Texas Wesleyan Law Review

Volume 8 | Issue 3 Article 7

7-1-2002

The Impact of Computer Security Regulation on American Companies

Dean William Harvey

Amy White

THE IMPACT OF COMPUTER SECURITY REGULATION ON AMERICAN COMPANIES

Dean William Harvey†
Amy White‡

I. INTRODUCTION 505
A. *Privacy and Security* 506
II. PRIVACY POLICIES AND SECURITY 507
A. FTC v. Eli Lilly 509
B. *Suggested Policies and Procedures* 510
III. FEDERAL STATUTORY SECURITY REQUIREMENTS 511
A. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* 511
1. Requirements Under the Proposed HIPAA Security Regulation 512
2. Scope of Security Compliance 516
3. Importance of Compliance 517
B. *The Gramm-Leach-Bliley Act* 518
1. Security Requirements Promulgated by Federal Agencies Under the GLB Act 519
2. Importance of Compliance 523
C. *Children's Online Privacy Protection Act* 523
1. Importance of Compliance 524
IV. EUROPEAN DATA REQUIREMENTS 524
A. *European Union Directive* 525
1. Safe Harbor 526
2. Effect on U.S. Companies 527
V. CONCLUSION 527

I. INTRODUCTION

Since the mid 1990's, e-business and electronic communication have spread rapidly and widely throughout the United States. According to one study, the majority of the U.S. population, fifty-four percent, used the Internet in September 2001, up twenty-six percent from the year before.[1] Companies are targeting their e-business efforts to reach this

† Partner, Vinson & Elkins L.L.P., 2001 Ross Avenue, 3700 Trammell Crow Center, Dallas, Texas 75201; Chair, Internet Practice Group; J.D., The University of Texas School of Law, Austin, Texas; B.S. Computer Science, West Virginia University, dharvey@velaw.com.

‡ Associate, Vinson & Elkins L.L.P., 2001 Ross Avenue, 3700 Trammell Crow Center, Dallas, Texas 75201; J.D., The University of Texas School of Law, Austin, Texas; M.P.A., The University of Texas, Austin, Texas; B.B.A., The University of Texas, Austin, Texas; CPA, awhite@velaw.com.

1. Press Release, Cyber Atlas Staff, U.S. Internet Population Continues to Grow (Feb. 9, 2002) *at* http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_969541,00.html (on file with the Texas Wesleyan Law Review).

DOI: https://doi.org/10.37419/TWLR.V8.I3.6

expanding customer base. By entering the world of e-business, companies can benefit from lower transaction costs, improvement in the time to take products to market, cost savings in inventory and supply chain reduction, improved communications, and the ability to outsource organizational tasks such as payroll and customer-relations management. Cost savings and easy access for both online businesses and consumers depend on the ability of such online businesses to collect, store, transfer, and analyze vast amounts of data.

As more and more business is conducted online, electronic security has become more of a concern. In 2001 alone, $380 million was lost due to breaches in electronic security.[2] While terrorist attacks and financial fraud should motivate companies to carefully consider their information security, recent developments in the law *require* some companies to safeguard certain types of consumer information.

Additionally, Internet users appear concerned about disclosing personal identifying information. According to a recent study, eighty-nine percent of Internet users are worried that companies may sell their private information, and eighty-one percent of Internet users who seek health information want the right to sue an online web company for violations of their privacy policies.[3] Companies that wish to collect and use such data need to consider what steps they can take to reassure customers and to overcome their fears. The implementation of adequate security measures may improve consumer confidence. According to one survey conducted by Cyber Dialogue, retailers lost $6.2 billion in sales in 2001 from consumers concerned about the privacy of their information.[4] The focus of this Article is on legal requirements for the implementation of security safeguards to protect the privacy of information.

A. *Privacy and Security*

It is important to distinguish between the concepts of "privacy" and "security." For the purposes of this Article, "privacy" involves the right of individuals to control the use and disclosure of information about them. "Security" means the safeguards (including personnel policies, information practice policies, disaster preparedness, hardware, software, and oversight) to protect information from unautho-

2. *See* Computer Security Institute Article, Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar *at* http://www.gocsi.com/prelea/000321.html (last visited Feb. 28, 2002) (on file with the Texas Wesleyan Law Review).

3. Press Release, Institute for Health Care Research and Policy, Study Shows Majority of Internet Users Concerned About Online Privacy (Nov. 29, 2000) *at* http://www.healthprivacy.org (on file with the Texas Wesleyan Law Review).

4. Press Release, UCO Software Inc., UCO Software to Address Retailers' $6.2 Billion Privacy Problem *at* http://www.cyberdialogue.com/news/releases/2001/11-07-uco-retail.html (last visited Feb. 20, 2002) (on file with the Texas Wesleyan Law Review).

rized access, attacks from outside the organization, and from misuse and negligence within the organization. Intuitively, without security, it is not possible to provide complete privacy, because unauthorized access and use of personal information can occur.

To date, many commentators and regulators have focused on the requirements for the privacy of information.[5] As a result, many companies have taken steps to protect the privacy of consumers, such as establishing and updating privacy policies, appointing privacy officers, and other similar steps to ensure that customers understand, and to some extent, control the uses of information about them. However, often no equivalent emphasis has been placed on the security of such information.

A number of laws which were passed primarily to address privacy concerns, either directly or indirectly implicate security. Examples include the Health Insurance Portability and Accountability Act (HIPAA); the Gramm-Leach-Bliley Act (the GLB Act); and the Children's Online Privacy Protection Act (COPPA).

This Article will discuss what companies should do to comply with the security requirements of recent federal legislation governing the electronic collection and transmission of personal information. Part II of this Article will discuss online privacy policies and the security measures companies should implement to comply with statements made in such policies. Part III of this Article will discuss federal statutory security requirements, and in particular, the security measures required under HIPAA, the GLB Act, and COPPA. Part IV of this Article will discuss European regulation regarding the security of information.

II. PRIVACY POLICIES AND SECURITY

The Federal Trade Commission (the Commission) began studying online privacy issues and the effect of industry self-regulation in 1995.[6] As a result of this survey, the Commission established four fair information principles, which the Commission believed all companies should address in their online privacy policies.[7] These four core principals are: (1) notice; (2) choice; (3) access; and (4) security.[8] Notice requires website operators to provide consumers with clear and conspicuous notice of the operators' information practices, including the collection, use, and disclosure of information.[9] Choice requires web-

5. FTC REP. TO CONG., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000); Jeffrey P. Cunard & Jennifer B. Coplan, *Developments in Internet and E-Commerce Law: 2001*, 678 PRAC. L. INST. 935 (2001); Bradley A. Slutsky & Allison S. Brantley, *Privacy on the Internet: A Summary of Government and Legal Responses and a Practical Guide to Protecting Your Client*, 637 21ST ANN. INST. ON COMPUTER L. 85 (2000).

6. FTC REP. TO CONG., *supra* note 5, at i.

7. *Id.* at iii.

8. *Id.*

9. *Id.* (stating a more complete definition of this principle).

site operators to offer consumers choices as to how their personal identifying information is used (both internally and externally) beyond the use for which the information was provided, *e.g.*, to consummate a transaction.[10] Access requires website operators to offer consumers reasonable access to information maintained about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.[11] Security requires website operators to take reasonable steps to protect the security of the information they collect from consumers.[12]

The Commission has encouraged companies to voluntarily create and publish privacy policies in conformance with its fair information principles for privacy policies.[13] Many companies are not aware of the fact that by publishing such a policy, they may incur liability under the FTC Act. However, the FTC Act empowers the Commission to take action against companies for misleading or deceptive practices.[14] Moreover, pursuant to § 57 of the FTC Act, the Commission has the authority to prescribe rules and general statements of policy which define with specificity those acts or practices which are unfair, or deceptive acts or practices in or affecting commerce.[15] Under such authority, the Commission has treated the misuse or disclosure of confidential information other than as described in a company's privacy policy as an unfair or deceptive trade practice, and has filed claims against companies who have failed to abide by their privacy policies regarding the collection, use, and disclosure of information.[16]

Until recently, the Commission's enforcement actions under the FTC Act have focused on violations of the *privacy* principles.[17] That changed recently with the Commission's enforcement action against Eli Lilly and Company (Eli Lilly).[18] For the first time, the Commission brought an action against a company for failing to take adequate *security* measures.[19]

---

10. *Id.*

11. *Id.*

12. *Id.*

13. *Id.* at 10–14 (describing how the implementation of privacy notices has increased since the Commission's 1998 Report to Congress).

14. 15 U.S.C. §§ 41–57a (2000).

15. *Id.* § 57a(a)(1)(B).

16. *See* Fed. Trade Comm'n v. Toysmart.com, L.L.C., No. CIV. A. 00-CV11341RG5, 2000 WL 1523287 (D. Mass. Aug. 21, 2000); Liberty Fin. Cos., No. 982-3522, 1999 WL 275191 (FTC May 6, 1999); GeoCities, a Corp., No. C-3839, 1999 WL 69858 (FTC Feb. 5, 1999).

17. Such principles as previously discussed refer to the individual's right to control the use and disclosure of information about him or her.

18. Complaint, Eli Lilly & Co., No. 012–3214 (FTC filed 2002), *at* http://www.ftc.gov/os/2002/01/lillycmp.pdf (on file with the Texas Wesleyan Law Review).

19. *Id.* at para. 5–9.

A. FTC v. Eli Lilly

According to a recent settlement between the Commission and Eli Lilly, Eli Lilly operated an email reminder service known as "Medi-Messenger," which it marketed through its Lilly.com and Prozac.com websites.[20] Customers who utilized this service could design and receive personal email messages reminding them to take medication, or could request the receipt of other information.[21] On June 27, 2001, Eli Lilly sent out a notice that it would be discontinuing its "Medi-Messenger" program and re-launching Prozac.com with a "new navigation and feel."[22] Due to a programming mistake by a computer programmer, this message was mistakenly sent to all Medi-Messenger recipients with each person's email address in the "To:" line of the message.[23] Eli Lilly's privacy policy specifically stated, "Eli Lilly and Company respects the privacy of visitors to its Web sites, and we feel it is important to maintain our guests' privacy as they take advantage of this resource. As a result, we have developed this privacy code."[24] Additionally, the privacy policy promised that, "Our websites have security measures in place . . . ."[25] The Commission filed a complaint because Eli Lilly failed to implement or maintain appropriate internal measures to protect consumer sensitive information in violation of its privacy policy.[26] Specifically, the complaint alleged that Eli Lilly failed to:

> provide appropriate training for its employees regarding consumer privacy and information security; provide appropriate oversight and assistance for the employee who sent out the e-mail, who had no prior experience in creating, testing, or implementing the computer program used; and implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the e-mail.[27]

On January 18, 2002, Eli Lilly agreed to settle Commission charges that it violated provisions of the FTC Act by failing to take adequate security measures to prevent the disclosure of sensitive personal information collected from consumers in violation of its privacy policy.[28]

---

20. *Id.* at para. 3–4.

21. *Id.*

22. Exhibit D, Eli Lilly & Co., No. 012–3214 (F.T.C. filed 2002), *at* http://www.ftc.gov/os/2002/01/eliappadpdf.pdf (on file with the Texas Wesleyan Law Review).

23. *Id.*

24. Exhibit B, Eli Lilly & Co., No. 012–3214 (F.T.C. filed 2002), *at* http://www.ftc.gov/os/2002/01/eliappadpdf.pdf (on file with the Texas Wesleyan Law Review).

25. *Id.*

26. Complaint, *supra* note 18, at para. 3–9.

27. *Id.* at para. 7.

28. Press Release, Fed. Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* http://www.ftc.gov/opa/2002/01/elililly.htm (on file with the Texas Wesleyan Law Review).

Pursuant to the Agreement containing the Commission's consent order, Eli Lilly must do the following:

1. Not misrepresent the extent to which it maintains and protects the privacy of personally identifiable information;

2. Establish a security program which includes: designating appropriate personnel, identifying reasonably foreseeable internal and external security risks, conducting an annual review by qualified persons within ninety days of the order and yearly thereafter, and adjusting the program in light of any findings or recommendations;

3. For a period of five years, make certain items available to the Commission, upon the Commission's request, such as: sample advertisements or other documents which discuss Eli Lilly's collection, use, and security of personal information; all reports, studies, review, audits, etc., prepared by Eli Lilly or by someone on Eli Lilly's behalf; and any documents, prepared by or on behalf of Eli Lilly which contradict or call Eli Lilly's compliance with information security into question;

4. Deliver a copy of the order to all future officers, directors, and appropriate personnel;

5. Provide thirty days advance written notice prior to any significant corporate change such as a sale, merger, assignment, or dissolution; and

6. File a report with the Commission no later than one hundred twenty days after service of the order which details the manner and form in which Eli Lilly has complied with the order.[29]

Commissioner Orson Swindle filed a concurring statement with the consent order in which he stated, "Lilly's unfortunate and unintended disclosure of prescription drug users' personal information has given us all the opportunity to evaluate how to improve upon security practices for confidential information."[30]

B. *Suggested Policies and Procedures*

The Eli Lilly action provides some guidance as to what security measures online companies should take to avoid possible violations of the FTC Act, and to comply with the Commission's fair information practices principles. A key lesson to be learned is that even though the security breach that resulted in the release of personal information was unintended by the company, the Commission still brought an action against the company. To avoid similar problems, companies which have established privacy policies should consider establishing a

29. Agreement Containing Consent Order, Eli Lilly & Co., No. 012–3214 (F.T.C. filed 2002), *at* http://www.ftc.gov/os/2002/01/lillyagree.pdf (on file with the Texas Wesleyan Law Review).

30. Concurring Statement of Commissioner Orson Swindle, Eli Lilly & Comp., No. 012–3214 (F.T.C. filed 2002), *at* http://www.ftc.gov/os/2002/01/lillyswindlestat.htm (on file with the Texas Wesleyan Law Review).

security program to safeguard the privacy of information collected pursuant to the privacy policy. Based upon *Eli Lilly*, it appears that the Commission requires that the security program include training of personnel regarding the importance of protecting the confidentiality of information collected from consumers, and annual audits to produce audit reports which identify possible security risks and make recommendations.[31] In addition, companies may want to consider taking additional security precautions, such as establishing a security team, requiring annual security training, providing security reminders, enforcing user access controls and authentication, logging system usage, entering into confidentiality agreements with business partners, establishing emergency back up plans, establishing plans for testing and installing new software, and providing more technical safeguards.[32]

III. Federal Statutory Security Requirements

In addition to the Commission's requirement that companies take steps to ensure the security of information collected pursuant to a privacy policy, there are federal statutes that impose information security obligations on companies in different industries. This section describes the security requirements of such statutes.

A. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*

Congress passed HIPAA with the stated purpose to:

> improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.[33]

HIPAA has three components: privacy, electronic transactions standards, and security and electronic signature standards.[34] The Department of Health and Human Services (HHS) has established rules regarding each of these components.[35] The standards for electronic transactions regulation, effective October 16, 2000, require electronic code sets for certain transactions to simplify and improve the effi-

31. *See* Agreement Containing Consent Order, *supra* note 30.

32. See generally the security requirements promulgated under HIPAA, Security and Electronic Signature Standards, 63 Fed. Reg. 43,242 (proposed Aug. 12, 1998) (to be codified at 45 C.F.R. pt. 142).

33. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936.

34. DHHS General Administration Requirements, 45 C.F.R. § 160 (2001); DHHS Security and Privacy, 45 C.F.R. § 164 (2001); Security and Electronic Signature Standards, 63 Fed. Reg. 43,242.

35. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, § 264, 110 Stat. 1936.

ciency of electronic transmissions throughout the health care industry.[36] H.R. 3323, passed in December of 2001, extended the compliance date for this rule from October 16, 2002, to October 16, 2003.[37] The security and electronic signature standards regulation, proposed by HHS in 1998, but not yet effective, will require covered entities to develop and maintain security programs for the protection of patient health information.[38]

HIPAA directly imposes security requirements on "covered entities."[39] "Covered entities" include healthcare providers, which conduct certain transactions electronically, health plans, and health care clearinghouses.[40] If a company maintains a self-funded health plan for its employees, it is likely that the plan will be subject to the security requirements of the HIPAA regulations.[41] The HIPAA regulations indirectly regulate companies which are not part of the health care industry, as they require covered entities to execute contracts with business partners to impose the same obligations on them.[42] Thus, even if a company is not a "covered entity," it may still have to comply with the requirements set forth in the HIPAA regulations if it receives or processes protected health information from covered entities, and those covered entities impose such obligations via contract. Covered entities have until April 14, 2003, to comply with the privacy regulation,[43] and will have two years from its final release date to comply with the final security regulation.[44]

1. Requirements Under the Proposed HIPAA Security Regulation

The security measures required under the rule are divided into four categories: (1) Administrative Procedures; (2) Physical Safeguards; (3) Technical Security Services within the covered entity; and (4) Technical Security Mechanisms to protect the confidentiality of information transmitted outside the covered entity.[45] Generally, each measure includes a requirement, and implementations for that requirement. However, the regulation does not specify technology solutions for each requirement. Instead, each covered entity must assess the risk and make a business decision as to what solution will provide adequate risk reduction at a bearable cost.

36. DHHS General Administrative Requirements, 45 C.F.R. § 160; DHHS Administrative Requirements (2001) 45 C.F.R. § 162.
37. Administrative Simplification Act, Pub. L. No. 107–105, 115 Stat. 1003 (2001).
38. Security and Electronic Signature Standards, 63 Fed. Reg. 43,242.
39. *Id.*
40. 45 C.F.R. § 160.102.
41. *Id.*
42. DHHS Security and Privacy, 45 C.F.R. § 164.504(e)(1) (2001).
43. *Id.* § 164.534.
44. Security and Electronic Signature Standards, 63 Fed. Reg. 43,269 (to be codified at 45 C.F.R. pt. 142.312).
45. *See id.* at 43,266–68 (to be codified at 45 C.F.R. pt. 142.308).

(a) *Administrative Procedures.* Administrative Procedures generally include formal procedures and documentation, to manage the selection and execution of security measures and to prescribe the conduct of personnel. HHS specifically lists twelve requirements:

(i) *Certification.* This requirement requires a covered entity to develop a checklist of required security measures and review its compliance with those measures, and to certify that the measures are in compliance with the security requirements of HIPAA.[46] A third party may be used to conduct this certification.[47]

(ii) *Chain of Trust Partner Agreements.* This requirement requires a covered entity to analyze its relationship with third parties and to enter into specific agreements whereby such third parties agree to protect the confidentiality and security of protected heath information.[48]

(iii) *Contingency Planning.* This requirement requires a covered entity to analyze its response plan for dealing with an emergency. A covered entity must first perform a data criticality analysis, then based on such analysis, develop a response plan.[49] A response plan should include procedures for data backup, disaster recovery, and general procedures for personnel and records processing in an emergency mode.[50] As part of Contingency Planning, the covered entity should test its response plan, and revise specific procedures as necessary.[51]

(iv) *Records Processing.* This requirement requires a covered entity to document policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information, including proper access controls, user authorization, and user authentication.[52]

(v) *Information Access Control.* This requirement consists of granting different levels of access to health care information by establishing policies and procedures to: authorize different levels of access, ensure that only certain levels have access to certain information, and enable modification of access levels.[53]

(vi) *Internal Audit.* This requirement requires the review of systems activity, including the testing, reporting and revising of procedures relating to logins, file access, and the handling of security incidents.[54]

46. *Id.* at 43,266.
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*

(vii) *Personnel Security.* This requirement ensures that personnel have the required authority and clearances. As part of Personnel Security, there should be procedures to assure supervision of information technology maintenance personnel, to record access authorizations, to assure supervision of personnel and their information access, to require background checks, to control electronic communications, such as email, and to require security awareness training.[55]

(viii) *Security Configuration Management.* This requirement shall include procedures for hardware and software installation and management, hardware and software inventory, testing of security features, and virus checking.[56]

(ix) *Security Incident Procedures.* This requirement includes procedures to report security incidents, and procedures to respond when such incidents are reported.[57]

(x) *Security Management Process.* This requirement includes procedures to: perform risk and cost/benefit analyses, assess internal controls, develop methods to reduce risks to acceptable levels, and establish and enforce disciplinary policies.[58] As part of the Security Management Process, a covered entity shall establish a commitment to security by training employees regarding their responsibilities for protecting information.[59]

(xi) *Termination Procedures.* This requirement includes appropriate security measures for the termination of an employee's access to information, including: lock changes, the employee's surrender of keys or other access cards, the termination of the employee's user account I.D., and the termination of the employee's authorization.[60]

(xii) *Training.* This requirement includes security awareness training for all personnel, the sending of periodic security reminders, user education concerning virus protection, user education concerning the importance of log-in success, and user education in password management.[61]

(b) *Physical Safeguards.* Physical Safeguards generally protect the physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion.[62] HHS specifically lists six safeguards:

55. *Id.*
56. *Id.*
57. *Id.* at 43,266–67.
58. *Id.* at 43,267.
59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.* at 43,267–68.

(i) *Assignment of Security Responsibility.* This requirement requires the appointment of a security officer and perhaps a security team to oversee the implementation and continued maintenance of the other security procedures.[63]

(ii) *Media Controls.* This requirement governs the receipt and removal of hardware and software, including: system compatibility; tracking usage; and the management of data storage, data backup, and disposal of data.[64]

(iii) *Physical Access Controls.* This requirement requires a plan to secure the building and equipment from unauthorized access, including procedures to sign-in visitors.[65] It also includes the implementation of the procedures described under Administrative Procedures such as: disaster recovery, user access, and records processing.[66]

(iv) *Policies and Guidelines on Workstation Use.* This requirement includes the documentation of formal policies delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical surroundings required around specific computer terminal sites depending upon the sensitivity of information accessed at such sites.[67]

(v) *Secure Workstation Location.* This requirement requires a company to establish policies governing the location of workstations and access to workstations.[68]

(vi) *Security Awareness Training.* This requirement requires training personnel, including management, about the importance of security issues as described in *Training* under Administrative Procedures.[69]

(c) *Technical Security Services.* Technical Security Services generally deal with the processes in place to protect information and control individual access to information.[70] HHS specifically lists five processes:

(i) *Access Control.* This requirement includes the establishment of specific emergency access procedures dependent upon the context of the transaction, such as: (a) the time of day or the workstation location, (context-based access), (b) the user's role in the covered entity and his or her level of authorization (role-

63. *Id.* at 43,267.
64. *Id.*
65. *Id.* at 43,267–68.
66. *Id.*
67. *Id.* at 43,268.
68. *Id.*
69. *Id.*
70. *Id.*

based access), and (c) the user's identity (user-based access).[71] Access control may also include the encryption of data.[72]

(ii) *Audit Controls.* This requirement includes the establishment of mechanisms employed to monitor, record, and examine system activity with respect to the other processes described herein.[73]

(iii) *Authorization Controls.* This requirement includes the establishment of procedures for user authorization based upon his or her role in the organization or his or her employment status with the covered entity.[74]

(iv) *Data Authentication.* This requirement includes the establishment of tests such as check sum, double keying, message authentication code, or digital signature to ensure that data has not been altered or destroyed in an unauthorized manner.[75]

(v) *Entity Authentication.* This requirement includes the establishment of procedures for automatic logoff and unique user identification.[76] Regarding user identification, a covered entity must require the assignment to users of one of the following: biometric numbers, passwords, personal identification numbers, telephone callback, or token cards.[77]

(d) *Technical Security Mechanisms.* To ensure a covered entity's security standards will protect information electronically transmitted or stored, the Technical Security Mechanisms, require the establishment of integrity controls (ensuring the validity of information), or message authentication (ensuring the message received matches the message sent), and the utilization of access controls or encryption.[78] If the covered entity transmits communications electronically over open networks, it must ensure that the information cannot be easily intercepted and interpreted by parties other than the intended recipient.[79] Such assurance can be achieved through the implementation or installation of alarms, audits, authentication procedures, and event/security incident reporting procedures.[80]

2. Scope of Security Compliance

A review of the foregoing HIPAA security requirements should make it clear that security has three major components: people, process, and technology. The HIPAA security regulation tries to address

71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*

the "process component" repeatedly by requiring the establishment and enforcement of security policies.[81] It addresses the people component also through policies, but in addition, by requiring training, documented procedures, and audits. Finally, technology is the smallest of the components, and really only addressed in Technical Security Services and Technical Security Mechanisms. While HIPAA acknowledges the need for technology solutions,[82] the majority of effort involved in complying with the HIPAA security regulation is organizational and operational, rather than the implementation of technology.

3. Importance of Compliance

Even though compliance with the privacy and security components of HIPAA is not yet required, companies should be aware that courts are starting to emphasize the importance of the HIPAA regulations. In one recent court case in Virginia, the district court judge denied a hospital's motion to quash the government's subpoena of patient medical records.[83] Citing the provisions of HIPAA and applying a balancing test, the judge said "in light of the strong federal policy in favor of medical records, I find that it would be 'unreasonable or oppressive' to permit disclosure of these records at trial without the opportunity for the affected patient to object."[84] This case appears to be the first example of courts looking to the HIPAA regulations for guidance, even when such regulations were clearly not effective or applicable.

Additionally, a violation of HIPAA can result in civil penalties assessed by HHS of up to $100 per occurrence, up to a maximum amount of $25,000 per year, per person who violates a single requirement.[85] If HHS assesses separate fines for each component of a privacy rule requirement, these penalties may multiply to an amount in excess of one million dollars per person per violation of a single privacy rule requirement. HHS has interpreted not using standard code sets mandated by the transaction standards as four possible violations, and is considering imposing separate fines for each component of the security requirements.[86]

81. *See generally id.* at 43,263–69.

82. *Id.* at 43,268.

83. United States v. Sutherland, 143 F. Supp. 2d 609 (W.D. Va. 2001) (order denying motion to quash).

84. *Id.* at 613.

85. 42 U.S.C. § 1320d–5(a)(1) (Supp. V 1999). It is important to note that no penalty (or a reduced penalty) will be assessed if noncompliance was reasonably discovered, provided there was reasonable cause and no willful neglect, or if a violation was corrected within thirty (30) days of discovery.

86. RICHARD ZON OWEN, HAW. MED. SERV. ASS'N, HIPAA APPLICABILITY, PENALTIES, ENFORCEMENT, & CERTIFICATION, *at* http://www.hipaadvisory.com/regs/PenaltiesbyZon.htm (last modified Mar. 7, 2002) (on file with the Texas Wesleyan Law Review).

Individuals may also be charged with criminal penalties for knowing and wrongful disclosure of individually identifiable health information.[87] The general penalty assessed for knowing and wrongful disclosure is a $50,000 fine, or one year imprisonment, or both.[88] If the disclosure was made under false pretenses, the penalty is a $100,000 fine, or five years imprisonment, or both.[89] If the disclosure was made with the intent to sell the protected health information, the penalty is a $250,000 fine, or ten years imprisonment, or both.[90]

B. *The Gramm-Leach-Bliley Act*

The Gramm-Leach-Bliley Act (the GLB Act), also known as Title V of the Financial Services Act, was signed into law on November 12, 1999.[91] Comments to the statute indicate that Congress passed this law because of its belief that each financial institution[92] has "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[93] "Nonpublic personal information" is defined as any personally identifiable financial information provided by a consumer to a financial institution as a result of a transaction, or otherwise obtained by the financial institution.[94]

The scope of the GLB Act is broader than might be expected. The term "financial institution" is not simply limited to banks.[95] It appears to include banks, mortgage loan companies, credit unions, broker/dealers, companies which issue credit cards, and any other institution which engages in financial transactions with or provides financial products or services to consumers.[96] It should be noted, however, that simply accepting a credit card, or having a lay-away plan should not bring a retailer under the scope of the GLB Act.[97]

Privacy regulations promulgated by federal agencies[98] pursuant to the GLB Act require a financial institution to provide each individual

87. 42 U.S.C. § 1320d-6(a).
88. *Id.* § 1320d-6(b).
89. *Id.*
90. *Id.*
91. *See generally* 15 U.S.C. §§ 6801-09, 6821-27 (2000).
92. *Id.* § 6809(3)-(4) (defining financial institution and consumer).
93. *Id.* § 6801(a).
94. *Id.* § 6809(4)(A).
95. *See* FTC Privacy of Consumer Financial Information, 16 C.F.R. § 313.3(k)(2) (2001).
96. *See id.*
97. *Id.* § 313.3(k)(4).
98. Federal banking agencies (the Office of Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (FRB), the Board of Directors of the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS), collectively, the Banking Agencies); the Secretary of the Treasury; the State insurance authorities; the Board of the National Credit Union Administration (NCUA); the Securities Exchange Commission; and the Federal Trade Commission. 15 U.S.C. § 6804(a).

customer with a clear statement of its policies and practices for protecting the privacy of non-public personal information.[99] Financial institutions must also provide clear and conspicuous notice about how information may be disclosed to third parties, and must provide customers an opportunity to opt out of such disclosures in advance.[100]

1. Security Requirements Promulgated by Federal Agencies Under the GLB Act

Pursuant to 15 U.S.C. § 6801(b), various agencies are granted the authority to establish their own "Safeguards Rule," setting out appropriate administrative, technical, and physical safeguards for financial institutions subject to the agencies' jurisdiction to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[101] The remainder of this section shall focus on the Safeguards Rule as implemented by each of these agencies (except for the Department of the Treasury which adheres to the rules promulgated by the OCC and OTC, and except for state insurance authorities, because the scope of this article is limited to federal security issues).

(a) *Interagency and NCUA*[102] *Safeguards Rules.* The Interagency Guidelines[103] (the Guidelines) require covered financial institutions to develop and implement an information security program which will: (1) involve the board of directors and management; (2) assess security risks; (3) manage and control risk as part of a comprehensive risk management plan; and (4) oversee outsourcing arrangements.[104] Compliance was required by July 1, 2001.[105]

---

99. 15 U.S.C. § 6803(b).

100. *Id.* § 6802(b).

101. *Id.* § 6801(b).

102. NCUA Rule applying to credit unions tracks the same requirements for security as the Interagency Guidelines, but phrases the requirements with the word "should," rather than "shall," 12 C.F.R. § 748 (2001).

103. OCC Safety and Soundness Standards, 12 C.F.R. § 30 (2001); FRS Membership of State Banking Institutions in the Federal Reserve System, 12 C.F.R. § 208 (2001); FRS International Banking Operations, 12 C.F.R. § 211 (2001); FRS Bank Holding Companies and Change in Banking Control, 12 C.F.R. § 225 (2001); FRS Rules of Practice for Hearings, 12 C.F.R. § 263 (2001); FDIC Rules of Practice and Procedure, 12 C.F.R. § 308 (2001); FDIC Standards for Safety and Soundness, 12 C.F.R. § 364 (2001); OTS Security Procedures, 12 C.F.R. § 568 (2001); OTS Submission and Review of Safety and Soundness Compliance Plans and Issuance of Orders to Correct Safety and Soundness Deficiencies, 12 C.F.R. § 570 (2001).

104. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

105. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

(i) *Involve the Board of Directors and Management.* Specifically, the Guidelines require that the board of directors of each financial institution shall approve the financial institution's written information security policy and oversee the development, implementation, and maintenance of an effective information security program.[106] The financial institution's management shall regularly: (a) evaluate the impact on the financial institution's security program of changing business arrangements; (b) document compliance with the Guidelines; and (c) report to the board on the overall status of the information security program, including material matters related to: risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements in the information security program.[107]

This requirement was imposed because the "[a]gencies believe that a financial institution's overall information security program is critical to the safety and soundness of the institution. Therefore, the final Guidelines continue to place responsibility on an institution's board to approve and exercise general oversight over the program."[108] Thus, the agencies placed a responsibility on directors (who have a fiduciary duty to their company)[109] to become involved in creating and evaluating the information security policy.

(ii) *Assess Security Risks.* Further, each financial institution shall identify and assess the risks that may threaten the security, confidentiality, or integrity of customer information systems.[110] As part of the risk assessment, a financial institution shall determine the sensitivity of customer information and the internal or external threats to the financial institution's customer information systems.[111] Each financial institution shall assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.[112] In addition, each financial institution shall monitor, evaluate, and adjust its risk as-

106. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

107. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

108. Interagency Guidelines, Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616, 8620 (Feb. 1, 2001).

109. See Sec. 35 of the Investment Company Act of 1940 and generally, most state corporation laws.

110. *Id.*

111. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

112. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

sessment in light of any relevant changes to technology, the sensitivity of customer information, and the internal or external threats to information security.[113]

(iii) *Manage and Control Risk.* Each financial institution shall establish written policies and procedures that are adequate to control the identified risks and achieve the overall objectives of the financial institution's information security program.[114] In establishing the policies and procedures, each financial institution should consider appropriate: (a) access rights to customer information; (b) access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies; (c) access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities; (d) encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access; (e) procedures to confirm that customer information system modifications are consistent with the financial institution's information security program; (f) dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information; (g) contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by service providers; (h) systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems; (i) response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected; (j) protection against destruction of customer information due to potential physical hazards, such as fire and water damage; and (k) response programs to preserve the integrity and security of customer information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged customer information.[115]

In addition to the establishment of policies and procedures, each financial institution shall train staff to recognize, respond to, and, where appropriate, report to regulatory and law enforcement agencies any unauthorized or fraudulent attempts to obtain customer information.[116] Each financial institution shall also regularly employ independent third parties to test the key controls,

113. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

114. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

115. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

116. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

systems, and procedures of the information security program.[117] The frequency and nature of such tests should be determined by the risk assessment.[118] In light of any relevant changes in technology, the sensitivity of customer information, or the threats to information security, each bank shall adjust its policies and procedures accordingly.[119]

(iv) *Oversee Outsourcing Arrangements.* Each financial institution shall establish policies and procedures to monitor and manage outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with the Guidelines.[120]

(b) *The Federal Trade Commission's Safeguards Rule.* The Commission's proposed Safeguards Rule[121] also requires the development, implementation, and management of a security program; an assessment of security risks; procedures to manage and control risk; and oversight of outsourcing arrangements similar to the requirements of the Interagency Guidelines, but applicable to all financial institutions not otherwise subject to the authority of the other agencies listed herein. In its Safeguards Rule, the Commission has proposed modifications to the Interagency Guidelines. First, the Commission allows a financial institution to designate an employee or employees to coordinate the information security program, rather than requiring the board of directors and management to perform this task.[122] Second, the Commission requires an assessment of security risks in each relevant area of operations, including: (1) employee and management training; (2) information systems, including: information processing, storage, transmission and disposal; and (3) prevention and response measures for system failures or other unauthorized intrusions.[123] Finally, the Commission does not require provisions granting financial institutions oversight authority in their contracts with service providers.[124]

(c) *The Securities Exchange Commission's (SEC) Safeguards Rule.* The SEC's Safeguards Rule, or Regulation S-P,[125] was promulgated to

117. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

118. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

119. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

120. *See* 12 C.F.R. § 30; 12 C.F.R. § 208; 12 C.F.R. § 211; 12 C.F.R. § 225; 12 C.F.R. § 263; 12 C.F.R. § 308; 12 C.F.R. § 364; 12 C.F.R. § 568; 12 C.F.R. § 570.

121. Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484 (proposed May 23, 2002) (to be codified at 45 C.F.R. pt. 314).

122. *Id.* at 36,493–94.

123. *Id.*

124. *Id.*

125. SEC Regulation S-P: Privacy of Consumer Information, 17 C.F.R. § 248 (2001).

require investment advisors registered with the SEC, brokers, dealers, and investment companies to adopt appropriate policies and procedures that address the protection of customer information and records. Consistent with all of the above Safeguards Rules, the SEC requires that the aforementioned persons or entities comply with the GLB Act by "taking reasonable measures to ensure the security and confidentiality of information," protecting against anticipated threats or hazards, and protecting against unauthorized access to or use of customer records that could result in substantial harm or inconvenience to customers.[126] While the other Safeguards Rules set forth specific criteria for a security program, the SEC requires only that covered entities establish policies and practices designed to address the GLB Act provisions.[127] In establishing these policies and practices, investment companies and broker dealers should consider that the SEC may well look to the more developed regulations of the Federal Trade Commission and other federal agencies in determining whether such broker dealers and investment companies have adopted appropriate policies and procedures.

2. Importance of Compliance

The GLB Act places enforcement of the Act on the regulating agencies.[128] Thus, the primary legal risk of failing to comply is that the appropriate regulating agency will bring an action against the company. However, companies should also consider the business risk, such as the impact on their business of a major public security breach involving customer financial data. It is possible that a large scale security breach could undermine consumer confidence in the financial institution, negatively impacting customer relationships.

C. *Children's Online Privacy Protection Act*

Primarily in response to the Federal Trade Commission's report to Congress in 1998, Congress passed COPPA, which was enacted on October 21, 1998.[129] Generally, COPPA makes it unlawful for an operator of a website or online service provider directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child under the age of 13, without verifiable parental consent.[130] Specifically, the online service provider must provide notice of what information is collected; how the information will be used; how parental consent should be obtained; and the opportunity for a parent to review, make changes, delete, or prohibit the provider's use and mainte-

126. *Id.* § 248.30.
127. *Id.*
128. 15 U.S.C. § 6805(a) (2000).
129. *Id.* §§ 6501–06.
130. *Id.* § 6502(a).

nance of previously submitted information.[131] An operator is also required to send new notice if collection, use, or disclosure practices materially change.[132]

In addition to the foregoing privacy requirements, by law, the operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information from children.[133] The Act does not describe what actions constitute such reasonable procedures.[134] However, the Commission has given guidance as to what it thinks are reasonable security procedures for financial institutions in its Safeguard Rule promulgated in the GLB Act,[135] and for companies in general under the terms of the settlement with Eli Lilly.[136] Given the public policy inherent in protecting children from commercial exploitation, companies which are subject to COPPA should consider reviewing the Commission's public statements on security, and should carefully consider their information security programs.

1. Importance of Compliance

The Commission may bring enforcement actions and impose civil penalties for violations of COPPA in the same manner as for other rules under the FTC Act.[137] In addition, under the FTC Act which generally prohibits unfair or deceptive trade practices, the Commission is authorized to examine unfair information practices in use before COPPA's effective date.[138] The Commission is authorized to impose fines of up to $10,000 per occurrence and may also issue cease and desist orders.[139] In addition, companies should consider the possible negative business impact of a security breach involving the personal data of children.

IV. European Data Requirements

While the U.S. has fairly extensive regulation of security, it is not alone in such regulation. Member states of the European Union also impose security requirements on companies which collect consumer data in Europe.

131. *Id.* § 6502(b).
132. FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.4 (2001).
133. 15 U.S.C. § 6502(b).
134. *Id.*
135. 16 C.F.R. pt. 314 (2001).
136. *See* Agreement Containing Consent Order, *supra* note 29, at pt. 1.
137. 16 C.F.R. § 312.9.
138. 15 U.S.C. § 57a.
139. *Id.* § 41–57a.

A. *European Union Directive*

It has been estimated that Internet growth in Europe will surpass that in the U.S. within the next two to three years.[140] U.S. companies that collect data in Europe should be familiar with the European Union's (EU's) comprehensive privacy legislation, the Directive on Data Protection (the Directive). The Directive is designed to regulate the collection, transfer, and use of personal data from European Internet users.[141] The Directive requires each member country to implement legislation requiring creation of government data protection agencies, registration of data bases with those agencies, and in some instances, prior approval before personal data may be processed.[142] With respect to security, the directive specifically requires:

> 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
>
> 2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect to the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
>
> 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: (i) the processor shall act only on instructions from the controller, and (ii) the obligations set out in paragraph 1, as defined by the law of the Member

140. JOHN GANTZ, EUROPE IS GETTING RIPE FOR MORE NET BUSINESS *at* http://www.computerworld.com/cwi/story/0,1199,NAV65-665_STO50349,00.html (Sept. 18, 2002) (on file with the Texas Wesleyan Law Review); RACHEL KONRAD, EUROPE—THE GUARDIAN OF THE NET, ZDNET *at* http://zdnet.com.com/2100-1106-814510.html (Jan. 15, 2002) (on file with the Texas Wesleyan Law Review).

141. *See* Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. To date, eleven (Austria, Belgium, Denmark, Finland, Greece, Italy, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom) of the fifteen EU member states have implemented the Directive, leaving France, Germany, Ireland, and Luxembourg as having not implemented the Directive. *See* http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.htm.

142. *Id.*

State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.[143]

Companies which collect data in Europe should review the laws of the appropriate member state to determine how the security requirements of the Directive have been implemented. In addition, companies which export such data to the U.S. may want to consider taking advantage of a safe harbor. The U.S. Department of Commerce, in consultation with the European Commission, has developed a "safe harbor" agreement (the Safe Harbor).[144]

1. Safe Harbor

The Safe Harbor permits U.S. companies to export European data to the U.S., and with limited exceptions, any claims regarding compliance with the Safe Harbor requirements will be decided in the U.S. in accordance with U.S. legal principles.[145]

To be assured of Safe Harbor benefits, an organization must review its practices regarding the collection and use of personal information from EU member states, and then take the necessary steps to ensure that its practices comply with Safe Harbor and the seven data principles set forth below.[146] In general terms, the principles require the following:

- *Notice*: An organization collecting and using personal information must notify individuals about the purposes for which the information will be used, ways in which they can limit the use of their own information, and complaint procedures.
- *Choice*: Individuals must be given the choice to prohibit their personal information from being disclosed to third parties or used for purposes other than originally stated.
- *Transfers to Third Parties*: Organizations must conform to the notice and choice principles to transfer information to a third party.
- *Access*: Individuals must have access (unless the burden or expense is unduly burdensome) to their own personal information held by an organization, and be able to check and correct that information where it is inaccurate.

143. *Id.*

144. U.S. DEPT. OF COMMERCE, SAFE HARBOR OVERVIEW *at* http://www.export.gov/safeharbor/sh_overview.html (last visited June 23, 2002).

145. *Id.*

146. *Id.*

- *Security*: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction.
- *Data Integrity*: An organization must only collect the minimum information necessary, and must take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
- *Enforcement*: An organization must ensure that it has mechanisms in place to address complaints from individuals; that it has procedures for verifying compliance with the Safe Harbor; and that it can remedy problems.[147]

2. Effect on U.S. Companies

It should be noted that while these principles are similar to the FTC's four guiding principles, they are in some ways stricter. However, U.S. companies may want to look at the FTC's interpretation of its principles for some guidance in interpreting the Safe Harbor principles. An organization trying to reach the Safe Harbor may also follow the guidance set forth in the frequently asked questions on self-certification.[148] As of July 2, 2002, only 208 companies are reported to have sought the Safe Harbor and to be current in their compliance.[149]

V. CONCLUSION

While commentators and companies have focused on privacy requirements, recent developments indicate that companies should also focus their attention on security. Companies which collect data pursuant to privacy policies should be concerned with taking adequate security measures to meet the promises that they made in their privacy policies. Companies which are in the health care industry, or which maintain a self-funded health plan, should be concerned about the need to comply with the security obligations with respect to health information under HIPAA. Financial institutions have had a duty, for the last eight months, to comply with federal security regulations, and companies which collect data in Europe also appear to be subject to security requirements, either through European law or the Safe Harbor.

In addition to the legally imposed security requirements, companies should consider the potential impact to their businesses of a major public security breach. Security will never be perfect, and for most companies it will not be a revenue source. However, many companies

147. *Id.*

148. EU Council Directive 95/46/EC, Article 28(1).

149. See the list of organizations who have notified the U.S. Department of Commerce that they adhere to the Safe Harbor framework *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe%20harbor%20list!OpenDocument&Start=175.

now appear to be required by law, and pragmatic considerations of protecting their businesses, to implement new information security solutions.