Credit Transactions Act (FACTA) pursuant to Pub. L. No. 108-159, 117 Stat. 1952, § 318(b) (stating that "Section 603 of the Fair Credit Reporting Act (15 U.S.C. § 1681a) is amended by adding at the end the following: '(q) Definitions Relating to Fraud Alerts. . . . (3) Identity theft. The term 'identity theft' means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation. . . .'"); and 16 C.F.R. § 603.2 (Dec. 1, 2004) (stating that "(a) The term 'identity theft' means a fraud committed or attempted using the identifying information of another person without authority. (b) The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any (1) name, [S]ocial [S]ecurity number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (2) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) unique electronic identification number, address, or routing code; or (4) telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e).").

[38] It should be noted that individuals have no Fourth Amendment protection for personal information that is voluntarily conveyed to another. As a result, end users must rely on statutory (rather than constitutional) protections for data disclosed to third party providers. See, e.g., § 10.01[3][b] *infra* for a discussion of Fourth Amendment analysis of expectations of privacy in connection with electronic searches pursuant to United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (holding that bank records are disclosed information and thus not subject to Fourth Amendment protection). It should also be noted that, although conceptually related, "data privacy" is treated as a separate and distinct topic from the privacy issues that arise under the Fourth Amendment in connection with electronic surveillance. See § 10.01 *infra* for a discussion of the Fourth Amendment's application to government surveillance. In addition, it should be noted that various intellectual property issues have a direct effect on privacy. See, e.g.: § 11.01[1] *infra* for a discussion of U.S. Const., Amend. I, § 8 in the context of the Copyright Act (17 U.S.C. §§ 101 *et seq*.) and the Patent Act (35 U.S.C. §§ 1-376); § 11.01[3][f][i] *infra* for a discussion of 17 U.S.C. § 512(m) (stating that "[n]othing in this section shall be construed to condition the applicability of subsections (a) through (d) on (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law"). See: § 1.02[3] *infra* for a discussion of the different laws that apply to (1) consumer data, (2) financial data, (3) credit data,

example, networks that store large amounts of personal and financial information will become increasingly attractive targets for criminals who perpetrate identity theft and fraud. In addition, portable devices such as laptop computers and personal digital assistants (PDAs), which are capable of storing large amounts of business data, subject customers to a wide range of potential harms and organizations to extensive remedial costs when these devices are lost or compromised.

[b]—Metcalfe's Law

The value of a network is a function of the number of users[39] connected to the network and the number of interconnections among users. This is "Metcalfe's Law," attributed to Robert Metcalfe, a pioneer of computer networking. As more powerful computing systems interconnect, information security increasingly becomes a "communal" issue that requires the sharing of sensitive information with affected organizations, customers, and regulators.[40]

[c]—Network Effects

"Network effects" occur when the value of a good or service to a potential customer is dependent on the number of customers already owning that good or using that service. The total value of a good or service that possesses network effects is roughly proportional to the square of the number of customers already owning that good or using that service (i.e., the purchase of such a good by one individual will indirectly benefit others who own the good).[41] Network effects may result in market dominance and limit the availability of alternative products and services. In the context of information security, market leaders must remain vigilant as dominant technologies perforce become attractive targets for computer criminals (and class action attorneys). Network effects exponentially increase potential damage to such products' end users when security flaws are subsequently exposed.[42] In the

---

(4) medical data, and (5) government data; Chs. 4-8 *infra* for a discussion of the various laws that protect the privacy of such data. Also see, § 9.05 *infra* for a discussion of fraudulent use of personal information that may occur in connection with a network breach.

[39] See, e.g., the definition of "user" under HIPAA pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [u]ser means a person or entity with authorized access").

[40] See, e.g., § 3.01[2] *infra* for a discussion of the actions an organization must take when responding to a network breach. See Computer Security Incident Handling Guide, 800-61 (Jan. 2004), available at http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf (last visited April 12, 2006).

[41] For example, "[a]n individual consumer's demand to use (and hence benefit from) the telephone network . . . increases with the number of other users on the network whom she can call or from whom she can receive calls." Shelanski and Sidak, "Antitrust Divestiture in Network Industries," 68 U. Chi. L. Rev. 1, 8 (2001). Once a product or standard achieves wide acceptance, it becomes more or less entrenched.

[42] In markets characterized by network effects, one product or standard tends towards dominance because "the utility that a user derives from consumption of the good increases with the number of other agents consuming the good." Katz and Shapiro, "Network Externalities, Competition, and Compatibility," 75 Am. Econ. Rev. 424 (1985). See, e.g., § 4.02[5] *infra* for a dis-

absence of a suitable industry response, government may have no choice but to impose legislation mandating proactive information security measures.[43]

[4]—Network Classification

Computer networks may be classified according to size and physical distribution of network resources such as servers, communications lines, access points, etc.[44] Generally, networks may be categorized in terms of spatial distance and intended users:

---

cussion of Microsoft's potential liability under the Federal Trade Commission Act's (FCTA's) Fair Information Practice Principles (FIPPs) and the increased risk of danger to end users of pervasive operating systems, In the Matter of Microsoft Corp., File No. 012 3240 (Dec. 24, 2002), available at http://www.ftc.gov/os/2002/08/microsoftana.htm (last visited April 12, 2006) (addressing alleged false security promises relating to the level of online security employed to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers in connection with the Passport and Passport Wallet services).

[43] See § 12.01[2][a] *infra* for a discussion of the various congressional committees that draft laws pertaining to information security and for references to current legislation pending in such bodies.

[44] Security plays different roles, and results in different forms of liability, depending on the system layer implicated by the behavior in question. For example, hardware may be protected through proper configuration of routing technology, anti-virus software, firewalls and filtering software. Communications that are routed through such hardware may also be protected by encryption. Different theories of liability will apply to theft of hardware, interception of specific communications, unauthorized decryption of data, and subsequent use or dissemination of the compromised data. In addition, software that resides on a network may be protected from unauthorized distribution through various intellectual property laws. See § 12.01[1][j] *infra* for a discussion of the Federal Communications Commission's role in regulating the physical layer of cyberspace. See Open Systems Interconnection (OSI) Reference Model, available at http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci523729,00.html (last visited April 12, 2006). Open Systems Interconnection (OSI) is a standard description or "reference model" for how messages should be transmitted between any two points in a network. OSI was officially adopted as an international standard by the International Organization of Standards (ISO). This model facilitates interoperability of products on the network by defining seven layers of functions that take place at each end of a communication. These layers are separated into two groups. The upper four layers are used whenever a message passes from or to a user. The lower three layers (up to the network layer) are used when any message passes through the host computer. Messages intended for a target computer pass to the upper layers. Messages destined for a third party host are forwarded without passing to the upper layers. See § 12.03[3] *infra* for a discussion of the ISO. See Benkler, "Coase's Penguin, or Linux and the Nature of the Firm," (2002), available at http://www.yale.edu/yalelj/112/BenklerWEB.pdf (last visited Aug. 6, 2005) (discussing how the Internet and other communication systems may be divided into three layers: (1) Physical (i.e., the physical hardware used to interconnect computers and users); (2) Logical (i.e., protocols and software that guide and manipulate the data reside in the physical infrastructure); and (3) Content (i.e., the information or data that the user receives at her computer)). See Ch. 12 *infra* for a discussion of the importance of procedures to achieve technical, legal and policy standards that are required by global network interoperability and coherence. See § 8.04 N. 3 *infra* for the definition of "interoperability" under the E-Government Act pursuant to 107 Pub. L. No. 347, 116 Stat. 2899, 2901-2902 § 101(a) (Dec. 17, 2002) (codified in 44 U.S.C. § 3601) (stating that "Title 44, United States Code, is amended by inserting after chapter 35 the following . . . 'Sec. 3601. Definitions. In this chapter, the definitions under section 3502 shall apply, and the term . . . (6) "interoperability" means the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner. . . .'").

(1) *Local Area Networks:* a local area network (LAN) comprises a group of computers that share a common communications line and typically share the resources of a single processor or server within a small geographic area (e.g., within an office building);

(2) *Wide Area Networks:* a wide area network (WAN) is a geographically dispersed telecommunications network that may be privately owned or rented;

(3) *Intranet:* an intranet is a private network contained "within" an enterprise, which is typically used to share information and computing resources among users; and

(4) *Extranet:* an extranet is a private network that uses the public telecommunication system to share securely its information or operations with suppliers, vendors, partners, customers or other businesses.

Organizations must adopt technical and procedural mechanisms that are appropriate *vis-à-vis* their specific network configurations, and specify the scope of acceptable use of network resources in established policies.[45]

Cloud computing is a computer network system that allows consumers, businesses, and public entities to store data off site and manage it with third party-owned software applications accessed through the Internet. The National Institute of Standards and Technology (NIST) working technical definition of "cloud computing" includes five "essential characteristics": on-demand self-service; ubiquitous network access; location-independent resource pooling; rapid elasticity; and measured service.[46] The NIST definition also identifies different ways in which the cloud vendor provides software applications, and different general categories of cloud computing depending on who is allowed access to and shares the cloud computing service platform. The popularity and widespread impact of cloud computing has lead the Federal Trade Commission to initiate a series of public roundtables to explore the challenges posed to consumer privacy by cloud computing.[47]

[5]—Network Access

Network access generally is the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any network resource.[48] Access presents a host of legal and security issues that

---

[45] See § 3.01 *infra* for a general discussion of information security policies and procedures.

[46] See NIST Computer Security Resource Center, available at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html (last visited Dec. 2, 2009).

[47] See Federal Trade Commission Annual Report, April 2010, available at http://www.ftc.gov/os/2010/04/2010ChairmansReport_screen.pdf.pdf (last visited April 27, 2010).

[48] See § 9.01[2] *infra* for a discussion of liability for unauthorized access to protected computers under the CFAA pursuant to 18 U.S.C. § 1030(a)(1)-(a)(5) and a discussion of the definition of "exceeds authorized access" under the CFAA pursuant to 18 U.S.C. § 1030(a)(1)-(e)(6) (stating that "[a]s used in this section . . . the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"). See § 10.01[4] *infra* for a discussion of Fourth Amendment protection to digital devices that are seized by government actors. See § 11.01[3] *infra* for a discussion of the DMCA, 17 U.S.C. §§ 1201 *et seq.*, and how "access" has become a focal point in statutes addressing digital works and computer systems

depends on the manner in which the user is accessing the network. As a general matter, computer networks can be accessed via:

(1) *Network Terminal:* users may be provided with "on-site" access to network resources via computer terminals that are physically located within the organization, which provides the organization with a greater degree of control of such networks;[49]

(2) *Virtual Private Network:* a virtual private network (VPN) allows an organization to use public telecommunication infrastructures such as cyberspace to provide remote offices or individual users with secure access to its network;[50]

(3) *Wireless Connection:* some networks permit access via "wireless" connections that use electromagnetic waves (rather than some form of wire) to transmit and receive signals.[51]

Unauthorized access to a network may facilitate criminal activity,[52] breach customer privacy,[53] and result in loss of valuable proprietary information.[54] In order to protect against such damage, organizations must imple-

---

and is echoed in various sections of the Copyright Act (17 U.S.C. §§ 101 *et seq.*). See § 10.03 *infra* for a discussion of unauthorized access to stored communications under the Stored Communications Act pursuant to 18 U.S.C. § 2701(a) (stating that "[e]xcept as provided in subsection (c) of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section"). See § 7.02[4] *infra* for a discussion of HIPAA's security standards pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings. . . . Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to 'access' as used in this subpart, not as used in subpart E of this part.) . . .").

[49] See, e.g., the definition of "workstation" under the HIPAA pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [w]orkstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment").

[50] A VPN maintains its security through procedures and tunneling protocols such as the Layer Two Tunneling Protocol. In effect, the protocols, by encrypting data at the sending end and decrypting them at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that are not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

[51] Wireless networks present many legal issues and are subject to "wardriving" attacks, where unauthorized users seek network access by search for unprotected signals. See § 4.02[3] *infra* for a discussion of liability for unauthorized access to protected computers under the CFAA pursuant to 18 U.S.C. § 1030(a)(1)-(a)(5). See § 11.01[4] *infra* for a discussion of the MPAA's proposed Super-DMCA legislation, which prohibits unauthorized access to various types of communications services (e.g., "signal" theft).

[52] See Ch. 9 *infra* for a discussion of criminal liability in connection with computer crimes.

[53] See: Chs. 4-8 *infra* for a discussion of the privacy laws that apply to information security.

[54] See Ch. 11 *infra* for a discussion of the various intangible assets that may be stored within networks.

ment access policies and engage in constant monitoring of network resources.[55]

Individuals who use or traffic in passwords to gain unauthorized access to protected computers[56] or copyrighted works[57] may be subject to both criminal liability and civil liability.[58] It should be noted that certain organizations may be required by regulation to adopt procedures that ensure proper authentication for access to their computer systems.[59] In addition to these

---

[55] See Ch. 10 *infra* for a discussion of the various laws that apply to electronic surveillance of computer networks.

[56] See § 9.01[1] *infra* for a discussion of the CFAA's definition of "protected computer" pursuant to 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as one "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States"). See § 10.03 *infra* for a discussion of unauthorized access to stored communications under the Stored Communications Act pursuant to 18 U.S.C. § 2701(a) (stating that "[e]xcept as provided in subsection (c) of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section").

[57] See § 11.01[2][g] *infra* for a discussion of 17 U.S.C. § 501(b) (stating that "[t]he legal or beneficial owner of an exclusive right under a copyright is entitled, subject to the requirements of section 411, to institute an action for any infringement of that particular right committed while he or she is the owner of it"), which requires a showing of unauthorized "copying" that may be inferred by demonstrating access to the work in question. See § 11.01[3] *infra* for a discussion of Lexmark International, Inc. v. Static Control Components, Inc., 253 F. Supp.2d 943 (E.D. Ky. 2003) (holding that § 1201(a) creates, and § 1201(a)(2) protects, the right of "access," violation of which is electronic equivalent of "breaking into a castle;" although the DMCA does not specifically define term "access," the term should be given its ordinary, customary meaning, which is the "ability to enter, to obtain, or to make use of"). See § 11.01[3][g] *infra* for a discussion of Recording Industry Ass'n. of America, Inc. v. Verizon Internet Services, Inc., Case No. 03-7015 (D.C. Cir. Dec. 19, 2003) (stating that "[a]s Verizon notes, the Congress considered disabling an individual's access to infringing material and disabling access to the internet to be different remedies for the protection of copyright owners, the former blocking access to the infringing material on the offender's computer and the latter more broadly blocking the offender's access to the internet (at least via his chosen ISP). *Compare*, 17 U.S.C. § 512(j)(1)(A)(i) (authorizing injunction restraining ISP 'from providing access to infringing material'), *with* 17 U.S.C. § 512(j)(1)(A)(ii) (authorizing injunction restraining ISP 'from providing access to a subscriber or account holder TTT who is engaging in infringing activity TTT by terminating the accounts of the subscriber or account holder').").

[58] See § 9.01[2][c][iii] *infra* for a discussion of liability under the CFAA in connection with unauthorized access that results in damage to computers via passwords. See § 9.01[4] *infra* for a discussion of liability under the CFAA for password trafficking pursuant to 18 U.S.C. § 1030(a)(6) (imposing liability on whoever "knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if (A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States"). Also see, § 9.01[2][c] *infra* for a discussion of I.M.S. Inquiry Management Systems v. Berkshire Information Systems, 2004 WL 345556 (S.D.N.Y. Feb. 23, 2004), which addresses the relation of the CFAA and DMCA in connection with the use of passwords to gain unauthorized access to a protected computer that contains copyrighted works.

[59] See § 8.08[1] *infra* for a discussion of the E-Government Act's information technology management requirements pursuant to Pub. L. No. 107-347, 116 Stat. 2899, 2957, § 303(a) (Dec. 17, 2002) (codified in 15 U.S.C. § 278g-3) (stating that "Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. § 278g-3), is amended by striking the text and

security concerns, authentication raises many issues relating to end user privacy, especially when such users are consumers.[60]

---

inserting the following: '(a) In General. The Institute shall (1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems. . . .'"). See § 9.05[5] *infra* for a discussion of the Fair and Accurate Credit Transactions Act's (FACTA's) authentication requirements pursuant to Pub. L. No. 108-159, 117 Stat. 1952, § 318(a)(2)(A) (stating that "[i]n conducting the study under paragraph (1), the Commission shall review (A) the efficacy of increasing the number of points of identifying information that a credit reporting agency is required to match to ensure that a consumer is the correct individual to whom a consumer report relates before releasing a consumer report to a user, including (i) the extent to which requiring additional points of such identifying information to match would (I) enhance the accuracy of credit reports; and (II) combat the provision of incorrect consumer reports to users; (ii) the extent to which requiring an exact match of the first and last name, social security number, and address and ZIP Code of the consumer would enhance the likelihood of increasing credit report accuracy; and (iii) the effects of allowing consumer reporting agencies to use partial matches of social security numbers and name recognition software on the accuracy of credit reports . . ."). See § 5.06[3] *infra* for a discussion of 66 Fed. Reg. 8616, § III.C.1.a (Feb. 1, 2001) (stating that "[y]ou shall . . . [d]esign your information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of your activities. You must consider whether the following security measures are appropriate for you and, if so, adopt those measures you conclude are appropriate . . . [a]ccess controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means. . . ."). See § 7.02[4] *infra* for a discussion of HIPAA's security standards requirements pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [a]uthentication means the corroboration that a person is the one claimed . . ."). Also see, Putting an End to Account-Hijacking Identity Theft, Federal Deposit Insurance Corporation (Dec. 14, 2004), available at http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf (last visited April 12, 2006) (studying a subset of identity theft that relates to unauthorized access to and misuse of existing asset accounts primarily through phishing and hacking, referred to as "account hijacking," which has largely resulted from reliance on single-factor authentication for remote access to online banking, and the lack of e-mail and Web site authentication).

[60] For instance, in order to ensure privacy, authentication systems for consumer-initiated transactions and government services should: (1) provide user control (i.e., the informed consent of the individual should be obtained before information is used for enrollment, authentication and any subsequent uses); (2) support a diversity of services (i.e., individuals should have a choice of authentication tools and providers in the marketplace); (3) use individual authentication only when appropriate (i.e., authentication systems should be designed to authenticate individuals by use of identity only when such information is needed to complete the transaction); (4) provide notice (i.e., individuals should be provided with a clear statement about the collection and use of information upon which to make informed decisions); (5) minimize collection and storage (i.e., institutions deploying or using authentication systems should collect only the information necessary to complete the intended authentication function); (6) provide accountability (i.e., authentication providers should be able to verify that they are complying with applicable privacy practices). The development of authentication systems for e-government services also raises a host of privacy concerns. Many e-government projects that intend to develop and/or use authentication systems are currently being developed. However, this raises not only concerns about the use of personal information similar to those arising in the commercial context but also concerns about the creation of a centralized government identity system or card. See § 4.02 *infra* for a discussion of evolving Fair Information Practice Principles (FIPPs). See § 8.06 *infra* for a discussion of privacy provisions that relate to e-government services under the E-Government Act pursuant to Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002). See § 10.01 *infra* for a discussion of the Fourth Amendment's application to government surveillance.

[6]—Authentication

Typically, the first step in controlling access to computer networks involves "authentication," which is the process whereby the network determines the identity of a user.[61] Authentication may be accomplished through various means or "factors," including the use of biometric identifiers,[62] logon passwords,[63] or tokens. As society increases its reliance on cyberspace,

---

[61] See: Cryptographic Algorithms and Key Sizes for Personal Identity Verification, National Institute of Technology Standards, Special Publication 800-78 (April 2005), available at http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf (last visited April 12, 2006) (discussing the technical specifications needed for the mandatory and optional cryptographic keys specified in FIPS 201 as well as the supporting infrastructure specified in FIPS 201 and the related Special Publications 800-73, Interfaces for Personal Identity Verification, and 800-76, Biometric Data Specification for Personal Identity Verification, that rely on cryptographic functions); Electronic Authentication Guideline, National Institute of Technology Standards, Special Publication 800-63 (Sept. 2004), available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf (last visited April 12, 2006). Also see: § 9.05[5][a] *infra* for a discussion of identity theft victim authentication pursuant to Pub. L. No. 108-159, 117 Stat. 1952, § 112(a) (2003) (stating that "[t]he Fair Credit Reporting Act (15 U.S.C. §§ 1681 *et seq.*) is amended by inserting after section 605 the following. . . . 'Sec. 605A. Identity theft prevention; fraud alerts and active duty alerts. . . . (h) Limitations on Use of Information for Credit Extensions. (1) Requirements for initial and active duty alerts. . . . (B) Limitation on users. (ii) Verification. If a consumer requesting the alert has specified a telephone number to be used for identity verification purposes, before authorizing any new credit plan or extension described in clause (i) in the name of such consumer, a user of such consumer report shall contact the consumer using that telephone number or take reasonable steps to verify the consumer's identity and confirm that the application for a new credit plan is not the result of identity theft. . . .'"); § 7.02[5] for a discussion of authentication under HIPAA pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [a]uthentication means the corroboration that a person is the one claimed . . .").

[62] Translated literally, "biometrics" means "life measurement." *Bios* is Greek for "life"; *Metricus* is Latin for "relating to measurement." See The Counterdrug Technology Information Network, An Introduction to Biometrics, available at http://www.ctin.com/Biometrics/Biometrics.htm (last visited April 14, 2006). See, e.g., Rand, Biometrics: Will Digital Fingerprints, Iris Scans and Speaker Recognition Soon Replace Passwords and Personal Identification Numbers?, available at http://www.rand.org/natsec/products/bionav.html (last visited April 14, 2006). See § 9.05[5][j] *infra* for a discussion of Pub. L. No. 108-159, 117 Stat. 1952 § 157(a) (2003) (stating that "[t]he Secretary of the Treasury shall conduct a study of the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction").

[63] Initially, each user will register using an assigned or self-declared password. Subsequently, each time the user attempts to access the network, the user must know and use the previously established password. Password systems, however, present weaknesses for commercially significant transactions. This is because passwords can be stolen, accidentally revealed, or forgotten. For this reason, many transactions require a more stringent authentication process. Such processes include the use of digital certificates that are issued and verified by a Certificate Authority as part of a public key infrastructure (PKI). This PKI system is considered likely to become the standard way to perform authentication in cyberspace. See: § 7.03[2][a] *infra* for a discussion of HIPAA's administrative safeguards requirements pursuant to 45 C.F.R. § 164.308(a)(5)(i) (July 22, 2004) (stating "Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management)."); 45 C.F.R. § 164.308(a)(5)(ii)(D) (July 22, 2004) (stating "Password management (Addressable). Procedures for creating, changing, and safeguarding passwords."); 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [p]assword means confidential authentication information composed of a string of characters"). See § 10.01[6] *infra* for a discussion of Fourth Amendment protection

however, government and industries are reevaluating the methods used to facilitate access in order to address online threats. One method for addressing evolving threats includes "layered security" (i.e., implementing multiple controls so that a weakness in one control is generally compensated for by the strength of a different control). For example, financial institutions have been advised by regulators to implement muti-factor authentication for certain types of users.[64] Such factors may include USB tokens or "out-of-band" authentication to multiple devices (e.g., a transaction that is initiated via one delivery channel such as the Internet must be re-authenticated via an independent delivery channel such as the telephone in order to complete the transaction). In addition, the use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered a more secure way to authenticate users on the Internet. Moreover, the United States has officially recognized that online authentication of people and devices has lead to insecurity in cyberspace and has begun to remedy this situation by calling for the establishment of "trusted identities."[65]

New models for digital identity have been evolving in order to streamline online interactions and facilitate authentication, including "user-centric identity." These new models for identity management differentiate between the service provider and the identity provider, allowing users to log in to multiple Web sites using a single set of credentials. This trust framework will connect the user, the identity provider, and the service provider, by establishing a set of conditions that each party must adhere to in order to maintain a "trusted system." For example, in user-centric identity systems (also called "federated identity"), a user logs in to a Web site via a third party identity provider, who passes on information at the user's request. This system is "user centric" because of the fact that the user is at the center of the interaction, in contrast to a system that requires users to authenticate directly to a site or having a third party authenticate the user without the user's direct involvement. These identity systems may become subject to increased regulatory scrutiny to ensure that consumer protection is adequately addressed. For instance, some argue that identity providers should be subject to the Fair Credit Reporting Act's requirements regarding the collection, dissemination and use of consumer information.[66]

---

of shared computers under Trulock v. Freeh, 275 F.3d 391, 403-404 (4th Cir. 2001) (analogizing password-protected files to locked footlockers inside a bedroom, which the court had previously held to be outside the scope of common authority consent). See § 9.02[2][c] *infra* for a discussion of I.M.S. Inquiry Management Systems v. Berkshire Information Systems, 2004 WL 345556 (S.D.N.Y. Feb. 23, 2004), which addresses the relation of the CFAA and DMCA in connection with the use of passwords to gain unauthorized access to a protected computer that contains copyrighted works.

[64] See § 5.06[3[a] *infra* for a discussion of FFIEC Supplement to Authentication in an Internet Banking Environment (June 2011), available at http://www.fdic.gov/news/news/press/2011/pr11111a.pdf (last visited Aug. 20, 2011).

[65] See National Strategy for Trusted Identities in Cyberspace (April 2011), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (last visited July 20, 2011).

[66] See § 6.01[2] *infra* for a discussion of consumer reporting agencies and Protecting Privacy in Online Identity: A Review of the Letter and Spirit of the Fair Credit Reporting Act's Application to Identity Providers, Center for Democracy & Technology (Feb. 26, 2010).

§ 1.02 Data

Networks facilitate communications by transferring data along various configurations of connection points within a system called "nodes." These data are a key asset of any organization and may be protected via policy,[1] contract[2] and various laws that relate to privacy,[3] crime[4] and intellectual property.[5] As discussed earlier, the extent of security required by a given organization will be governed by the value an organization assigns to the data residing within its network.[6] When analyzing the security and legal implications of data, two common data types are considered: (1) data "at rest" (i.e., stored data) and (2) data "in motion" (i.e., communications).

[1]—Stored Data

Data "at rest" are stored within a network and should only be accessible to specified users.[7] Such data include intra-office communications, propri-

---

[1] See Ch. 3 *infra* for a general discussion of information security policies and procedures used to secure assets in digital environments.

[2] See, e.g.: § 5.06[1][c] *infra* for a discussion of the Gramm-Leach-Bliley Act (GLBA) FTC Safeguards Rule's service provider requirements as set forth in 16 C.F.R. § 314.4(d)(2) (stating that "[i]n order to develop, implement, and maintain your information security program, you shall . . . [o]versee service providers, by . . . [r]equiring your service providers by contract to implement and maintain such safeguards"); § 7.03[2][b] *infra* for a discussion of the HIPAA Security Safeguard Rule's business associate contract requirements pursuant to 45 C.F.R. § 164.308(b)(1) (July 22, 2004) (stating that "Standard: Business associate contracts and other arrangements. A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.").

[3] See Chs. 4-8 *infra* for a discussion of the various laws that protect the privacy of data. Also see, § 9.05[5][e][ii] *infra* for a discussion of identity theft victims' rights under the Fair and Accurate Credit Reporting Act (FACTA) pursuant to Pub. L. No. 108-159, 117 Stat. 1952, § 151(a)(1) (2003) (stating that "[s]ection 609 of the Fair Credit Reporting Act (15 U.S.C. 1681g) is amended by adding at the end the following: '. . . (e) Information Available to Victims. . . . (5) Authority to decline to provide information. A business entity may decline to provide information under paragraph (1) if, in the exercise of good faith, the business entity determines that (A) this subsection does not require disclosure of the information; (B) after reviewing the information provided pursuant to paragraph (2), the business entity does not have a high degree of confidence in knowing the true identity of the individual requesting the information; (C) the request for the information is based on a misrepresentation of fact by the individual requesting the information relevant to the request for information; or (D) the information requested is Internet navigational data or similar information about a person's visit to a website or online service. . . .'").

[4] See Ch. 9 *infra* for a discussion of criminal liability in connection with computer crimes.

[5] See Ch. 11 *infra* for a discussion of the laws that protect intangible assets such as data.

[6] See, e.g., § 5.06[1][c] *infra* for a discussion of the GLBA FTC Safeguards Rule's flexible standards pursuant to 67 Fed. Regs. 36484, 36488 (May 23, 2002) (stating that "[t]his standard is highly flexible, consistent with the comments, the Banking Agency Guidelines, and the Advisory Committee's Report, which concluded that a business should develop 'a program that has a continuous life cycle designed to meet the needs of a particular organization or industry'").

[7] See, e.g., § 7.03[2][a] *infra* for a discussion of HIPAA's administrative safeguards pursuant to 45 C.F.R. § 164.308(a)(3)(i) (July 22, 2004) (stating that "Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of

etary material, information submitted by customers, network applications, and meta-data (i.e., information about these data, such as authors, recipients, access/modification dates, etc.). Typically, data are protected on networks by limiting access via properly configured user accounts and the use of passwords. It should be noted that such data (and passwords) are subject to discovery demands in civil litigation and search and seizure in the context of criminal litigation.[8] Data are also becoming vulnerable to potential security breaches that might occur at border security checkpoints.[9] In addition, these data, which may contain valuable, proprietary information,[10] are subject to theft by network intruders.[11] More disturbingly, improper security procedures[12] may constitute a breach of fiduciary duty in connection with certain classes of data.[13] Companies may be restricted from transferring data as part of a sale or bankruptcy if such transfers are restricted by terms contained in user agreements or privacy policies or both.[14]

---

this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.").

[8] See: § 3.06 *infra* for a discussion of those policies that an organization must adopt to address retention and destruction of data and documents; § 2.04[7] *infra* for a discussion of the Sarbanes-Oxley Act's (SOX's) data retention provisions set forth in Pub. L. No. 107-204, § 802(a), 116 Stat. 745, 800 (2002); § 10.01[4][a] *infra* for a discussion of Fourth Amendment protection of seized digital devices that have "intermingled" data in light of large storage capacity pursuant to *Manual for Complex Litigation* § 11.446, at 77 (4th ed. 2004) (stating that a megabyte of memory holds the equivalent of 500 typewritten pages of text and a floppy disk generally has a capacity of 1.44 megabytes, which means a capacity of 720 pages of plain text).

[9] See United States v. Arnold, No. 06-50581 (9th Cir. 2008) (stating that the expectation of privacy for border searches was lower and reasonable suspicion is not required for it). Also see: ACLU of Northern California, "The Privacy of Your Laptop at International Borders," available at http://www.aclunc.org/issues/technology/blog/the_privacy_of_your_laptop_at_international_borders.shtml (last visited Dec. 5, 2011); § 3.03[3] *infra* for a discussion of employer policies on passwords; § 10.01 *infra* for a discussion of the Fourth Amendment.

[10] See: Ch. 11 *infra* for a discussion of the various intangible assets that may be stored within networks; § 11.01[2][a][i] *infra* for a discussion of copyright protection pursuant to 17 U.S.C. § 101(a)(1) (stating that "Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Works of authorship include the following categories . . . literary works.").

[11] See: § 9.01 *infra* for a discussion of federal laws that apply to unauthorized access to protected computers under the Computer Fraud and Abuse Act (CFAA) pursuant to 18 U.S.C. § 1030; § 9.05 *infra* for a discussion of the various laws that apply to identity theft.

[12] See § 3.01 *infra* for a discussion of the policies that bolster information security technologies.

[13] See § 1.02[3] *infra* for a discussion of the different laws that apply to consumer data, financial data, credit data, health data, and government data. See Chs. 4-8 *infra* for a discussion of the various laws that protect the privacy of such data.

[14] See, e.g., Perkins v. Verified Identity Pass Inc., No. 09-5951 (S.D.N.Y. Aug. 18, 2009) (holding that Verified Identity Pass Inc. must secure and refrain from selling or otherwise disclosing biometric and other personal information belonging to travelers enrolled in its now-

Organizations may attempt to store data or gain access to data already stored in the terminal equipment of users for a variety of reasons. Such storage and access should only take place with the user's consent.[15] One common piece of technology used to send information from a user's browser is called a "cookie." Different types of cookies include:

(1) First-party cookies: either originate on or are sent by the host Web site of the service currently being accessed by the user, and are commonly used to store information (e.g., user preferences such as log-in name).

(2) Third-party cookies: are often used to track Web pages used for advertising or other marketing purposes, and deliver advertising content into a Web page from an external source (e.g., "sponsored links" columns or banner advertising networks).

(3) Session cookies: are used to store only temporary information and are deleted when the current Internet browsing session ends (i.e., when the user closes his browser); they include a unique session ID that does not personally identify users; data are stored in the temporary memory of the computer and not written to the hard drive, are anonymous, and are used to identify the computer browser.

(4) Persistent cookies: enhance or streamline user experience by storing preferences or user data, are used by Web sites to store information such as the sign-in name so users do not have to sign-in again when returning to the site, and stay on the hard drive after the current browsing session until erased by the user or expire at the time set by the issuing Web server.

(5) Flash cookies: also called "Local Shared Objects," these cookies are software files created using a "flash" authoring tool and are designed to avoid deletion, permitting browsers to continue to be identifiable by a server and facilitating reinstallation of deleted HTTP cookies even after the user intentionally deletes the cookie (i.e., "re-spawning").

Although cookies are not considered software (i.e., they cannot be programmed to carry out functions), they may be used for authentication[16] and may facilitate tracking of users' browsing activities. Specific "cookies laws" have evolved in certain countries to govern the use of such technology, while in the United States such technologies are typically governed by consumer protection laws.[17]

---

defunct CLEAR registered traveler program). The court found that defendant Verified Identity Pass Inc. agreed in its CLEAR membership agreement and related privacy policy to maintain safeguards to protect subscribers' information, and promised that it would not sell or otherwise distribute compilations of that data. As a result, the court found that former customers will likely succeed with their request for a permanent injunction prohibiting the company from selling or disclosing any of their confidential personal information.

[15] See § 4.02[2] *infra* for a discussion of Fair Information Practice Principles (FIPPs) and user choice.

[16] See § 1.01[6] *supra* for a discussion of authentication technology.

[17] See § 4.01 *infra* for a discussion of consumer protection under the Federal Trade Commission Act pursuant to 15 U.S.C. §§ 41 *et seq*.

[2]—Communications

Data may be "in motion" either within a network or when transferred outside the network. Such data are protected from unauthorized electronic surveillance by various laws.[18] These laws protect both the data themselves and data associated with their transfer (i.e., meta-data) from unauthorized interception[19] and unauthorized access while residing within the intermediate communications systems.[20] These statutes demonstrate how communication integrity is dependent upon both the communication itself and the system on which the communication resides.[21] It has been argued that individuals have no Fourth Amendment interest in personal information that is voluntarily conveyed to another. As a result, privacy protections for personal information must be established by legislation.[22] Although conceptually related, "data privacy" is treated as a separate and distinct topic from the privacy

---

[18] See § 10.02[2][a] *infra* for a discussion of the different types of electronic communications protected by the Wiretap Act (Title III) under 18 U.S.C. § 2510(12) (stating that "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds").

[19] See, e.g., § 10.02[2][b] *infra* for a discussion of the Wiretap Act's general prohibition against the interception of communication under 18 U.S.C. § 2511(1)(a) (stating that "[e]xcept as otherwise specifically provided in this chapter [18 U.S.C. §§ 2510 *et seq*.] any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).").

[20] See § 10.03[1] *infra* for a discussion of liability under the Stored Communications Act for intentional unauthorized access to electronic communications facilities.

[21] For example, when computers that are connected to cyberspace communicate with each other, they break down messages into discrete chunks known as "packets," and then send each packet out to its intended destination. Every packet contains addressing information in the "header" of the packet (e.g., like the "to" and "from" addresses on an envelope), followed by the content of the message (e.g., like a letter inside an envelope). E-mail messages consist of sets of headers that contain addressing and routing information generated by the mail program, followed by the actual contents of the message authored by the sender. The addressing and routing information includes the e-mail address of the sender and recipient, as well as information about when and where the message was sent on its way (roughly analogous to the postmark on a letter). See § 10.04[3] *infra* for a discussion of court orders to install monitoring devices pursuant to the Pen Register and Trap and Trace Devices Act under 18 U.S.C. § 3122. The Pen/Trap statute permits law enforcement to obtain the addressing information of Internet e-mails (with the exception of the subject line, which can contain content) using a court order, in the same manner that court orders permit government agents to obtain addressing information for phone calls and individual Internet "packets" using a court order. Conversely, the interception of e-mail contents, including the subject line, requires careful compliance with Title III. See § 1.04[2] *infra* for a discussion of firewall technology, which examines each network packet and determines whether to forward it to its destination.

[22] See, e.g., § 10.01[3][b] *infra* for a discussion of United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (holding that bank records are disclosed information and thus not subject to Fourth Amendment protection).

issues that arise under the Fourth Amendment in connection with electronic surveillance by government actors.[23]

[3]—Data Classification

In addition to considering the state of data (i.e., whether data are "at rest" or "in motion"), security and legal issues must be analyzed based upon the type of information to which the data relate. A wide variety of domestic and international laws govern the integrity of such data classes.[24] These laws must be addressed when collecting and utilizing:

(1) Consumer Data: consumer data (and particularly children's data)[25] are subject to regulation under the Federal Trade Commission Act (FTCA),[26] which prohibits unfair and deceptive practices in and affecting commerce;[27]

(2) Financial Data: the Sarbanes-Oxley Act of 2002 (SOX)[28] addresses the integrity of corporate financial disclosures and the Gramm-Leach-Bliley Act (GLBA)[29] imposes privacy obligations on institutions that engage in financial activities;[30]

---

[23] See § 10.01 *infra* for a discussion of the Fourth Amendment's application to government surveillance.

[24] See Chs. 4-8 *supra* for a discussion of the various laws that protect the privacy of such data. Also see, § 5.06[1][c] *infra* for a discussion of the Gramm-Leach-Bliliey Act FTC Safeguard Rule, which provides different levels of protection depending on the sensitivity of such data, as set forth in 67 Fed. Regs. 36484, 36488 at n.46 (May 23, 2002) (stating that "[t]he adaptability of the standard according to 'the sensitivity of information' mirrors the Advisory Committee's finding that 'different types of data warrant different levels of protection'").

[25] See § 4.03 *infra* for a discussion of the Children's Online Privacy Protection Act (COPPA) pursuant to 15 U.S.C. §§ 6501-6506, Pub. L. No. 105-277, 112 Stat. 2681-2728 (1998).

[26] 15 U.S.C. §§ 41 *et seq*.

[27] See § 4.01 *infra* for a discussion of 15 U.S.C. § 45(a)(1) (stating that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful"), and 15 U.S.C. § 45(n) (stating that "[t]he Commission shall have no authority under this section or section 18 [15 U.S.C. § 57a] to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.").

[28] See Ch. 2 *infra* for a discussion of corporate governance under SOX pursuant to Pub. L. No. 107-204, 116 Stat. 745 (July 30, 2002) (codified in scattered sections of 11, 15, 18, 28 and 29 U.S.C.).

[29] Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (codified in 15 U.S.C. §§ 6801-6809 and §§ 6821-6827).

[30] See: § 5.01 *infra* for a discussion of 15 U.S.C. § 6809(3)(A) (stating that "[a]s used in this subtitle . . . [t]he term 'financial institution' means any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 [12 U.S.C. § 1843(k)]"); § 5.06[1] *infra* for a discussion of 67 Fed. Reg. 36484 at p.4 (May 23, 2002) (stating that "[b]ecause, as noted below, 'financial institution' is defined as it is in section 509(3)(A) of the Act and the Privacy Rule, the Rule covers a wide range of entities, including: non-depository lenders; consumer reporting agencies; debt collectors; data processors; courier services; retailers that extend credit by issuing credit cards to consumers;

(3) Credit Data: the Fair Credit Reporting Act (FCRA),[31] as amended by the Fair and Accurate Credit Transactions Act (FACTA)[32] to address specific issues raised by identity theft,[33] requires organizations to adopt reasonable procedures to ensure the confidentiality, accuracy, relevancy and proper use of consumer credit, personnel, insurance and other information;[34]

---

personal property or real estate appraisers; check-cashing businesses; mortgage brokers, and any other entity that meets this definition"); § 9.05[5][p] *infra* for a discussion of the Fair and Accurate Credit Report Act's (FACTA's) revisions to the Fair Credit Reporting Act (FCRA) to address negative information pursuant to Pub. L. No. 108-159, 117 Stat. 1952, § 217(a) (Dec. 4, 2003) (stating that "[s]ection 623(a) of the Fair Credit Reporting Act (15 U.S.C. 1681s-2(a)) as amended by this Act, is amended by inserting after paragraph (6), the following new paragraph: '(7) Negative information. . . . (G) Definitions. For purposes of this paragraph, the following definitions shall apply . . . (ii) Customer; financial institution. The terms "customer" and "financial institution" have the same meanings as in section 509 Public Law 106-102.'"). Also see, Individual Reference Services Group, Inc. v. FTC 145 F. Supp.2d 6 (D.C. Cir. 2001) (rejecting a consumer reporting agency's contention that it is a non-financial institution and, therefore, not regulated by the FTC and related agencies, owing to the fact that it did not contest fact that it is a "credit reporting bureau," because 15 U.S.C. § 6809(3)(A) defines financial institution as "any institution the business of which is engaging in financial activities as described in 12 U.S.C. § 1843(k)" and that statute, as well as regulations promulgated thereunder, clearly includes activities closely related to banking including credit bureau services).

[31] 15 U.S.C. §§ 1681 *et seq*.

[32] See § 9.05[5] *infra* for a discussion of Pub. L. No. 108-159, 117 Stat. 1952 (Dec. 4, 2003).

[33] See: § 9.05 *infra* for a discussion of the various laws that apply to identity theft; § 9.05[5] *infra* for a discussion of Pub. L. No. 108-159, 117 Stat. 1952 (Dec. 4, 2003) (stating that FACTA is an act "[t]o amend the Fair Credit Reporting Act, to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes"), and a discussion of the definition of "identity theft" under the Fair and Accurate Credit Transactions Act pursuant to Pub. L. No. 108-159, 117 Stat. 1952, § 318(b) (Dec. 4, 2003) (stating that "[s]ection 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a) is amended by adding at the end the following: '(q) Definitions Relating to Fraud Alerts. . . . (3) Identity theft. The term 'identity theft' means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation. . . .'"); and 16 C.F.R. § 603.2 (Dec. 1, 2004) (stating that "(a) The term 'identity theft' means a fraud committed or attempted using the identifying information of another person without authority. (b) The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any (1) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (2) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) unique electronic identification number, address, or routing code; or (4) telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e).").

[34] See: § 6.01 for a discussion of FCRA pursuant to 15 U.S.C. § 1681(b) (stating that "[i]t is the purpose of this title to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this title"); Guimond v. Trans Union Credit Information Co., 45 F.3d 1329 (9th Cir. 1995) (holding that FCRA was crafted to protect consumers from transmission of inaccurate information about them, and to establish credit reporting practices that use accurate, relevant and current information in a confidential and responsible manner).

(4) Health Data: the Health Insurance Portability and Accountability Act (HIPAA)[35] creates standards relating to electronic data exchange, unique health identifiers, code sets, security, electronic signatures, health plan data transfers, and health information privacy;[36] and

(5) Government Data: the E-Government Act of 2002,[37] which created the Federal Information Security Management Act of 2002 (FISMA)[38] to address information security controls in federal computer networks,[39]

---

[35] Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[36] See § 7.03 *infra* for a discussion of HIPAA's information privacy standards as set forth in Pub. L. No. 104-191, 110 Stat. 1936 § 264 (1996) (codified in 42 U.S.C. § 1320d-2 note); Pub. L. No. 104-191, 110 Stat. 1936, 2021-2022 § 262(a) (1996) (codified in 42 U.S.C. § 1320d-2) (stating that "Title XI (42 U.S.C. 1301 *et seq*.) is amended by adding at the end the following . . . 'Part C Administrative Simplification DEFINITIONS Sec. 1171. (42 USC 1320d) For purposes of this part . . . (4) Health information. The term 'health information' means any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.'"); and Pub. L. No. 104-191, 110 Stat. 1936, 2021-2022 § 262(a) (1996) (codified in 42 U.S.C. § 1320d-2) (stating that "Title XI (42 U.S.C. 1301 *et seq*.) is amended by adding at the end the following . . . 'Part C Administrative Simplification DEFINITIONS Sec. 1171. (42 USC 1320d) For purposes of this part . . . (6) Individually identifiable health information. The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.'"); and 45 C.F.R. § 160.103 (July 22, 2004) (stating that "[e]xcept as otherwise provided, the following definitions apply to this subchapter . . . [h]ealth information means any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.").

[37] Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).

[38] See § 8.07 *infra* for a discussion of Pub. L. No. 107-347, 116 Stat. 2899, 2946 § 301(a) (Dec. 17, 2002) (codified in 44 U.S.C. § 101 note) (stating that "[t]his title may be cited as the 'Federal Information Security Management Act of 2002'").

[39] See § 8.07 *infra* for a discussion of: Pub. L. No. 107-347, 116 Stat. 2899, 2946 § 301(b)(1) (Dec. 17, 2002) (codified in 44 U.S.C. § 101 note) (stating that "[c]hapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter: 'SUBCHAPTER III—INFORMATION SECURITY' . . ."); and Pub. L. No. 107-347, 116 Stat. 2899, 2946-2947 § 301(b)(1) (Dec. 17, 2002) (codified in 44 U.S.C. § 101 note) (stating that "[c]hapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter . . . Sec. 3542. Definitions. (a) In General. Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter. (b) Additional Definitions. As used in this subchapter: (1) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (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.'"). Also see, Rec-

enhances citizen access to government information and services[40] in a manner consistent with laws regulating such things as protection of personal privacy, national security,[41] records retention, and access for persons with disabilities.[42]

The prevalence of powerful mobile devices has created new classes of location-based services and applications. In addition, companies are using new technologies that are capable of targeting specific users based on Internet Protocol (IP) addresses.[43] The resulting "location data" become increasingly commoditized as the accuracy of the services and applications improves and the expense of calculating and obtaining the data declines. The increasing availability of such location data raises several privacy concerns. Because individuals often carry mobile devices on their person, location data may be collected at any time and without user interaction. These data may describe both activities a person is engaged in and where these activities take place. Location data's prevalence may also increase risks of violent crimes if criminals are able to gain access to location data about potential victims. This data will also continue to be of interest to governments and law enforcement, which may seek to access detailed records of individuals' movements.

---

ommended Security Controls for Federal Information Systems, 800-53 (Feb. 2005), available at http://csrc.nist.gov/publications/nistpubs/ (last visited Jan. 29, 2006).

[40] See § 8.01 *infra* for a discussion of Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002) (stating that the act was promulgated "[t]o enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes").

[41] See § 8.01 *infra* for a discussion of Pub. L. No. 107-347, 116 Stat. 2899, 2946-2947 § 301(b)(1) (Dec. 17, 2002) (codified in 44 U.S.C. § 101 note) (stating that "[c]hapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter . . . Sec. 3542. Definitions. (a) In General. Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter. (b) Additional Definitions. As used in this subchapter: . . . (2)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency (i) the function, operation, or use of which (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).'"). Also see, Guideline for Identifying an Information System as a National Security System, 800-59 (Aug. 2003), available at http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf (last visited Jan. 29, 2006).

[42] See § 8.01 *infra* for a discussion of Pub. L. No. 107-347, 116 Stat. 2899, 2900-2901 § 2(b)(11) (Dec. 17, 2002) (codified in 44 U.S.C. § 3601 note) (stating that "[t]he purposes of this Act are the following . . . [t]o provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws").

[43] See § 4.02 *infra* for a discussion of Fair Information Practice Principles and the use of IP addresses.

§ 1.03 Network Attacks

Many organizations connect their networks to cyberspace in order to offer services (e.g., via browser-based technologies) or to ease communications with customers, employees and vendors. Each computer that is connected to cyberspace, however, is susceptible to intrusion. To mitigate the risks associated with such "open" networks, it is necessary to establish effective information security programs,[1] analyze unauthorized network access,[2] take remedial measures,[3] and limit potential liability for compromised systems.[4] This requires understanding the primary cyber security risks that face networks, the motivations of computer criminals, and the methods they employ to infiltrate systems. These threats will guide companies in drafting their security policies and aid regulators when drafting and enforcing laws.[5] This knowledge will also be necessary in the context of litigation in order to prepare for discovery requests and ensure successful prosecution of perpetrators.

---

[1] See § 3.01 *infra* for a discussion of the information security policies organizations must implement to secure computer systems. It should be noted that corporate practices may also compromise network security. For instance, senior executives sometimes circumvent established security procedures and policies in order to expedite various requests. This may cause staff not to question future requests that purport to come from the corporate officer. This may lead to liability for corporate officers and is best avoided by enforcing established policy. See § 2.04[6] *infra* for a discussion of how the Sarbanes-Oxley Act applies to corporate information security.

[2] See § 9.01[2] *infra* for a discussion of liability for unauthorized access to protected computers under the Computer Fraud and Abuse Act (CFAA) pursuant to 18 U.S.C. § 1030(a)(1)-(a)(5). See § 11.01[3] *infra* for a discussion of the Digital Millennium Copyright Act (DMCA) (17 U.S.C. §§ 1201 *et seq.*) and how "access" has become a focal point in statutes addressing digital works and computer systems and is echoed in various sections of the Copyright Act (17 U.S.C. §§ 101 *et seq.*). See § 10.03 *infra* for a discussion of unauthorized access to stored communications under the Stored Communications Act pursuant to 18 U.S.C. § 2701(a) (stating that "[e]xcept as provided in subsection (c) of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section"). See § 7.02[4] *infra* for a discussion of the Health Insurance Portability and Accountability Act's (HIPAA) definition of "access" pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to 'access' as used in this subpart, not as used in subpart E of this part.) . . ."). See § 3.04 *infra* for a discussion of the contractual provisions organizations create to establish "authorized use."

[3] See § 3.01[2] *infra* for a discussion of the policies organizations must adopt to address security breaches.

[4] See § 1.02[3] *supra* for a discussion of the different laws that impose security obligations on those that collect, use or disseminate consumer data, financial data, credit data, health data, and government data. See: Chs. 4-8 *infra* for a discussion of the various laws that protect the privacy of such data.

[5] See § 3.01 *infra* for a discussion of the information security policies organizations must implement to secure computer systems. See Ch. 12 *infra* for a discussion of the governmental, industrial and international bodies that shape information security law and policy.

[1]—Primary Vulnerabilities

Studies demonstrate that the most pressing cyber security vulnerabilities exist in devices, operating systems and applications,[5.1] and among end users.[5.2] Critics state that operating system providers and application developers do not incorporate adequate cyber protections into their products during product design. Furthermore, failing to disclose known vulnerabilities to trusted third parties who may be able to offer assistance compounds the problem. Simultaneously, end users often fail to implement the precautions against malware and other threats. The problem is further exacerbated by the public release of security patches that are necessary to correct security flaws, but potentially expose critical vulnerabilities, allowing bad actors to exploit users who fail to implement the patches.[5.3]

[1A]—Network Intruders

Network intruders (or "computer trespassers")[5.4] possess a variety of expertise and employ a wide range of methods. Intruders may be classified as follows:

(1) *Hackers:* "hacker" is a generic term used by computer programmers to describe a clever programmer (in the world of computer science, this term *does not* necessarily connote malicious intent);

(2) *System Crackers:* the term "cracker" (as in "safe cracker") is used to describe one who intentionally breaches a computer security system to gain unauthorized access either for profit, maliciously, for some altruistic purpose or cause, or simply for the challenge;[6]

[5.1] See Executive Summary: The State of Software Security—The Intractable Problem of Insecure Software (Sept. 22, 2010), available at http://www.veracode.com/images/pdf/soss/executive-summary-veracode-state-of-software-security-report-volume2.pdf (last visited Jan. 3, 2012) (stating that 57% of all applications fail to meet an acceptable level of security and that 81% of software applications supplied by third parties fail to meet acceptable security standards).

[5.2] See Internet Security Alliance, *Implementing the Obama Cyber Security Strategy via the ISA Social Contract Model* (2009).

[5.3] See Bowden, "The Enemy Within," Atlantic Magazine (June 2010), available at http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098 (last visited Aug. 13, 2011).

[5.4] See § 10.01[3][c] *infra* for a discussion of network intruders' lack of reasonable expectations of privacy under 18 U.S.C. § 2510(21)(A) (stating that "'computer trespasser' . . . means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer . . .").

[6] See § 9.01[2] *infra* for a discussion of liability for unauthorized access to protected computers under the Computer Fraud and Abuse Act (CFAA) pursuant to 18 U.S.C. § 1030(a)(1)-(a)(5). See § 11.01[3] *infra* for a discussion of the Digital Millennium Copyright Act (DMCA) (17 U.S.C. §§ 1201 *et seq.*) and how "access" has become a focal point in statutes addressing digital works and computer systems and is echoed in various sections of the Copyright Act (17 U.S.C. §§ 101 *et seq.*). See § 10.03[1] *infra* for a discussion of unauthorized access to stored communications under the Stored Communications Act pursuant to 18 U.S.C. § 2701(a) (stating that "[e]xcept as provided in subsection (c) of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is pro-

(3) *Script Kiddies:* "script kiddie" is a derogatory term used to describe one who uses existing and frequently well-known techniques or scripts to search for and exploit weaknesses in other networks.[7]

In general, network intruders may be associated with a variety of sources: foreign governments, criminals, terrorists, rival businesses, unfaithful employees, or simply individual pranksters and vandals.[7.1] Also, as discussed below, the methods employed by such individuals may be *either* technological *or* non-technological (i.e., "social engineering"). In the past, most computer criminals took advantage of widely known vulnerabilities that resulted from the lack of security features in popular operating systems and software,[8] simple-to-guess passwords,[9] and insecure network "ports."[10] Today,

---

vided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section"). See § 7.02[4] *infra* for a discussion of HIPAA's definition of "access" pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings. . . . Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to 'access' as used in this subpart, not as used in subpart E of this part.) . . .").

[7] Hackers view script kiddies with contempt because such individuals do nothing to advance the "art" of hacking, but rather draw law enforcement scrutiny of the entire hacker community.

[7.1] See, e.g., An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants (Nov. 2, 2007), available at http://www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf (last visited Jan. 20, 2009) (analyzing the commoditization of computer crime).

[8] Operating systems provide the foundation for system security. Mainstream operating systems, however, lack critical security features needed to enforce security policies. The companies that create and sell these systems usually learn about the vulnerabilities early and develop patches to cover them, but many customers, including huge corporations, government agencies, and individual users, do not learn about the patches until it is too late. As such, critics blame large computer manufacturers for failing to develop comprehensive policies and procedures for dealing with increasingly sophisticated attacks and failing to implement security regimes in their products. But see, § 9.01 *infra* for a discussion of insulation against civil liability under the CFAA in connection with the negligent design of software that results in a compromised network, 18 U.S.C. § 1030(g) (stating that "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware"). Also see, § 4.02[5] *infra* for a discussion of In the Matter of Microsoft Corp., File No. 012 3240 (Dec. 24, 2002), available at http://www.ftc.gov/os/2002/08/microsoftana.htm (last visited April 12, 2006) (addressing alleged false security promises relating to the level of online security employed to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers in connection with the Passport and Passport Wallet services).

[9] Attackers frequently take advantage of easy-to-guess passwords. This threat can be leveraged by both outside hackers and employees. Although the most secure passwords include random or partly random series of numbers, symbols and letters, many people use passwords that are easy to remember and often write them down for quick reference or use the same passwords for multiple functions. Even carefully chosen passwords, however, are vulnerable to sophisticated password-cracking programs. Some password crackers use word lists: lists of words, phrases or other combinations or letters, numbers and symbols that computer users often use as passwords. Others use "brute-force" techniques, which use every combination and permutation of characters, even nonsensical combinations. Unauthorized individuals who use or traffic in passwords may be subject to criminal liability. See § 1.01[5] *supra* for a discussion of authentication of network users as a means of restricting access to network resources. See § 9.01[2][c] *infra* for a discussion of I.M.S. Inquiry Management Systems v. Berkshire Information Systems, 2004 WL 345556 (S.D.N.Y. Feb. 23, 2004), which addresses the relation of the CFAA and

cross-platform applications and network operating systems are becoming increasingly popular targets (e.g., backup software, antivirus software, database software, media players, network devices, etc.)[11] Although network intruders generally do not possess a reasonable expectation of privacy when accessing networks, their communications may receive statutory protection in certain limited circumstances.[12]

[2]—Attack Modes

Experts generally recognize four different "attack modes," each of which will implicate different laws:

DMCA in connection with the use of passwords to gain unauthorized access to a protected computer that contains copyrighted works. See § 10.01[6] *infra* for a discussion of Fourth Amendment protection of shared computers under Trulock v. Freeh, 275 F.3d 391, 403-404 (4th Cir. 2001) (analogizing password-protected files to locked footlockers inside a bedroom, which the court had previously held to be outside the scope of common authority consent). See: § 7.03[2][a] *infra* for a discussion of HIPAA's security requirements: 45 C.F.R. § 164.308(a)(5)(i) (July 22, 2004) (stating that "Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management)."); 45 C.F.R. § 164.308(a)(5)(ii)(D) (July 22, 2004) (stating that "Password management (Addressable). Procedures for creating, changing, and safeguarding passwords."); 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [p]assword means confidential authentication information composed of a string of characters").

[10] Computer criminals typically use cyberspace to access computer systems via "ports," which act as points of entry into the network. In programming, a port is a "logical connection place" where a client program specifies a particular server program on a computer in a network. Computer systems are designed to have hundreds of ports for different types of uses such as electronic mail, remote log-in, or telnet. Most of these ports are not in use and remain closed, and can only be opened by a system administrator. System crackers can obtain the same privileges as a system administrator on a network, known as "superuser" or "root" status, and open one or more of these ports. Internet service providers (ISPs) may block access to "commonly exploited" communications ports on customers' computers. While it would not prevent all Internet threats, this could address the bulk of the problems. For example, the four ports, 135, 137, 139 and 445, are not necessary for most Internet use and are routinely disabled in securing (or "hardening") a system. See § 9.01[2][b] *infra* for a discussion of *United States v. Ivanov*, where the court determined that gaining root access constitutes "value" under the Computer Fraud and Abuse Act (CFAA). See § 10.01[6][c] *infra* for a discussion of the effect of system administrator consent to government actors' search in connection with criminal investigations and the Fourth Amendment.

[11] See 20 Most Critical Internet Security Vulnerabilities in 2005, SANS Institute (Nov. 22, 2005) (stating that thirteen of the top twenty vulnerabilities were in these two types of technology, which are among the least protected computer assets in many organizations), at http://www.sans.org/top20/ (last visited May 25, 2006). This shift from targeting operating systems to targeting popular applications may be the result of improved protections and automatic patching by operating system providers.

[12] See: § 10.01[3][c] *infra* for a discussion of United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (stating in *dicta* that "we seriously doubt that [a hacker whose communications were monitored by the system administrator of a victim network] is entitled to raise . . . objections to the evidence [under Title III]"); § 10.01[6][a] *infra* for a discussion of when courts may choose not to classify a network intruder as a "party to a communication" for the purposes of Title III's "non-government actor" exception to interception of communications and law enforcement's reliance upon the "computer crime investigation" exception when intercepting a network intruder's communications; § 10.02[2][c] *infra* for a discussion of the "non-government

(1) *Denial:* compromising an information system to stop it from operating;[13]

(2) *Deception:* inserting false data or malicious code to generate faulty results;[14]

---

actor" exception under 18 U.S.C. § 2511(2)(d) (stating that "[i]t shall not be unlawful under this chapter [18 U.S.C. §§ 2510 *et seq.*] for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State"); and the "computer crime investigation" exception under 18 U.S.C. § 2511(2)(i) (stating that "[i]t shall not be unlawful under this chapter [18 U.S.C. §§ 2510 *et seq.*] for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer; (II) the person acting under color of law is lawfully engaged in an investigation; (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser").

[13] See § 1.03[4] *infra* for a discussion of distributed denial of service attacks. See: §§ 9.01 and 9.03[1] *infra* for a discussion of criminal law theories that may apply in the event of a DDoS attack. Also see, Princeton's Center for Information Technology Policy, "Lest We Remember: Cold Boot Attacks on Encryption Keys," available at http://citp.princeton.edu.nyud.net/pub/coldboot.pdf (last visited June 13, 2008). A "cold boot attack" is a hardware attack that compromises encryption products that store their keys in DRAM. It is unique because it works during "powering off" and even "after a few minutes of shutdown."

[14] See § 9.01[2][a] *infra* for a discussion of liability under the Computer Fraud and Abuse Act, for unauthorized access to protected computers that results in the loss of information, pursuant to 18 U.S.C. § 1030(a)(2)(C) (imposing liability on whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information

(3) Destruction: physically or electronically destroying the target system;[15] and

(4) Exploitation: tapping into a system to steal data.[16]

Another aspect of network-based attacks is the offensive use of cyberattacks. For instance, in 2009 the United States began to articulate tactical and strategic goals cyberattacks might serve when protecting national interests, and considered the risks that the use of cyberattacks by the United States would entail.[16.1] Private companies must also consider such factors prior to engaging in "active defense" against cyberattackers by launching preemptive or retaliatory strikes.

Critics state that a cohesive national cyberwar strategy must be created that addresses both deterrence and preemption.[16.2] A deterrence strategy requires attribution (i.e., understanding the source of attack), location (i.e., knowing where a strike came from), response (i.e., the ability to respond,

---

from any protected computer if the conduct involved an interstate or foreign communication"). See § 2.04[2] *infra* for a discussion of corporate responsibility for ensuring the integrity of financial records pursuant to Pub. L. No. 107-204, § 302(a), 116 Stat. 745, 777 (2002) (codified in 15 U.S.C. § 7241) (stating that "[t]he Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that . . . based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report . . ."). See § 2.04[6] *infra* for a discussion of how the Sarbanes-Oxley Act applies to corporate information security.

[15] See § 9.01[2][c] *infra* for a discussion of liability under the CFAA for unauthorized access to protected computers that results in network damage pursuant to 18 U.S.C. § 1030(a)(5)(A)(ii) and (iii) (imposing liability on whoever "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage . . . [or] intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage").

[16] See § 9.01[2][b] *infra* for a discussion of liability under the CFAA for obtaining value via unauthorized computer access pursuant to 18 U.S.C. § 1030(a)(4) (imposing liability on whoever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period") and a discussion of *United States v. Ivanov*, in which the court determined that gaining root access constitutes "value" under the Computer Fraud and Abuse Act. See § 11.01[2][g] *infra* for a discussion of copyright infringement pursuant to 17 U.S.C. § 501(b) (stating that "[t]he legal or beneficial owner of an exclusive right under a copyright is entitled, subject to the requirements of section 411, to institute an action for any infringement of that particular right committed while he or she is the owner of it"), which requires a showing of unauthorized "copying" that may be inferred by demonstrating access to the work in question.

[16.1] See National Research Council of the National Academies, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (2009), available at http://www.nap.edu/openbook.php?record_id=12651&page=1 (last visited Jan. 6, 2010).

[16.2] See, e.g., "Mike McConnell On How to Win the Cyber-war We're Losing," The Washington Post (Feb. 28, 2010), available at http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (last visited July 8, 2010).

even if attacked first), and transparency (i.e., the enemy's knowledge of the target's capability and intent to counter with massive force). Official statements relating to a U.S. deterrence strategy must be backed up with practical policies and international legal agreements to define norms and identify consequences for destructive behavior in cyberspace. A preemption strategy, on the other hand, will require a more resilient cyberspace that can absorb attacks and quickly recover, as well as the ability to degrade, interdict and eliminate hostile forces' leadership and capabilities to mount cyber-attacks. Some argue that the National Security Agency (NSA)[16.3] is the appropriate agency in the United States with the legal authority, oversight and budget to address preemption. Any such leadership will require effective partnership with the private sector in order to facilitate information sharing to protect the nation's critical infrastructure.

[3]—Malicious Code

Programmers may create and distribute malicious code (also called "malware")[17] in order to access, damage and disrupt computer systems.[18] Such malicious code may be categorized as follows:

(1) Viruses: a virus is a program that copies itself into other programs and becomes active when a program is executed, moving on to infect other files;

(2) Worms: a worm is a "self-replicating" virus that does not alter files but resides in active memory and duplicates itself;[19]

(3) Trojans: a trojan or "trojan horse" is a program in which malicious code is contained inside apparently harmless programming or data in such a way that it can get control of, and possibly damage, the target system.[20]

[16.3] See § 12.01[1][h] *infra* for a discussion of the National Security Agency.

[17] Malicious applications can be broken down into five component parts/phases: (1) Propagation/Migration (i.e., local replication over a computer and/or network); (2) Payload (i.e., the mechanism through which malicious code causes damage or has an effect); (3) Signature (i.e., the pattern with which malicious code is detected by security software); (4) Detection Avoidance (i.e., the method by which malicious code attempts to hide itself); and (5) Trigger (i.e., the action through which malicious code is activated).

[18] See, e.g., § 7.02[4] *infra* for a discussion of HIPAA's security standards that address malicious code pursuant to 45 C.F.R. § 164.308(a)(5)(ii)(B) (July 22, 2004) (stating that "Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software."), and 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [m]alicious software means software, for example, a virus, designed to damage or disrupt a system").

[19] Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. In addition to raising computer crime issues, complicated legal theories are implicated when worms are designed to repair vulnerable third party networks without permission.

[20] It should be noted that sometimes a Trojan horse is widely redistributed as part of a computer virus. Also, trojans are increasing in sophistication, have been used to facilitate the spread of unsolicited commercial e-mail, and may eventually lead to claims based on "attractive

Trojan horses can also be used for ransom encryptions when blackmailers use high-level encryption to compromise the victim's private data on the Internet. Subsequently, blackmailers threaten public disclosure if their decryption software is not acquired.[21]

(4) Storm Attacks: A storm attack is a "combination of a worm, a Trojan horse, a bot, and a spam agent all blended into one." Multiple attack vectors are used "including DNS, Web, P2P, encryption, and several evasion techniques," making these particularly difficult to remove.[22]

Typically, organizations attempt to protect themselves from malware via the use of anti-virus software.[23] The release of malicious code may result in liability under various laws, including the Computer Fraud and Abuse Act (CFAA).[24]

[4]—Distributed Denial of Service Attacks

Distributed denial of service (DDoS) attacks use multiple compromised systems (called "zombies" or "botnets") to attack a single target, which causes a denial of service for users of the target system. The flood of incoming requests to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. DDoS attacks may target Web sites, routers,[25] and key hubs of the Internet's infrastructure such as the Domain Name System (DNS).[26] Such attacks constitute a crime under the

---

nuisance." In addition, some have argued that the presence of trojans may be used as a "plausible deniability" defense to computer crime allegations.

[21] Websense Security Labs, available at http://www.websense.com/securitylabs/docs/SecurityLabsReport_Q4_011808.pdf (last visited June 13, 2008). Also see, § 9.01[5] *infra* for discussion of CFAA's imposition of liability for a threat to damage a protected computer with intent to extort anything of value.

[22] Websense Security Labs, available at http://www.websense.com/securitylabs/docs/SecurityLabsReport_Q4_011808.pdf (last visited June 13, 2008).

[23] See § 1.04[3] *infra* for a discussion of anti-virus software. Critics state that anti-virus software presents an imperfect solution to network threats because, as discussed *supra*, several events must occur after malicious code is released into cyberspace in order for an "inoculation" to be issued by the anti-virus provider.

[24] See § 9.01[3] *infra* for a discussion of liability under the CFAA for unauthorized program transmission pursuant to 18 U.S.C. § 1030(5)(A)(i) (imposing liability on whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer").

[25] A router is a device or, in some cases, software, that determines the next network point to which a packet should be forwarded toward its destination. Compromised routers can be used to conduct "man-in-the-middle" attacks, altering data that are sent or "injecting" phony traffic into the network. Routers can also be targeted by distributed denial of service attacks. These problems can be mitigated through the use of routing filters and cryptographic authentication.

[26] A domain name is a meaningful and easy-to-remember method for an Internet address. Essentially, the domain name system is the way that Internet domain names are located and translated into Internet Protocol addresses. Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority. The root server system is the way that an authoritative master list of all top-level domain names (i.e., .com, .net, .org, etc.) is

CFAA[27] and may require the assistance of law enforcement.[28] In 2009, groups that monitor the frequency and magnitude of DDoS attacks noted a sharp increase in particularly virulent attacks that target critical Internet infrastructure systems, which may be a prelude to a larger scale attack against key resources.[28.1] Targets have successfully argued that courts should issue temporary restraining orders to cut off Internet domains believed to be hijacked by criminals.[28.2]

---

maintained and made available to all routers. The central or "A" server is operated by Network Solutions, Inc., the company that originally managed all domain name registration, and the master list of top-level domain (TLD) names is kept on the A server. This list is replicated daily to twelve other geographically dispersed file servers that are maintained by an assortment of agencies. The most potentially devastating DDoS attacks would be directed at Network Access Points and Domain Name Servers, which consists of thirteen file servers. Simultaneously targeting such points could cause a cascading effect, bringing all Internet communications to a halt. See § 11.04[1][c][i] *infra* for a discussion of domain names in the context of trademark infringement claims. See § 11.04[2] *infra* for a discussion of the Anti-cybersquatting Consumer Protection Act's definition of "domain name" pursuant to 15 U.S.C. § 1127 (stating that "[t]he term 'domain name' means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet"). See § 9.03[2] *infra* for a discussion of Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003) (holding that the tort of conversion equally applies to real property and intangible property such as a domain name and permitting the registrant to seek redress from the domain name registrar for negligent transfer). See § 12.02[4] *infra* for a discussion of ICANN's role in regulating cyberspace. See § 1.01[2] *supra* for a discussion of the computer systems that make up society's critical infrastructure.

[27] See § 9.01[3] *infra* for a discussion of 18 U.S.C. § 1030(5)(A)(i) (imposing liability on whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer").

[28] See § 10.04[3][d] *infra* for a discussion of 18 U.S.C. § 3125(a)(1) (stating that "[n]otwithstanding any other provision of this chapter [18 U.S.C. §§ 3121 *et seq*.], any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that . . . an emergency situation exists that involves . . . an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year . . . that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained . . . may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title").

[28.1] See Shadow Server DDoS Chart, available at http://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSCharts (last visited Dec. 2, 2009).

[28.2] See, e.g., Microsoft v. John Does 1-27, 1:10CV156 (E.D. Va. Feb. 22, 2010), available at http://www.microsoft.com/presspass/events/rsa/docs/Complaint.pdf (last visited April 27, 2010) (granting Microsoft's temporary restraining order cutting off 277 Internet domains believed to be run by criminals as the Waledac bot).

[5]—Social Engineering

"Social engineering" refers to non-technological security threats that typically involve the use of disguise and diversion in order to extract proprietary information from businesses and consumers.[29] For example, social engineers attempt to infiltrate systems by persuading unwitting staff to part with vital information, including log-in names and passwords.[30] Social engineers typically research their targets before attacking in order to understand the corporate culture, organizational structure, information access controls, and location of target information.[31] As part of a test, one company used freely available but infected USB flash drives to lure employees to insert the USB flash drives into their workstation computers. The insertion of even one of these USB Flash drives into a workstation computer caused the entire network to be infected.[32] Another form of social engineering attack is "robot chatters." It tricks humans into confusing bots as potential suitors and collects valuable personal information rather than attacking the system flaws.[33]

---

[29] See, e.g.: § 5.07 *infra* for a discussion of the Gramm-Leach-Bliley Act's (GLBA's) prohibition of "pretexting" under Pub. L. No. 106-102, 113 Stat. 1338 Subtitle B—Fraudulent Access to Financial Information (Nov. 12, 1999) (codified in 15 U.S.C. §§ 6821-6827); The Gramm-Leach-Bliley Act: Pretexting, available at http://www.ftc.gov/privacy/privacyinitiatives/pretexting.html (last visited April 14, 2006) (stating that "[t]he Gramm-Leach-Bliley Act prohibits 'pretexting,' the use of false pretenses, including fraudulent statements and impersonation, to obtain consumers' personal financial information, such as bank balances. This law also prohibits the knowing solicitation of others to engage in pretexting.").

[30] See § 7.03[2][a] *infra* for a discussion of HIPAA's administrative safeguards: 45 C.F.R. § 164.308(a)(5)(i) (July 22, 2004) (stating that "Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management)."); 45 C.F.R. § 164.308(a)(5)(ii)(D) (July 22, 2004) (stating that "Password management (Addressable). Procedures for creating, changing, and safeguarding passwords."); 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [p]assword means confidential authentication information composed of a string of characters"). See § 5.06[3] *infra* for a discussion of bank requirements to address potential social engineering in their security policies under the GLBA's Bank Safeguards Rule pursuant to 66 Fed. Reg. 8616, § III.C.1.a (Feb. 1, 2001) (stating that "[y]ou shall . . . [d]esign your information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of your activities. You must consider whether the following security measures are appropriate for you and, if so, adopt those measures you conclude are appropriate . . . [a]ccess controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means. . . .").

[31] For example, on February 15, 1995 Kevin Mitnick was the first person to be convicted by the FBI of gaining access to an interstate computer network for criminal purposes. Mr. Mitnick was able to take control of U.S. telecommunications operator Sprint's switching equipment by calling the company and posing as an engineer from switch maker Nortel Networks. Sprint provided log-in names and passwords for the switches so that the "Nortel engineer" could perform remote maintenance.

[32] Johansson, Security Watch, "Island Hopping: The Infectious Allure of Vendor Swag" (Jan. 2008), Microsoft TechNet, at http://technet.microsoft.com/en-us/magazine/cc137730.aspx (last visited July 28, 2008).

[33] Fried, "Pillow talking bots latest Russian malware threat" (Dec. 10, 2007), available at http://www.zdnet.com.au/news/security/soa/Pillow-talking-bots-latest-Russian-malware-threat/0,130061744,339284439,00.htm (last visited July 28, 2008).

Social networking sites are increasingly used by identity thieves to facilitate social engineering and spear phishing.[34] For example, the data provided by social network users may be used to gain access to proprietary systems or cross-referenced with other data to open credit card accounts, obtain birth certificates, etc. Programs are readily available on the Internet that automate the process of collecting and cross-referencing such data. In addition, software has been created to facilitate spear phishing and automate targeted attacks on the users' followers.

---

[34] See § 9.05 *infra* for a discussion of identity theft and § 10.01[6[e] *infra* for a discussion of social network searches.

§ 1.04 Network Security

Various technologies are employed to control digital assets in networked environments. For instance, there are technological methods to secure both data and the systems on which data reside. These technologies are bolstered by laws that offer owners remedies against unauthorized access to (and use of) systems and data, and by information security policies that establish proper security practices within an organization.[1]

[1]—Encryption

Encryption is the conversion of data into a form (also called "ciphertext") that cannot be easily understood by unauthorized recipients.[2] Decryption, on the other hand, is the process of converting encrypted data back into their original, understandable form through the use of a "decryption key" (this unencrypted text is sometimes called "cleartext"). This key is typically an algorithm that "unlocks" the encryption algorithm. Alternatively, software may be used to "break" the cipher. Technologies such as the Public Key Infrastructure (PKI) are evolving to facilitate encryption by users of unsecured public networks (i.e., the Internet) to exchange securely data and money through the use of a "public" and "private" cryptographic key pair that is obtained and shared through a trusted authority.

In certain circumstances, regulated entities must protect the security and confidentiality of customers' non-public personal information and guard against threats to such data. Regulators in certain industries are increasingly citing entities for failing to encrypt customer information.[3] In order to mitigate the risk associated with regulatory actions, organizations should be sure to encrypt sensitive information while it is both in transit and at rest.

Various laws govern the export of encryption technology to foreign countries, protect unauthorized interception of communications in general,[4] and

---

[1] See: § 3.01 *infra* for a discussion of the information security policies organizations must implement to secure computer systems; § 1.01[5] *supra* for a discussion of authentication technology; § 9.05[5][j] *infra* for a discussion of the Federal Trade Commission's (FTC's) obligations under the Fair and Accurate Credit Transaction Act (FACTA) to research various technological measures that may be used to prevent identity theft pursuant to Pub. L. No. 108-159, 117 Stat. 1952, § 157(a) (Dec. 4, 2003) (stating that "[t]he Secretary of the Treasury shall conduct a study of the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction").

[2] See, e.g., § 7.02[4] *infra* for a discussion of the Health Insurance Portability and Accountability Act's (HIPAA's) definition of "encryption" as set forth in 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [e]ncryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key").

[3] See § 5.06[1][e] *infra* for a discussion of In re James B. Nutter & Co., FTC File No. 0723108 (June 12, 2009) (issuing a complaint against a non-bank mortgage lender for safeguards deficiencies, including storing personal information in "clear readable text").

[4] See § 10.02[2][a] *infra* for a discussion of the different types of communications governed by the Wiretap Act (Title III) under 18 U.S.C. § 2510(1) (stating that "'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission

prohibit unauthorized decryption of encrypted data in certain circumstances.[5] Also, information security laws are evolving to encourage organizations to encrypt sensitive data, by imposing security breach notification duties in the event of unauthorized access to unencrypted personal information.[6] In addition,

---

of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce"), 18 U.S.C. § 2510(18) (stating that "'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception"), 18 U.S.C. § 2510(2) (stating that "'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication"), and 18 U.S.C. § 2510(12) (stating that "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds"). But see, § 10.05[3] *infra* for a discussion of encryption limitations under the Communications Assistance for Law Enforcement Act (CALEA) pursuant to 47 U.S.C. § 1002(b)(3) (stating that "[a] telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication").

[5] See § 11.01[3][a] *infra* for a discussion of the Digital Millennium Copyright Act's (17 U.S.C. §§ 1201 *et seq*.) anti-circumvention protections for copyrighted material pursuant to 17 U.S.C. § 1201(a)(1)(A) (providing that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title"). But see: §§ 11.01[3][e] and [f] *infra* for a discussion of 17 U.S.C. § 1201(g)(2) (stating that "[n]otwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if (A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work; (B) such act is necessary to conduct such encryption research; (C) the person made a good faith effort to obtain authorization before the circumvention; and (D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986 [18 U.S.C. § 1030(a)-(c), (e), (f)]"). Also see, § 11.01[2][g][vii] *infra* for a discussion of 17 U.S.C. § 117(a) (stating that "[n]otwithstanding the provisions of section 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided: (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or (2) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful").

[6] For example, encrypted account numbers are excluded from the Gramm-Leach-Bliley Act's (GLBA's) prohibitions relating to the disclosure of customer account numbers so long as the financial institution does not provide the recipient with the means to decrypt the number. Also, the Securities and Exchange Commission (SEC) addresses the issue of account number transmission in its Privacy Rule. See § 5.02[4] *infra* for a discussion of 17 C.F.R. § 248.12(c) (stating that "[a]n account number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as you do not provide the recipient with a means to decode the number or code"); and 17 C.F.R. § 248 (comments) (stating that "[m]any

individuals may be protected from disclosing passwords to encrypted files in certain situations.[7] The challenge for regulators is to balance national security[8] and privacy[9] against the use of encryption technology. The National Security Agency (NSA),[10] for example, which regulates some uses of encryption, must balance the interests of security in the use of so-called "strong" encryption (i.e., ciphers that are essentially unbreakable without a decryption key)[11] against

---

commenters urged us to exercise our exemptive authority to permit the transmission of account numbers in encrypted form or to clarify that the prohibition applies only to disclosure to non-affiliated third parties who are not subject to one of the exceptions under sections 248.13, 248.14, or 148.15. Several commenters noted that financial institutions frequently use encrypted account numbers and other internal identifiers of an account to ensure that a consumer's instructions are properly executed. The inability to continue using these internal identifiers would increase the likelihood of errors in processing a consumer's instructions. These commenters also noted that if internal identifiers are not used, a consumer would have to provide an account number in order to ensure proper handling of a request. This procedure could expose the consumer to a greater risk than would the use of an internal tracking system that preserves the confidentiality of a number that may be used to access the account. One commenter also noted that customer account numbers are protected by strict contractual confidentiality provisions. We believe an encrypted account number without the key is not the same as the number itself and thus falls outside the prohibition in section 502(d). The GLBA focuses on numbers that provide access to an account. The encrypted number, however, operates as an identifier attached to an account for internal tracking purposes only, and without the key does not permit someone to access an account. For this reason the final rule clarifies that an account number, or similar form of access number or access code, does not include a number or code in an encrypted number form, as long as the financial institution does not provide the recipient with the means to decrypt the number."). See § 5.05 *infra* for a discussion of the SEC's Privacy Rule that implements the GLBA's provisions relating to notice and disclosure requirements pursuant to 17 C.F.R. § 248 (June 29, 2000). It should be noted that, unlike the Federal Trade Commission, the SEC issued both its Privacy Rule and Safeguards Rule within the same final rule. See § 5.06[2] *infra* for a discussion of the SEC's implementation of the GLB Act's information security requirements. See § 5.06[3] *infra* for a discussion of the Bank Safeguards Rule that requires regulated banks to consider encryption as part of their security program pursuant to 66 Fed. Reg. 8616, § III.C.1.c (Feb. 1, 2001) (stating that "[y]ou shall . . . [d]esign your information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of your activities. You must consider whether the following security measures are appropriate for you and, if so, adopt those measures you conclude are appropriate . . . [e]ncryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access. . . ."). See § 12.01[1][l] *infra* for a discussion of the SEC's role in regulating information security.

[7] See § 10.01[3][b] *infra* for a discussion of In re Boucher, 2007 WL 4245473 (D. Vt. Nov. 29, 2007) (holding that requiring defendant to reveal or enter the encryption code he used to protect his alleged child pornography triggered his Fifth Amendment rights, which prevent compelled disclosure of incriminating information of a testimonial nature).

[8] See § 1.01[2] *infra* for a discussion of the importance of information security laws in securing critical infrastructures.

[9] See: Chs. 4-8 *infra* for a discussion of the various laws that protect privacy.

[10] See § 12.01[1][h] *infra* for a discussion of the National Security Agency's role in regulating encryption technology.

[11] Some governments view strong encryption as a potential tool for criminal activity. For instance, the United States has previously attempted legislatively to require a "key-escrow" arrangement. In such a "government escrow" relationship, all users would be required to provide the government with a copy of their decryption key. These decryption keys would be stored in a secure place to be used only by authorities if backed by a court order. Critics of government escrow argue that criminals could infiltrate such a key-escrow database and illegally obtain, steal, or alter the keys. See § 12.01[1][b] *infra* for a description of the Office of Management and Budget's (OMB's) report card of government system security.

commercial development interests. The Bureau of Industry and Security (BIS) also regulates the export of encryption technologies to foreign countries.[12] In addition, agencies such as the National Institute of Standards and Technology (NIST) are tasked with determining appropriate encryption levels for government systems and data.[13] States have enacted laws that penalize businesses for failing to encrypt personal information.[14]

---

[12] See § 12.01[1][n] *infra* for a discussion of the BIS's role in administering restrictions on encryption export. Export and re-export controls on commercial encryption products are administered by the BIS. Rules governing exports and reexports of encryption items are found in the Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774. Sections 740.13, 740.17 and 742.15 of the EAR are the principal references for the export and re-export of encryption items.

[13] See 69 Fed. Reg. 142 (July 26, 2004) (determining that the strength of the DES algorithm is no longer sufficient to protect adequately federal government information). See § 12.01[1][n] *infra* for a discussion of NIST. See § 8.07[3][c] *infra* for a discussion of the Federal Information Security Management Act's (FISMA's) creation of a federal information security incident center pursuant to Pub. L. No. 107-347, 116 Stat. 2899, 2946-2954, § 301(b) (Dec. 17, 2002) (codified in 44 U.S.C. § 3546) (stating that "[c]hapter 35 of title 44, United States Code, is amended by adding at the end the following . . . 'Sec. 3546. Federal information security incident center. (a) In General. The Director shall ensure the operation of a central Federal information security incident center . . . (4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.'"). See § 8.08 *infra* for a discussion of Pub. L. No. 107-347, 116 Stat. 2899, 2956, § 302(a) (Dec. 17, 2002) (codified in 40 U.S.C. § 11331) (stating that "Section 11331 of title 40, United States Code, is amended to read as follows: 'Sec. 11331. Responsibilities for Federal information systems standards. (a) Standards and Guidelines. (1) Authority to prescribe. Except as provided under paragraph (2), the Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(a)), prescribe standards and guidelines pertaining to Federal information systems.'"); Pub. L. No. 107-347, 116 Stat. 2899, 2956, § 302(a) (Dec. 17, 2002) (codified in 40 U.S.C. § 11331) (stating that "Section 11331 of title 40, United States Code, is amended to read as follows: 'Sec. 11331. Responsibilities for Federal information systems standards. . . . (b) Mandatory Requirements. (1) Authority to make mandatory. Except as provided under paragraph (2), the Secretary shall make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of Federal information systems.'"); and Pub. L. No. 107-347, 116 Stat. 2899, 2956-2957, § 302(a) (Dec. 17, 2002) (codified in 40 U.S.C. § 11331) (stating that "Section 11331 of title 40, United States Code, is amended to read as follows: 'Sec. 11331. Responsibilities for Federal information systems standards. . . . (d) Exercise of Authority. To ensure fiscal and policy consistency, the Secretary shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget.'"). See § 8.08[1] *infra* for a discussion of Pub. L. No. 107-347, 116 Stat. 2899, 2957, § 303(a) (Dec. 17, 2002) (codified in 15 U.S.C. § 278g-3) (stating that "Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), is amended by striking the text and inserting the following: '(a) In General. The Institute shall (1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems . . .'").

[14] See Nev. Rev. Stat. § 597.970 (stating businesses shall not "transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission").

[2]—Firewalls

Firewalls are sets of related programs that protect networks from external users and may control user access to external resources.[15] A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming data (which may contain malicious code) can penetrate private network resources.[16] Basically, a firewall examines each network packet[17] and determines whether to forward it toward its destination.[18] There are several firewall screening methods. For instance, requests are

---

[15] See § 9.01[2] *infra* for a discussion of liability for unauthorized access to protected computers under the CFAA pursuant to 18 U.S.C. § 1030(a)(1)-(a)(5). See § 11.01[3] *infra* for a discussion of the Digital Millennium Copyright Act (17 U.S.C. §§ 1201 *et seq*.) and how "access" has become a focal point in statutes addressing digital works and computer systems and is echoed in various sections of the Copyright Act (17 U.S.C. §§ 101 *et seq*.). See § 10.03 *infra* for a discussion of unauthorized access to stored communications under the Stored Communications Act pursuant to 18 U.S.C. § 2701(a) (stating that "[e]xcept as provided in subsection (c) of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section"). See § 7.02[4] *infra* for a discussion of the definition of "access" under HIPAA pursuant to 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings. . . . Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to 'access' as used in this subpart, not as used in subpart E of this part.) . . .").

[16] See § 9.01[3] *infra* for a discussion of liability in connection with malicious code under the CFAA pursuant to 18 U.S.C. § 1030(a)(5)(A)(i) and 18 U.S.C. § 1030(a)(5)(B)(ii). See § 7.02[4] *infra* for a discussion of 45 C.F.R. § 164.308(a)(5)(ii)(B) (July 22, 2004) (stating that "Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software."), and 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [m]alicious software means software, for example, a virus, designed to damage or disrupt a system"). See § 1.03[3] *supra* for a discussion of the technical aspects of malicious software.

[17] When computers that are connected to cyberspace communicate with each other, they break down messages into discrete chunks known as "packets," and then send each packet out to its intended destination. Every packet contains addressing information in the "header" of the packet (e.g., like the "to" and "from" addresses on an envelope), followed by the content of the message (e.g., like a letter inside an envelope). E-mail messages consist of sets of headers that contain addressing and routing information generated by the mail program, followed by the actual contents of the message authored by the sender. The addressing and routing information includes the e-mail address of the sender and recipient, as well as information about when and where the message was sent on its way (roughly analogous to the postmark on a letter). See § 10.04[3] *infra* for a discussion of court orders to install monitoring devices pursuant to the Pen Register and Trap and Trace Devices Act under 18 U.S.C. § 3122. The Pen/Trap statute permits law enforcement to obtain the addressing information of Internet e-mails (with the exception of the subject line, which can contain content) using a court order, in the same manner that court orders permit government agents to obtain addressing information for phone calls and individual Internet "packets" using a court order. Conversely, the interception of e-mail contents, including the subject line, requires careful compliance with Title III.

[18] See § 1.01[1] *supra* for a discussion of packet-based communications in cyberspace. Essentially, each computer on the Internet (known as a "host") has at least one Internet Protocol (IP) address that uniquely identifies it from all other computers on the Internet. When data are sent or received over the Internet, the message gets divided into little chunks called "packets." Each of these packets contains both the sender's IP address and the receiver's IP address.

sometimes screened to ensure that they come from acceptable (i.e., previously identified) domain name and Internet Protocol addresses.[19]

[3]—Anti-Virus Software

Anti-virus software searches computer systems for any known or potentially malicious code[20] by "inoculating" networks against known viruses. Typically, anti-virus software development involves the following cycle:

(1) *Infection*: An end user is infected with the specific virus;
(2) *Alert*: The user must alert the anti-virus vendor;
(3) *Signature Updates*: The vendor must provide signature updates to address the vulnerability; and
(4) *Download*: The end user must download the update.

It is possible, therefore, for a well-crafted virus to spread before the anti-virus vendor is able to provide the identifying signature to end-users.[21] Anti-virus software providers are entitled to immunity under the safe harbor provisions of the Communications Decency Act (CDA).[22]

Vendors may be immune from liability under Section 230(c)(2)(B) of the Communications Decency Act for classifying software as "malware" and

---

[19] See § 1.01[1] *supra* for a discussion of Internet protocols such as Transmission Control Protocol (TCP), which uses a set of rules to exchange messages with other Internet points at the information packet level, and Internet Protocol (IP), which uses a set of rules to send and receive messages at the Internet address level. Additional protocols are usually packaged with a TCP/IP suite, including the Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP), each with defined sets of rules to use with corresponding programs elsewhere on the Internet, and Internet Protocol (IP), which is the method by which data are sent from one computer to another on the Internet. Each computer on the Internet (known as a "host") has at least one IP address that uniquely identifies it from all other computers on the Internet. When data are sent or received over the Internet, the message gets divided into little chunks called "packets." Each of these packets contains both the sender's IP address and the receiver's IP address.

[20] See § 9.01[3] *infra* for a discussion of liability in connection with malicious code under the CFAA pursuant to 18 U.S.C. § 1030(a)(5)(A)(i) and 18 U.S.C. § 1030(a)(5)(B)(ii). See § 7.02[4] *infra* for a discussion of HIPAA's security standards that address malicious code pursuant to 45 C.F.R. § 164.308(a)(5)(ii)(B) (July 22, 2004) (stating that "Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software."); 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [m]alicious software means software, for example, a virus, designed to damage or disrupt a system"). See § 1.03[3] *supra* for a discussion of the technical aspects of malicious software.

[21] See § 1.03[3] *supra* for a discussion of a malware lifecycle, which can be broken down into five component parts/phases: (1) Propagation/Migration (i.e., local replication over a computer and/or network); (2) Payload (i.e., the mechanism through which malicious code causes damage or has an effect); (3) Signature (i.e., the pattern with which malicious code is detected by security software); (4) Detection Avoidance (i.e., the method by which malicious code attempts to hide itself); and (5) Trigger (i.e., the action through which malicious code is activated).

[22] See Zango, Inc. v. Kaspersky Lab, Inc., No. C07-0807-JCC (W.D. Wash. Aug. 28, 2007) (holding that a provider of anti-virus/anti-malware software is an "access software provider" that enables users to filter, screen, allow or disallow content, exactly as contemplated by 47 U.S.C. § 230(c)(2)).

blocking installation or interfering with the operation of such software.[23] Vendors that offer customers online access to update servers may be more likely to enjoy this protection because providing "access by multiple users to a computer server" fits within the meaning of the statutory definition of an "interactive service provider."

Regulators in certain industries have begun to focus on safeguards-related enforcement actions. In many circumstances, regulated entities must protect the security and confidentiality of customers' non-public personal information and guard against threats to such data. Regulators are increasingly characterizing network defense methods such as anti-virus software as "basic safeguards" that must be used to prevent unauthorized access to network resources.[24]

[4]—Intrusion Detection Systems

Intrusion detection systems (IDS) use passive sensors to inspect Internet traffic entering a system in order to identify malicious code and unauthorized network access.[25] IDS may be capable of alerting system owners in real time to the presence of malicious or potentially harmful activity in network traffic and provide correlation and visualization of the derived data. In essence, IDS provides a real-time picture of user access to network resources that allow network administrators to mitigate damage in the event of a network breach.[26] IDS may also be used in conjunction with "honey pots" (i.e., areas of a network used to "lure" unauthorized users for the purposes of detection) to eliminate "false positives." Intrusion detection technology is rapidly advancing into intrusion protection systems (IPS). This technology combines pattern matching, protocol analysis, pre-emptive behavioral inspection, anomaly detection, and firewall blocking to detect and block online threats.

---

[23] See Zango v. Kaspersky Lab, Inc., 2009 U.S. App. LEXIS 13682 (9th Cir. June 25, 2009) (holding that § 230(c)(2)(B) immunity for "good Samaritan" blocking and screening of offensive material is available, not only to Web site operators and Internet service providers who provide access to content, but also to developers that provide access to tools that filter content).

[24] See § 5.06[2] *infra* for a discussion of In re Commonwealth Equity Services, Securities Exchange Act Rel. No. 60733 (Sept. 29, 2009) (issuing a cease-and-desist order against an investment adviser for failing to implement adequate safeguards).

[25] See, e.g., § 7.03[2][a] for a discussion of HIPAA's administrative safeguards provisions requiring intrusion detection pursuant to: 45 C.F.R. § 164.308(a)(1)(i) (July 22, 2004) (stating that "[a] covered entity must, in accordance with § 164.306 . . . Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations."); 45 C.F.R. § 164.308(a)(1)(ii)(D) (July 22, 2004) (stating that "Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."); and 45 C.F.R. § 164.304 (July 22, 2004) (stating that "[a]s used in this subpart, the following terms have the following meanings . . . [s]ecurity incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system").

[26] See: § 10.01[6][d] *infra* for a discussion of the issues that arise when monitoring employer networks; §§ 3.01 and 3.03 *infra* for a discussion of the policies organizations implement to mediate the damage that results from security breaches.

As part of the Comprehensive National Cybersecurity Initiative,[27] the Department of Homeland Security ("DHS") is in the process of establishing an intrusion-detection system known as EINSTEIN 2.0.[28] This system is used to detect unauthorized network intrusions and data exploitations against federal systems, which provides greater situational awareness regarding malicious network activities. The government's use of such systems raises issues relating to the Fourth Amendment,[29] the Wiretap Act,[30] the Foreign Intelligence Surveillance Act,[31] the Stored Communications Act,[32] and the Pen/Trap Act.[33] Government use of IDS may comply with such laws provided that log-on banners or computer-user agreements are consistently adopted, implemented and enforced by the government.[34] It has been argued, for instance, that the need for coordinated situational awareness regarding all intrusions and exploitations against government networks is inconsistent with the requirement to obtain a warrant based upon probable cause prior to monitoring.[35] Such requirements are inapplicable to a search that serves special governmental needs, beyond the normal need for law enforcement. In addition, information acquired or shared by DHS in the course of EINSTEIN 2.0 operations is subject to minimization procedures designed to minimize the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons.[36] The important governmental interest in protecting

---

[27] See § 10.04[7] *infra* for a discussion of the Comprehensive National Cybersecurity Initiative.

[28] See § 10.04[3][c] *supra* for a discussion of EINSTEIN 1.0 and "packet header" analysis.

[29] See: § 10.01[1] *infra* for a discussion of expectations of privacy that are afforded to different types of Internet communications; § 10.01[2][a] *infra* for a discussion of warrantless search; § 10.01[2][c] *infra* for a discussion of reasonableness of searches; § 10.01[3][a] *infra* for a discussion of electronic search of in-transit communications; § 10.01[3][c] *infra* for a discussion of computer trespassers' expectations of privacy; § 10.01[4][c] *infra* for a discussion of warrant particularity requirements; § 10.01[6][d] *infra* for a discussion of consent in the context of workplace searches.

[30] See: § 10.02[2][b][i] *infra* for a discussion of interception and network monitoring technology under Title III; § 10.02[2][b][iii] *infra* for a discussion of interception devices under 18 U.S.C. §§ 2510-2522; § 10.02[2][c][i] *infra* for a discussion of the Service Provider Exception under 18 U.S.C. § 2511(2)(a)(i) (allowing service providers to use communications in the normal course of business); § 10.02[3] *infra* for a discussion of electronic communication service provider liability for disclosure of in transit communications under 18 U.S.C. § 2511(3)(a) (generally prohibiting service providers from voluntarily disclosing the contents of communications).

[31] 50 U.S.C. §§ 1801 *et seq*.

[32] See § 10.03[2] *infra* for a discussion of prohibitions against voluntary disclosure by electronic service providers pursuant to 18 U.S.C. § 2702(a)(1) and remote storage providers under 18 U.S.C. § 2702(a)(2).

[33] See § 10.04 *infra* for a discussion of 18 U.S.C. §§ 3121-3127.

[34] See § 3.05 *infra* for a discussion of monitoring policies and associated liability protections.

[35] See § 10.01[2][a] *supra* for a discussion of warrantless search under the special needs doctrine.

[36] *Cf*., In re Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (noting importance of minimization procedures in holding that electronic surveillance pursuant to FISA was reasonable under the Fourth Amendment).

federal systems from malicious actors, therefore, may outweigh the limited impact on potential privacy rights of users of such systems.[37] Analyzing compliance with these laws will become difficult as government collaborates with system owners to implement similar protections on private networks.[38] This public-private collaboration will raise complicated issues regarding legal compliance[39] and government regulatory authority,[40] and increase the importance of immunity for participating organizations.[41]

[5]—Filtering

Content filtering programs limit access to pre-determined types of data that reside on external systems.[42] For instance, pen trap technology should consider filtering systems that produce only dialed numbers, as opposed to representing the call content.[43] Many employers use content filtering programs to limit access to offensive material and avoid potential liability in employee harassment claims.[44] When implementing such filters, organiza-

---

[37] See LEGAL ISSUES RELATING TO THE TESTING, USE, AND DEPLOYMENT OF AN INTRUSION-DETECTION SYSTEM (EINSTEIN 2.0) TO PROTECT UNCLASSIFIED COMPUTER NETWORKS IN THE EXECUTIVE BRANCH, Office of Legal Counsel to the President (Jan. 9, 2009), available at http://www.justice.gov/olc/2009/e2-issues.pdf (last visited Sept. 4, 2010).

[38] See § 1.04[7] *infra* for a discussion of the National Strategy for Trusted Identities in Cyberspace (April 2011), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (last visited July 20, 2011).

[39] See § 10.01[5] *infra* for a discussion of the Fourth Amendment in the context of surveillance conducted by private and government actors. Also see, § 10.02[2][c] *infra* for a discussion of the Wiretap Act's exceptions that relate to surveillance conducted by government actors (i.e., those acting under "color of law") *vis-à-vis* private actors (i.e., those not acting under "color of law") as addressed by 18 U.S.C. § 2511(2)(c) and (d).

[40] See: § 12.01[1][d] *infra* for a discussion of the Department of Justice's (DOJ) role in protecting cyberspace; § 12.01[1][h] *infra* for a discussion of the National Security Agency's role in regulating cyberspace; § 12.01[1][i] *infra* for a discussion of the Department of Defense's (DOD) role in protecting cyberspace.

[41] See § 9.03[4] *supra* for a discussion of official immunity and Murray v. Northrop Grumman Information Technology, 444 F.3d 169, 174 (2d Cir. 2006) (granting absolute immunity to a government contractor from suit for state tort actions arising from sharing of information with federal agencies and dismissing appellants' claims of negligent misrepresentation and defamation).

[42] See § 11.01[3][e] *infra* for a discussion of the DMCA's exemption from liability for acts meant to further the development of filtering software that restricts minor's access to digital content, found in 17 U.S.C. § 1201(h) (stating that "[i]n applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which (1) does not itself violate the provisions of this title; and (2) has the sole purpose to prevent the access of minors to material on the Internet").

[43] See In the Matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, No. H-06-356m (5th Cir. 2006) (stating that a search warrant is required to collect the content of a telephone call, even if the content involves "dialed digits like bank account numbers, social security numbers or prescription refills"). Also see: § 10.01 *supra* for a discussion of warrants; § 10.04 *infra* for a discussion of the Pen Register and Trap and Trace Devices Act.

[44] See § 3.03[2] *infra* for a discussion of potential liability for sexual harassment in hostile workplaces.

tions should balance these interests against unwarranted use restrictions on end users.

[6]—Vulnerability Research

Attackers typically exploit vulnerabilities to take control of computers and networks. Vulnerabilities are software mistakes in specification design and programming. These vulnerabilities may remain dormant in software systems for years and, once discovered, they can be used to attack systems. Although security-patching attempts to eliminate known vulnerabilities, many systems do not get patched and this causes known, exploitable vulnerabilities to proliferate on the Internet. New vulnerabilities may be sold on the black market, used to blackmail the vendor with disclosure, or simply published without regard to consequences. Most important, the mere fact that a vulnerability is known by someone increases the risk to every user of that software. These factors have required the technical community to begin analyzing whether it is ethical to research new vulnerabilities.[45] These ethical discussions may guide future laws that permit (or prohibit) such vulnerability research.

[7]—National Cybersecurity

Shortly after taking office, President Obama ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America's critical infrastructure.[46] In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review, including the selection of an Executive Branch Cybersecurity Coordinator who will have regular access to the President.[47] The activities that implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI)[48] launched by President George W. Bush in the 2008 National Security Presidential Directive 54 and Homeland Security Presidential Directive 23. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader updated national U.S. cybersecurity strategy.

The CNCI consists of several mutually reinforcing initiatives designed to help secure the United States in cyberspace. These initiatives include:

(1) Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.[49]

---

[45] See Information Security Magazine, "Face-Off: Is vulnerability research ethical?" (May 2008), available at http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1313268,00.html (last visited Dec. 2, 2009).

[46] See § 1.01[2] *supra* for a discussion of the national infrastructure.

[47] See § 12.01[1] *infra* for a discussion of the Executive Branch's role in information security.

[48] See http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (last visited April 27, 2010).

[49] The Trusted Internet Connections (TIC) initiative, headed by the Office of Management and Budget and the Department of Homeland Security, covers the consolidation of the federal

(2) Deploy an intrusion detection system of sensors across the federal enterprise.[50]

(3) Pursue deployment of intrusion prevention systems across the federal enterprise.[51]

(4) Coordinate and redirect research and development efforts.[52]

(5) Connect current cyber operations centers to enhance situational awareness.[53]

(6) Develop and implement a government-wide cyber counterintelligence (CI) plan.[54]

---

government's external access points (including those to the Internet). This consolidation will result in a common security solution that includes: facilitating the reduction of external access points, establishing baseline security capabilities; and validating agency adherence to those security capabilities. Agencies participate in the TIC initiative either as TIC Access Providers (a limited number of agencies that operate their own capabilities) or by contracting with commercial Managed Trusted IP Service (MTIPS) providers through the GSA-managed NETWORX contract vehicle.

[50] Intrusion Detection Systems use passive sensors to identify when unauthorized users attempt to gain access to networks. DHS is deploying, as part of its EINSTEIN 2 activities, signature-based sensors capable of inspecting Internet traffic entering federal systems for unauthorized accesses and malicious content. The EINSTEIN 2 capability enables analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection technology. EINSTEIN 2 is capable of alerting US-CERT in real time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualization of the derived data. The Department of Homeland Security's Privacy Office has conducted and published a Privacy Impact Assessment for the EINSTEIN 2 program.

[51] This approach, called EINSTEIN 3, will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision making on network traffic entering or leaving these Executive Branch networks. The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to detect automatically and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense. EINSTEIN 3 will assist DHS US-CERT in defending, protecting and reducing vulnerabilities on Federal Executive Branch networks and systems. The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with federal departments and agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and when deemed necessary by DHS, to send alerts that do not contain the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA exercising its lawfully authorized missions.

[52] This initiative is developing strategies and structures for coordinating all cyber R&D sponsored or conducted by the U.S. government, both classified and unclassified, and to redirect that R&D where needed.

[53] Government information security offices and strategic operations centers must share data regarding malicious activities against federal systems in order to have a better understanding of the entire threat to government systems and to produce the best overall national cyber defense. This initiative enables shared situational awareness and collaboration across six centers that are responsible for carrying out U.S. cyber activities. The National Cybersecurity Center (NCSC) within the Department of Homeland Security will play a key role in securing U.S. Government networks and systems under this initiative by coordinating and integrating information from the six centers to provide cross-domain situational awareness, analyzing and reporting on the state of U.S. networks and systems, and fostering interagency collaboration and coordination.

[54] A government-wide cyber counterintelligence plan is necessary to coordinate activities across all federal agencies to detect, deter, and mitigate foreign-sponsored attackers on U.S. and

(7) Increase the security of our classified networks.[55]

(8) Expand cyber education.[56]

(9) Define and develop enduring "leap-ahead" technology, strategies and programs.[57]

(10) Define and develop enduring deterrence strategies and programs.[58]

(11) Develop a multi-pronged approach for global supply chain risk management.[59]

(12) Define the federal role for extending cybersecurity into critical infrastructure domains.[60]

In April 2011, the White House issued the National Strategy for Trusted Identities in Cyberspace (National Strategy).[61] The National Strategy recognizes that our digital infrastructure is a strategic national asset and protecting it, while safeguarding privacy and civil liberties, is a national security priority and an economic necessity. The National Strategy recognizes that one of the primary technical and policy shortcomings is the online authenti-

---

private sector information systems. The Cyber CI Plan is aligned with the National Counterintelligence Strategy of the United States of America (2007) and supports the other programmatic elements of the CNCI.

[55] Classified networks house the federal government's most sensitive information and enable crucial war-fighting, diplomatic, counterterrorism, law enforcement, intelligence, and homeland security operations.

[56] The government requires people with the right knowledge, skills, and abilities to implement cybersecurity technologies.

[57] This initiative seeks to develop strategies and programs to enhance the component of the government R&D portfolio that pursues high-risk/high-payoff solutions to critical cybersecurity problems.

[58] Policymakers must think through the long-range strategic cybersecurity options available to the United States. This initiative is aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors.

[59] Globalization of the commercial information and communications technology marketplace provides increased opportunities to penetrate the supply chain to gain unauthorized access to data, to alter data, or to interrupt communications. Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk requires a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions. This initiative will enable agencies to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks.

[60] The U.S. Government depends on a variety of privately owned and operated critical infrastructures to carry out the public's business. This initiative builds on the partnership between the federal government and the public and private sector owners and operators of Critical Infrastructure and Key Resources (CIKR). The Department of Homeland Security and its private-sector partners have developed a plan of shared action that includes a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR.

[61] See National Strategy for Trusted Identities in Cyberspace (April 2011), available at http:// whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (last visited July 20, 2011), and § 12.03[1] *infra* for a discussion of the Cyber Security Coordinator's role in setting a national agenda and for coordinating Executive Branch cyber security activities.

cation of people and devices.[62] In order to address this deficiency, the National Strategy calls for the establishment of "trusted identities," and charts a course for the public and private sectors to "collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions."[63] This public-private collaboration will raise complicated issues regarding government regulatory authority[64] and increase the importance of immunity for participating organizations.[65]

---

[62] See § 1.01[5] *supra* for a discussion of authentication technology.

[63] National Strategy, N. 61 *supra*, at p. 1.

[64] See: § 12.01[1][c] *infra* for a discussion of the Department of Homeland Security's (DHS) role in protecting cyberspace; § 12.01[1][d] *infra* for a discussion of the Department of Justice's (DOJ) role in protecting cyberspace; § 12.01[1][h] *infra* for a discussion of the National Security Agency's (NSA) role in regulating cyberspace; § 12.01[1][i] *infra* for a discussion of the Department of Defense's (DOD) role in protecting cyberspace.

[65] See § 9.03[4] *supra* for a discussion of official immunity and Murray v. Northrop Grumman Information Technology, 444 F.3d 169, 174 (2d Cir. 2006) (granting absolute immunity to a government contractor from suit for state tort actions arising from sharing of information with federal agencies and dismissing appellants' claims of negligent misrepresentation and defamation).