Washington Journal of Law, Technology & Arts

Volume 5 | Issue 1 Article 5

9-23-2008

Does the U.S. SAFE WEB Act Strike the Proper Balance Between Law Enforcement Interests and Privacy Interests?

Shaobin Zhu

Constitutional and Regulatory
Cite as: Shaobin Zhu, *Does the U.S. SAFE WEB Act Strike the Proper Balance Between Law Enforcement Interests and Privacy Interests?*, 5 Shidler J.L. Com. & Tech. 5 (Sep. 23, 2008), *at* http://www.lctjournal.washington.edu/Vol5/A05Zhu.html.

DOES THE U.S. SAFE WEB ACT STRIKE THE PROPER BALANCE BETWEEN LAW ENFORCEMENT INTERESTS AND PRIVACY INTERESTS?

Shaobin Zhu[1]

Abstract

The Internet and advances in telecommunications technology present unprecedented opportunities for cross-border fraud and deception directed at U.S. consumers and businesses. However, the Federal Trade Commission's ("FTC") ability to obtain effective relief may face practical impediments in prosecuting these cross-border wrongdoers. To help address the challenges posed by the globalization of fraud, President Bush signed the Undertaking Spam, Spyware and Fraud Enforcement With Enforcers Beyond Borders Act of 2006 ("U.S. SAFE WEB Act" or "Act") into law on December 22, 2006. This Article discusses the FTC's expanded enforcement authority granted by the Act to fight fraud and deception, and particularly to fight illegal spam, spyware, and cross-border fraud and deception. Privacy advocates have voiced concern that the FTC may now have more power to invade the privacy of U.S. citizens. This Article concludes that the Act's grant of power to the FTC is not too broad, and that the Act maintains an appropriate balance between law enforcement interests and privacy interests.

Table of Contents

Introduction

<1>Internet and telecommunications technology developments have brought many advantages to consumers. At the same time, they have also provided unprecedented opportunities for those engaged in illegal spam, spyware, fraud and deception to establish operations in one country and victimize a large number of consumers in other countries. Miscreants are now able to use the Internet to victimize consumers in ways not previously imagined. For example, "deceptive spammers can easily hide their identity, forge the electronic path of their email messages, and send messages from anywhere in the world to anyone in the world."[2] These businesses "can strike quickly on a global scale, victimize thousands of consumers in a short time, and disappear nearly without a trace – along with their ill-gotten gains."[3]

<2>There are no boundaries for the Internet and electronic commerce, and cross-border fraud and deception have been a growing problem for consumers and businesses in the U.S. and abroad.[4] The FTC received over 86,000 cross-border fraud complaints in 2005 and over 95,000 in 2006.[5] Cross-border fraud complaints comprised 20% of all fraud complaints received in 2005 and 22% in 2006.[6] Among cross-border complaints, 85% were from U.S. consumers complaining about foreign businesses in 2005 and 86% in 2006.[7] Further, many dangerous online networks, including some peer-to-peer networks, are often located outside the U.S. to avoid U.S. laws.[8]

<3>Consequently, cross-border fraud affecting American consumers is becoming an increasingly common problem facing the FTC.[9] Specifically, the FTC encounters:

> [P]ractical impediments when wrongdoers, victims, other witnesses, documents, money and third parties involved in the transaction are widely dispersed in many different jurisdictions. Such circumstances make it difficult for the [FTC] to gather all the information necessary to detect injurious practices, to recover offshore assets for consumer redress, and to reach conduct occurring outside the United States that affects United States consumers.[10]

<4>To address these impediments, President Bush signed the Undertaking Spam, Spyware and Fraud Enforcement With Enforcers Beyond Borders Act of 2006 ("U.S. SAFE WEB Act" or "Act")[11] into law on December 22, 2006.[12] Designed to help address the challenges posed by the globalization of fraud, the Act helps the FTC protect consumers from fraud and deception, particularly illegal spam, spyware, and cross-border fraud and deception, by "(1) improving the FTC's ability to cooperate with foreign counterparts in specific cases and investigations; (2) improving the FTC's ability to gather information; (3) enhancing the FTC's ability to obtain monetary consumer redress; and (4) strengthening the FTC's enforcement cooperation networks."[13]

<5>At the same time, there might be concerns that the U.S. SAFE WEB Act's grant of increased power to the FTC is too broad, permitting the FTC to invade the dealings of legitimate businesses and individuals' privacy. However, because the Act's grant of authority to the FTC is relatively modest in scope, privacy advocates' concerns seem overstated. The Act maintains an appropriate balance between law enforcement interests and privacy, and the FTC is monitored to make sure that privacy rights are not violated.

SUMMARY OF THE U.S. SAFE WEB ACT

<6>The U.S. SAFE WEB Act improves the FTC's ability to protect consumers from cross-border fraud and deception. The Act grants the FTC more power to cooperate with foreign and domestic authorities, obtain information supporting its cross-border investigations, enhance cooperation with the Department of Justice ("DOJ"), and utilize more resources to fight against cross-border fraud and deception.

<7>First, the Act improves the FTC's investigative cooperation with foreign authorities by broadening reciprocal information sharing and reducing restraints on evidence gathering.[14] Under the Act, the FTC can share confidential information in consumer protection cases with foreign law enforcers,[15] subject to appropriate confidentiality assurances.[16] The Act allows the FTC to conduct investigations and obtain evidence on behalf of its foreign counterparts if it determines that such actions are in the public interest.[17] The investigatory tools include civil investigative demand ("CID") process[18] and evidence gathering pursuant to 28 U.S.C. § 1782,[19] which were not available to the FTC in cross-border investigative cooperation.[20] The Act also authorizes the FTC to negotiate and conclude international agreements when required as a condition of reciprocal assistance.[21] Finally, the Act helps to obtain more confidential information from foreign sources, by exempting information provided by foreign agencies from public disclosure laws.[22]

<8>Second, the Act improves the FTC's ability to obtain information supporting cross-border cases[23] by protecting the confidentiality of FTC investigations.[24] It safeguards FTC investigations by:

> (1) [G]enerally [exempting] recipients of [FTC] CIDs from possible liability for keeping those CIDs confidential; (2) authorizing the [FTC] to seek a court order in appropriate cases to preclude notice by the CID recipient to the investigative target for a limited time; and (3) tailoring the mechanisms available to the [FTC] to seek delay of notification [at the time] required by the Right to Financial Privacy Act ("RFPA") or the Electronic Communications Privacy Act ("ECPA"), to better fit FTC cases.[25]

<9>The Act prevents notifying subjects of investigations if they may be likely to destroy evidence or move assets offshore or conceal them.[26] In addition, the Act protects certain entities "from liability for voluntary disclosures to the FTC [relating to] suspected fraud and deception,"[27] increasing the likelihood of such disclosures from third parties.[28] Furthermore, the Act allows information sharing with federal financial and market regulators.[29] In the cross-border context, interagency information sharing with financial regulators is particularly helpful in tracking assets for consumer redress.

<10>Third, the Act improves the FTC's ability to take effective action in cross-border cases by enhancing cooperation between the FTC and the Department of Justice in foreign litigation, confirming the FTC's remedial authority in cross-border cases, and clarifying the FTC's authority to make criminal referrals.[30] The Act permits the FTC to work with the DOJ in using additional staff and financial resources relating to FTC-related foreign litigation, such as freezing foreign assets and enforcing U.S. court judgments abroad.[31] The Act confirms the FTC's remedial authority in cross-border fraud and deception cases where injury or material conduct occurs within U.S. The FTC can apply all legal or equitable remedies, including restitution, available to it in cross-border cases. [32] Furthermore, the Act expressly authorizes the FTC to make criminal referrals for prosecution when violations of federal trade practice law also violate U.S. criminal laws.[33] This improves information sharing with foreign agencies that treat consumer fraud and deception as a criminal law enforcement

issue.

<11>Fourth, the Act strengthens the FTC's cooperation and relationship with foreign authorities by providing foreign staff exchange programs, authorizing expenditures on joint projects, and authorizing reimbursement from other law enforcement entities, including foreign agencies.[34] This gives the FTC more resources to fight against cross-border fraud and deception.

<12>Lastly, the Act requires the FTC to report to Congress within three years after the enactment of the Act, providing important information to Congress on FTC accountability and cross-border trends and needs. The report will describe the FTC's use of its new authority and recount the number and types of requests for information sharing and investigative assistance, the disposition of such requests, the foreign law enforcement agencies involved, and the nature of the information provided and received.[35]

IS THE U.S. SAFE WEB ACT'S GRANT OF POWER TO THE FTC TOO BROAD?

<13>The U.S. SAFE WEB Act raises concerns about the FTC's intrusion into U.S. citizens' privacy rights when foreign law enforcement agencies request investigative cooperation. These concerns are over the FTC's power to share confidential information with foreign law enforcers, delayed notice of process, third party voluntary disclosure, and the FTC's authority to access and disclose financial information.

<14>The first possible privacy concern raised by the Act involves the FTC's power to share confidential information with foreign law enforcers. Section 4(b) of the Act allows the FTC to conduct investigations and discovery to help foreign law enforcers in appropriate cases,[36] and §§ 4(a) and 6(a) authorize the FTC to share confidential information in its consumer protection files with foreign law enforcers,[37] subject to appropriate confidentiality assurances.[38] These provisions might lead to baseless intrusion into U.S. citizens' privacy rights when foreign law enforcers' allegations are unfounded.

<15>However, this concern seems remote. The FTC is not the first agency to have this authority; federal statutes have already granted several other federal agencies authority to share such information with foreign counterparts.[39] These agencies' practices have not created any real problems with regard to U.S. citizens' privacy rights or no such problems have been widely reported. Moreover, §§ 4(a) and 6(a) do not authorize any new privacy invasions because the information shared is from investigations already pending in the FTC.[40] Section 4(b) has a greater privacy impact than §§ 4(a) and 6(a),[41] however investigations and discovery under this section require the Commissioners approval.[42] Thus, the true privacy risk of the U.S. SAFE WEB Act may be minimal.

<16>A second possible cause for concern is delayed notice of process. Section 7 protects the confidentiality of FTC investigations by preventing or delaying notice of process to those under investigation if the FTC believes notification may produce an "adverse result."[43] This is similar to provisions of the proposed International Consumer Protection Act of 2003 ("ICPA"), which would grant the FTC power to access information about an individual but delay notice of process to the individual.[44] The Center for Democracy and Technology ("CDT") has criticized this ICPA provision because it might deprive an individual the right to challenge a subpoena.[45] Similar concerns might be raised with the U.S. SAFE WEB Act. Traditionally, when the government seeks records relevant to an authorized investigation from an individual, it can seize them with a court order.[46] The recipient of an order has the opportunity to challenge it.[47] However, the CDT's Associate Director has highlighted the specific concerns raised by the ICPA when an individual's information is sought though third-party subpoena:

> [M]ore and more records about individuals and companies are held by third parties – including [financial institutions] and online service providers – who may have no interest in seeking to ensure that a subpoena is narrowly focused, since the records do not pertain to them. Increasingly, the government is seeking to prohibit holders of data from disclosing to their customers the fact that the government has sought their records. This means that the person whose privacy is being breached has essentially no opportunity to challenge the subpoena.[48]

<17>These problems stemming from delayed subpoena notice become more serious in the international consumer protection context because "records will be disclosed to foreign governments, against whom redress may be extremely difficult if the records are misused."[49]

<18>Nevertheless, CDT's delayed notice concerns may not apply to the U.S. SAFE WEB Act. The ICPA would have authorized FTC cross-border cooperation in cases involving conduct that would not be

illegal if committed in the US.[50] In contrast, § 4 of the U.S. SAFE WEB Act explicitly states that the FTC provides investigative assistance to foreign law enforcers only if the assistance "concerns acts or practices that cause or are likely to cause injury to a significant number of persons," is limited to practices substantially similar to practices prohibited by any provision of laws administered by the FTC, and would not "prejudice the public interest of the United States."[51] Moreover, § 7 applies the delay of notice only when notification may cause an "adverse result."[52] The provision strictly confines the definition of "adverse result" to limited situations, such as endangering the life or physical safety of an individual, flight from prosecution, or the destruction of or tampering with evidence,[53] and there is the additional security of mandatory judicial approval for delaying notification and prohibiting disclosure.[54] Moreover, the provision sets upper limits for delaying notice at sixty days "if there is reason to believe that disclosure may cause an adverse result," or otherwise up to thirty days for each request, with a maximum of nine months.[55] Thus, concern over § 7's delayed notice provision seems attenuated.

<19>The U.S. SAFE WEB Act also raises concern about third party voluntary disclosure. Section 8 protects a limited category of entities[56] from liability for voluntary disclosures to the FTC about suspected fraud or deception, or about recovery of assets for consumer redress. However, the Act does not provide mechanisms for preventing these entities from abusing this right, nor does it impose liability or provide remedies for wrongful disclosure. Nevertheless, the Act's disclosure provision is similar to longstanding exemptions for financial institutions making disclosures of suspected wrongdoing to federal agencies.[57] The press has not reported that the American public is outraged by financial institutions abusing this right. In addition, permissible disclosures under § 8 are restricted to suspected fraud or deception, or for the purpose of recovery of assets for consumer redress.[58] For these reasons, the risk that information so disclosed will be abused under the U.S. SAFE WEB Act seems modest.

<20>One final concern about the Act relates to its disclosure of financial information provision. Section 10 adds the FTC to the RFPA's list of financial and market regulators allowed to share financial information.[59] This is similar to a provision of the proposed ICPA that would have authorized the FTC to disclose financial information. [60] The Electronic Privacy Information Center ("EPIC") was concerned that this ICPA provision would give the FTC authority to access bank reports and other financial data under the guise of fighting cross-border consumer fraud and deception.[61] The EPIC's concern may be relevant here. Under the U.S. SAFE WEB Act, the FTC would have "discretion to share financial information without any oversight to make sure it is shared appropriately."[62] There is no limit on what sort of information can be exchanged: the FTC could examine financial institutions' customer records, without notification to the customers, under the guise of examining records regarding the financial condition of the institution.[63]

<21>Concern over the FTC's authority to access and disclose financial information, however, may not be well founded. The FTC is one of only four federal financial and market regulators that have been authorized to share financial records.[64] The FTC would be subject to the same restrictions applied to other regulators. The U.S. SAFE WEB Act explicitly restricts sharing to only that "among and between the five member supervisory agencies."[65] Moreover, the Federal Trade Commission Act[66] already adds a safeguard—the FTC has no jurisdiction to investigate banks.[67] Thus, the concern over disclosure of financial information may be relieved. The concerns of privacy advocates about the FTC's expanded powers under the U.S. SAFE WEB Act may be somewhat exaggerated as the Act grants the FTC only limited powers.

FINDING A BALANCE BETWEEN LAW ENFORCEMENT INTERESTS AND PRIVACY INTERESTS

<22>The FTC's Internet investigation authority may be a double-edged sword. While the FTC's Internet investigation and information sharing authority would protect U.S. citizens from cross-board fraud and deception, it might also invade their privacy. Such potential for both favorable and unfavorable consequences begs the question: Has the U.S. SAFE WEB Act established an appropriate balance between law enforcement interests and privacy interests?

<23>The U.S. SAFE WEB Act may raise privacy concerns over the sufficiency of private information protection required of the FTC. The FTC has the duty to protect private information it collects from unlawful disclosure. The Privacy Act restricts federal agencies from disclosing private information from government records unless appropriate notice is given and individual consent is received.[68] The U.S. SAFE WEB Act protects certain entities from liability for voluntary disclosures of individuals' information relating to suspected fraud and deception,[69] and allows the FTC to share information with federal financial and market regulators.[70] The FTC will thus keep a huge collection of personal data that are aggregated, sifted, and networked at the national level. This clearly implicates privacy

concerns. The Act does not include any mandate requiring the FTC to treat collected information in a manner that complies with applicable federal law on privacy. It does not specify procedures for the FTC to protect individuals' constitutional and statutory privacy rights. Recent well-publicized incidents of breaches of databases containing personal data have increased public concern that the government may be unable to provide adequate protection for their personal data.[71] The FTC may also face growing pressure to ensure that the personal data they collect is protected.

<24>However, the FTC is not the only agency confronted with protecting private information and protecting such information is a challenge which likely predated the U.S. SAFE WEB Act. In the Internet age, adequate protection of private information is an increasing challenge for many federal agencies. In 2003, the Government Accountability Office estimated that about "70 percent of the agencies' systems of records contained electronic records and that 11 percent of information systems in use at those agencies contained personal information that was outside a Privacy Act system of records."[72] "Although the Privacy Act, the E-Government Act, and related OMB guidance set minimum requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles." [73] To cope with this challenge, the FTC has formed a Privacy Steering Committee to "oversee[] the FTC's own internal privacy policies and procedures" "for the collection, use, sharing, retention, storage, and disposal of FTC information, with particular emphasis on the treatment of personally identifiable information."[74] The committee will also ensure the FTC's compliance with federal privacy laws and guidelines.[75]

<25>In sum, the U.S. SAFE WEB Act does not provide any special mechanism to protect private information the FTC collects from unlawful disclosure, nor does it provide guidance on striking an appropriate balance between law enforcement interests and privacy interests. However, the FTC's on-going privacy protection measures may significantly relieve these privacy concerns.

CONCLUSION

<26>The U.S. SAFE WEB Act provides the FTC expanded enforcement authority to fight illegal spam, spyware, and cross-border fraud practices. Critics of the Act believe that this increase in authority may come at the price of reduced privacy rights for businesses and consumers. However, the Act strikes a careful balance between law enforcement interests and privacy interests, so these concerns are less serious than they first appear.

<< Top

Footnotes

1. Shaobin Zhu, University of Washington School of Law, J.D., 2008; Iowa State University, M.S., 1999; Renmin University of China School of Law, LL.B. and LL.M., 1994. Thank you to Professor Jane K. Winn and Professor Peter A. Winn of the University of Washington School of Law.
2. *The International Consumer Protection Act of 2003: Hearing on H.R. ____ Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. 2 (2003) (statement of the Hon. Timothy J. Muris, Chairman, Fed. Trade Comm'n), *available at* http://energycommerce.house.gov/reparchives/108/Hearings/09172003hearing1077/Muris1707.htm .
3. *Id.*
4. S. 1608, 109th Cong. §1(b)(1) (as introduced in Senate, July 29, 2005).
5. Federal Trade Commission, Cross-Border Fraud Complaints, January - December 2006, at 4, http://www.consumer.gov/sentinel/pubs/pdfs/Cross-Border%20CY-2006%20FINAL.pdf.
6. *Id.* at 3.
7. *Id.* at 6.
8. Cyber Security Industry Alliance, *U.S. SAFE WEB Act of 2005*, Cyber Security Industry Alliance Newsletter, Feb. 2006.
9. *Id.*.
10. S. 1608, *supra* note 4, at § 1(b)(4).
11. Pub. L. No. 109-455, 120 Stat. 3372 (codified in scattered sections of 15 U.S.C. and at 12

U.S.C. § 3412).

12. The White House, *Statement by the Press Secretary on Bill Signings*, Dec. 22, 2006, http://www.whitehouse.gov/news/releases/2006/12/20061222-1.html (last visited May 5, 2008).

13. FEDERAL TRADE COMMISSION, AN EXPLANATION OF THE PROVISIONS OF THE U.S. SAFE WEB ACT, at 1 (2005), http://www.ftc.gov/reports/ussafeweb/Explanation%20of%20Provisions%20of%20US%20SAFE%20WEB%20Ac [hereinafter "Act Explanation"].

14. *Id*. at 2-8.

15. 15 U.S.C. § 46(f) (2006).

16. "if--(A) the foreign law enforcement agency has set forth a bona fide legal basis for its authority to maintain the material in confidence . . . ." *Id*. at § 57b-2(b)(6).

17. *Id.* at § 46(j).

18. CID is a written request for information served by an authorized government entity such as the U.S. Attorney General or the FTC, prior to the institution of a civil or criminal proceeding, on any person who may have documents or information relevant to a civil or criminal investigation. *See* BLACK'S LAW DICTIONARY 262 (8th ed. 2004).

19. 28 U.S.C. § 1782 authorizes a federal district court to order a person to give testimony, a statement, or to produce a document or other thing for use in a proceeding in a foreign or international tribunal, including criminal investigations conducted before formal accusation. The order may be made pursuant to a letter rogatory issued, or request made, by a foreign or international tribunal or upon the application of any interested person.

20. Before the U.S. SAFE WEB Act, the FTC could not use a CID on behalf of its foreign counterparts to obtain information for use in their investigations. The Act now gives the FTC the power to gather evidence for its foreign counterpart, pursuant to 28 U.S.C. § 1782.

21. *Id.*

22. *Id.* at § 57b-2(f).

23. Act Explanation, *supra* note 13, at 8-12.

24. *Id.* at 8.

25. *Id.*

26. *Id.*

27. *Id.* at 10.

28. 15 U.S.C. § 57b-2b (2006).

29. 12 U.S.C. § 3412(e) (2006).

30. Act Explanation, *supra* note 13, at 13-17.

31. 15 U.S.C. § 56 (2006).

32. *Id.* at § 45(a).

33. *Id.* at § 46(j).

34. Act Explanation, *supra* note 13, at 17-20.

35. 15 U.S.C. § 44 NOTE (2006).

36. *Id*. at § 46(j).

37. *Id.* at § 46(f) and 57b-2(b)(6).

38. The FTC may share such confidential information "if . . . the foreign law enforcement agency has set forth a bona fide legal basis for its authority to maintain the material in confidence . . . ." *Id*. at 57b-2(a)(A).

39. Agencies with such information-sharing authority include the Securities and Exchange Commission, the Commodity Futures Trading Commission, and federal banking agencies. 15 U.S.C. § 78x(c) (2000); 7 U.S.C. § 12(e) (2000); 12 U.S.C. § 3109 (2006).

40. "[The] document, tangible thing, or transcript of oral testimony received by the Commission pursuant to compulsory process in an investigation…is to determine whether any person may have violated any provision of the laws administered by the Commission." 15 U.S.C. § 57b-2(b) (2006).

41. *Id*. at § 46(j).

42. "Upon a written request from a foreign law enforcement agency to provide assistance…the Commission may…conduct such investigation as the Commission deems necessary to collect information and evidence pertinent to the request for assistance." *Id*.

43. *Id*. at § 57b-2a (2006).

44. S. 1234, 108th Cong. § 206 (as introduced in the Senate, June 11, 2003; also called the Federal Trade Commission Reauthorization Act of 2003), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:sr127.108.pdf (last visited June 22, 2008).

45. *The International Consumer Protection Act of 2003: Hearing on H.R. ____ Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. (2003) (statement of Ari Schwartz, Associate Director, Center for Democracy and Technology), *available at* http://republicans.energycommerce.house.gov/108/Hearings/09172003hearing1077/Schwartz1710.htm (last visited Mar. 12, 2008) [hereinafter "Schwartz Testimony"].

46. The Fourth Amendment of U.S. Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV; Schwartz Testimony, *supra* note 43.

47. Schwartz Testimony, *supra* note 43.

48. *Id.*

49. *Id.*

50. *Id.*

51. 15 U.S.C. § 46 (2006).

52. *Id*. at § 57b-2a.

53. "(g) ADVERSE RESULT DEFINED.--For purposes of this section the term 'adverse result' means--"(1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) the destruction of, or tampering with, evidence; (4) the intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or proceeding related to fraudulent or deceptive commercial practices or persons involved in such practices, or unduly delaying a trial related to such practices or persons involved in such practices, including, but not limited to, by-- (A) the transfer outside the territorial limits of the United States of assets or records related to fraudulent or deceptive commercial practices or related to persons involved in such practices; (B) impeding the ability of the Commission to identify persons involved in fraudulent or deceptive commercial practices, or to trace the source or disposition of funds related to such practices; or (C) the dissipation, fraudulent transfer, or concealment of assets subject to recovery by the Commission." 15 U.S.C. § 57b-2a (2006).

54. *See Id.* at § 57b-2a (b)(1).

55. *Id*. at § 57b-2a.

56. "(d) APPLICATION.--This section applies to the following entities, whether foreign or domestic: (1) A financial institution as defined in section 5312 of title 31, United States Code. (2) To the extent not included in paragraph (1), a bank or thrift institution, a commercial bank or trust company, an investment company, a credit card issuer, an operator of a credit card system, and an issuer, redeemer, or cashier of travelers' checks, money orders, or similar instruments. (3) A courier service, a commercial mail receiving agency, an industry membership organization, a payment system provider, a consumer reporting agency, a domain name registrar or registry acting as such, and a provider of alternative dispute resolution services. (4) An Internet service provider or provider of telephone services." *Id*. at § 57b-2b.

57. *E.g.*, 12 U.S.C. § 3413 (1998) (authorizing "[d]isclosure of financial records not identified with particular customers" to a "supervisory agency pursuant to exercise of supervisory, regulatory, or monetary functions with respect to financial institutions, holding companies, subsidiaries, institution-affiliated parties, or other persons").

58. *Id*.

59. 12 U.S.C. § 3412(e).

60. *The International Consumer Protection Act of 2003: Hearing on H.R. ____ Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. (2003) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center), *available at* http://www.epic.org/privacy/whois/testimony.html (last visited Mar. 12, 2008).

61. *Id*.

62. 12 U.S.C. § 3412(e) (2006).

63. *Id.*

64. "[T]he exchange of financial records, examination reports or other information with respect to a financial institution, holding company, or any subsidiary of a depository institution or holding company, among and between the five member supervisory agencies of the Federal Financial Institutions Examination Council, the Securities and Exchange Commission, the Federal Trade Commission, and the Commodity Futures Trading Commission is permitted." 12 U.S.C. § 3412(e) (2006).

65. *Id.*

66. 15 U.S.C §§ 41-58 (2006).

67. 15 U.S.C. § 46(b) (2006).

68. Privacy Act, 5 U.S.C. § 552a (2004).

69. 15 U.S.C. § 57b-2b (2006).

70. 12 U.S.C. § 3412(e) (2006).

71. Attrition.org, *Errata: Data Loss Archive and Database*, http://attrition.org/dataloss/ (last visited May 5, 2008); Robert Lemos, *UCLA Alerts 800,000 to Data Breach*, SecurityFocus, Dec. 12, 2006, http://www.securityfocus.com/news/11429 (last visited May 5, 2008); Rachel Konrad, *Burned by ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance*, InformationWeek, Feb. 24, 2005, http://www.informationweek.com/showArticle.jhtml?articleID=60403319 (last visited Mar. 13, 2008).

72. Government Accountability Office, *Privacy: Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information*, GAO-08-795T, June 18, 2008, at 14 (Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate), available at http://www.gao.gov/new.items/d08795t.pdf (last visited Jun. 25, 2008).

73. *Id*. at 3.

74. Deborah Platt Majoras, Chairman, Fed. Trade Comm'n, Building A Culture of Privacy and Security – Together, Address at the IAPP Privacy Summit (Mar. 7, 2007), at 2-3, http://www.ftc.gov/speeches/majoras/070307iapp.pdf.

75. *Id.* at 3.