Notre Dame Journal of Law, Ethics & Public Policy

Volume 14
Issue 2 *Symposium on Privacy and the Law*

Article 6

1-1-2012

Consumer Privacy in Electronic Commerce: As the Millennium Approached, Minnesota Attacked, Regulators Refrained, and Congress Compromised

Mark E. Budnitz

CONSUMER PRIVACY IN ELECTRONIC COMMERCE: AS THE MILLENNIUM APPROACHED, MINNESOTA ATTACKED, REGULATORS REFRAINED, AND CONGRESS COMPROMISED

MARK E. BUDNITZ*

INTRODUCTION

The notion that individuals are entitled to privacy has been present in legal scholarship,[1] statutes, and case law[2] for a century. Brandeis articulated it as "the right to be let alone."[3] Supreme Court justices state as a given that "there is a zone of privacy surrounding every individual, a zone within which the State may protect him."[4] In speaking of a "right" to privacy, the law recognizes a deep human need,[5] and acknowledges that the expectation of privacy has been accepted as part of the mores of our society. That expectation carries over into various aspects of life,

* Professor of Law, Georgia State University College of Law. The author gratefully acknowledges the research assistance of Julie Simmermon. In addition, the author thanks Georgia State University College of Law for its financial support.

1. *See, e.g.*, Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

2. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 478 (1928). *See also* Robert Gellman, *Does Privacy Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 195-202 (1998) (discussing tort law theories to recover from invasions of privacy).

3. Olmstead, 277 U.S. at 478 (Brandeis, J., dissenting) ("[The makers of the Constitution] sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.").

4. Cox Broad. Corp. v. Cohn, 420 U.S. 469, 487 (1975). The quoted language refers to the State protecting the individual from "intrusion by the press." *See also* Los Angeles Police Dep't v . United Reporting Publ'g Corp., 120 S. Ct. 483 (1999) (upholding a California statute which restricted the public's access to arrested persons' names and addresses). The state's justification for the statute was that it protected the privacy of victims and those arrested. *See id.* at 492 (Stevens, J., dissenting).

5. *See* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1053 (noting Alan Westin's theory that a person's desire for privacy may be biological).

and many surveys[6] have shown that consumers' expectation of privacy encompasses their transactions with businesses.

Nevertheless, there is no generally accepted definition of privacy. Whereas the "right to be let alone" focuses on the individual, others prefer a definition which views privacy in the context of society.[7] Those focusing on the individual characterize invasion of privacy as "an offense to your dignity."[8] They point to people's concerns about personal safety and identity theft.[9] Those preferring a definition that takes into consideration the context in which privacy invasions occur emphasize the power of government and its many sources of information about its citizens[10] and the insatiable appetite of business for collecting, using, and sharing data about consumers.[11] In addition, there is a debate among legal scholars over whether privacy should be protected by liability rules or by treating privacy as a commodity to which a person has a property right subject to negotiation with parties who want an interest in that property.[12]

The ability of government and business to collect, store, analyze, retrieve, and transmit personal information has been greatly enhanced by advances in computer technology.[13] One of the features of much of this technology is its ability to "search without disturbing."[14] A persons' privacy is invaded, and they do not have any idea it is happening. Professor Lessig has identified several significant effects which he asserts have resulted from the increased capacity to collect, store, retrieve, and transmit per-

6. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 80 (1998); Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. REV. 847, 849 (1998); Sovern, *supra* note 5, at 1056-64.

7. *See* Gellman, *supra* note 2, at 193.

8. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 147 (1999). *See also* Sovern, *supra* note 5, at 1053-54.

9. *See* Sovern, *supra* note 5, at 1054.

10. *See* SWIRE & LITAN, *supra* note 6, at 6; Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 560-61 (1999). An example of a legislative response to this concern is the Privacy Act, 5 U.S.C. § 552(a)(1999), which establishes rules for the collection, use and disclosure of personal information held by federal agencies, with a special focus on using computers to invade privacy. *See also* Gellman, *supra* note 2, at 195-97.

11. *See* Sovern, *supra* note 5, at 1034-36. An example of a legislative response to this concern is the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (West 1998 & Supp. 1999).

12. *See* LESSIG, *supra* note 8, at 160-61.

13. *See* Berman & Mulligan, *supra* note 10, at 554-56.

14. LESSIG, *supra* note 8, at 149.

sonal information. People have lost the "benefit of innocence."[15] Formerly, it was comparatively easy to live anonymously. However, now the burden is on the individual to prove that, despite the questions raised by putting certain facts about the individual in a particular context, the true story is different from what appears from viewing the data in that context. As the ability to monitor our behavior increases, there will be a decrease in the diversity of values held by our citizens because those collecting the data will be better able to impose their values upon us.[16] Based on their ability to create profiles of each consumer, businesses will be able to discriminate, targeting certain groups of consumers for some products and prices, and ignoring or offering other options to consumers with different profiles.[17] This creates the danger of recreating "systems of status"[18] based on "social or economic criteria."[19] This may erode the relative equality that consumers in a more anonymous society enjoy when they purchase goods and services.[20]

Consumers' ever increasing use of electronic commerce has heightened concerns over privacy.[21] While consumers shop on the Web in the seclusion and privacy of their homes, increasingly they realize that companies can easily invade that privacy. Perhaps the very paradox of losing one's privacy while in a place which we regard as a refuge from life's involuntary intrusions increases consumers' anxiety. Incidents involving invasions which occurred within a few weeks of each other at the turn of the millennium illustrate that consumers have a legitimate basis for concerns about privacy. A person calling himself Maxim, believed to reside in Eastern Europe, stole more than 300,000

---

15. *Id.* at 152.

16. *See id.* at 153.

17. *See id.* at 153-55. *See also* Jennifer L. Alvey, *Internet Privacy: Consumer Fears About Online Privacy, Individual Profiling Threaten E-Commerce*, 68 U.S.L.W. 2318 (Nov. 30, 1999).

18. LESSIG, *supra* note 8, at 155.

19. *Id.* at 154.

20. *See id.*

21. *See* SWIRE & LITAN, *supra* note 6, at 80; Sovern, *supra* note 5, at 1060-61; Simson L. Garfinkle, *Someone is Watching*, ATLANTA J.-CONST., Jan. 16, 2000, at D1. Others assert that privacy risks are greatly exaggerated, as a person's credit card account number is far more likely to be stolen when he or she gives the card to a waiter. *See* Lesley Campbell, *A New Oracle: Dreams of Visions in the Future*, SUNDAY HERALD, Sept. 19, 1999, at 21, *available in* 1999 WL 22705346; *Technology-Insurers Insist They're Safe from the Hackers*, POST MAG., Sept. 9, 1999, at 13, *available in* 1999 WL 9020504. These observers ignore incidents such as the theft of 300,000 credit card account numbers from one company's database by a hacker who presumably was not a waiter, or who at least did not steal the information while waiting on tables. *See infra* text accompanying note 22.

credit card files from an Internet music seller.[22] When the seller refused Maxim's demand for $100,000, he published 25,000 of the files, containing credit card numbers, names, and addresses, on a Web site he had set up. Maxim claimed he had found a security defect in the software that the seller used to protect financial information. One industry representative downplayed the significance of the incident because it apparently involved access to the company's database rather than someone intercepting transactions from the Internet.[23] This occurrence illustrates the close connection between security and privacy. It also shows that data is vulnerable not only when it is transmitted through cyberspace from the consumer's computer to the seller, but also when it is in the seller's database. While it may be comforting to some in the industry that the theft seemingly occurred from the seller's database, it is unlikely that the distinction between thefts from cyberspace transmissions and databases will ease consumer concerns. It certainly did not lessen the fears of the Connecticut Attorney General who reacted by announcing he was considering "'measures and incentives'" to ensure better protection of the personal information which Web sellers collect.[24] While this article focuses on the legitimate consumer data practices of businesses, and not on the conduct of thieves and extortionists, consumers probably add this incident to their general mental image of e-commerce as a risky venture rather than differentiating among different types of privacy invasions.

There were several other occurrences at the turn of the new century as well. Amazon.com has made it a practice to publish its privacy policy even though no law required it to do so. Nevertheless, in December, 1999, a security expert filed a formal complaint with the FTC, alleging that one of Amazon.com's subsidiaries collects considerably more personal consumer information than its published policy disclosed.[25] The FTC itself took the initiative in another case in which it accused an online auction house of unfair or deceptive practices by unlawfully taking a competitor's list of its customers' e-mail addresses, sending deceptive spam to persons on that list, and falsely representing

22. *See* John Markoff, *An Online Extortion Plot Results in Release of Credit Card Data*, N.Y. TIMES, Jan. 10, 2000, at 1.

23. *See* Mark Harrington, *Hacker Sparks E-Tailer Concerns*, NEWSDAY, Jan. 11, 2000, at A37.

24. *Id.*

25. *See* John Markoff, *Bitter Debate on Privacy Divides Two Experts*, N.Y. TIMES, Dec. 30, 1999, *available in* 1999 WL 31761916.

that the competitor authorized the e-mailing.[26] The auction house obtained the list by registering with its competitor, the major online auction e-Bay, agreeing to comply with eBay's "User Agreement and Privacy Policy" which prohibited the auction house from using eBay's customer list for unauthorized purposes such as sending spam. The case illustrates that consumers must be concerned, not only with the use of information by companies with whom they do business and to whom they provide information, but also with the unauthorized actions of others with whom that business has contact. The case also demonstrates that the agreements a company imposes on others with whom it shares information are not always honored. ChoicePoint's contract with the Pennsylvania Department of Transportation was canceled when it transmitted confidential information from drivers' records to insurance companies over the Internet, in violation of its contract with the state.[27] This incident illustrates the close connection between privacy collection and sharing between government and business.[28] It is also another example of the violation of a confidentiality agreement.

DoubleClick uses advertising banners on Web sites to track persons who visit Web sites, but until January 2000, has known who the persons are only by way of an anonymous number assigned to each person.[29] Starting in January, the company began to use technology that enables it to link the person's conduct on the Web with the person's name, address, and off-line shopping history.[30] Among the Web sites from which DoubleClick collects information are Web sites which provide medical information.[31] It has more than 100 million files on visitors to these sites.[32] DoubleClick transfers information about each person's visit to another location. Therefore, if the visitor went to a page on the site which provided information about diabetes, that would be included in the company's database on that person. Information provided by the visitor in health evaluations

26. *Online Auction Site Settles FTC Privacy Charges*, (visited Jan. 18, 2000) <http://www.ftc.opa/2000/01/reverse4.htm> (the online auction firm agreed to settle the case).

27. *See* Editorial, *ChoicePoint Loses Contract Over Privacy*, ATLANTA J.-CONST., Jan. 7, 2000, at F2.

28. *See* Budnitz, *supra* note 6, at 872-74.

29. *See* Ryan Tate, *DoubleClick Damage Control*, UPSIDE TODAY, Feb. 2, 2000, *available in* 2000 Westlaw 4724326; Editorial, *Double Privacy Trouble*, USA TODAY, Jan. 31, 2000, at 16A [hereinafter Editorial]

30. *See* Editorial, *supra* note 29.

31. *See* John Schwartz, *Medical Web Sites Faulted on Privacy*, WASHINGTON POST, Feb. 1, 2000, at E1.

32. *See id.*

provided by the sites also is collected. Reaction was swift. The Center for Democracy and Technology urged people to bombard DoubleClick with e-mail complaints,[33] and an individual filed a lawsuit alleging that DoubleClick had obtained and sold personal information unlawfully.[34] The lawsuit requested an injunction to stop the company from continuing to collect information until it obtained explicit permission from visitors to the affected sites.

Finally, First Union bank announced it was suing a company engaged in "screen scraping."[35] Screen scrapers are companies that obtain a consumer's authorization to take information from another company's site for the purpose of consolidating the information all in one place so consumers can have all their account information at various banks on one site and can pay their bills through that site. First Union claimed the screen scraper was acting without the bank's consent and not adequately safeguarding consumer information. This lawsuit illustrates that when considering the privacy of financial information held by banks about consumers, it is necessary to look well beyond the banks themselves in order to have a complete picture of whether the data is truly protected.

The increased importance of consumers engaging in e-commerce and their privacy concerns have led to consideration of legislation that would protect consumers whether they shop online or off-line. This article explores important developments in consumer privacy which occurred during 1999 with an emphasis on e-commerce. As will be seen, however, it is impossible to limit the consideration to e-commerce, for the developments in e-commerce have had a major impact on traditional commerce as well. These developments illustrate the powerful influence of consumers' belief, not only that they have a right to be "let alone," but also that, once they share personal information with a company, they should retain some degree of control over that information.[36] The events of 1999 also illustrate that "privacy

33. *See* Tate, *supra* note 29. *See also* Center for Democracy and Technology, *DoubleClick Has Double-Crossed the Net* (visited Feb. 2, 2000) <http://www.cdt.org/action/doubleclick.shtml>.

34. *See New Media*, COMMUNICATIONS DAILY, Jan. 31, 2000, *available in* 2000 WL 4694404.

35. Carol Power, *First Union Confirms It is Suing a "Screen Scraper"*, AM. BANKER, Jan. 19, 2000, at 5.

36. *See* Berman & Mulligan, *supra* note 10, at 556 n.11.

issues are fundamentally matters of values, interests, and power."[37]

Privacy for consumers on the Internet has become an issue of increasing importance as electronic commerce has shown the promise of profitability. Until 1999, government primarily assumed a passive role, issuing reports, warning business they were monitoring e-commerce's activities, but insisting that at this early stage of development, the best course was for industry to operate free of government interference. In 1999, that began to change. This article focuses on three developments which illustrate various aspects of government involvement. First, the article examines a lawsuit brought by the Attorney General of Minnesota against US Bank. The lawsuit alleged, in part, that the bank violated the state's Consumer Fraud Act by promising consumers on its Web site that their personal information would be kept confidential, while selling that information to a third party marketer. Second, the article reviews actions and pronouncements in 1999 of two regulatory agencies, which edged closer to taking concrete action on privacy, while remaining ambivalent. Third, the article analyzes legislation containing significant consumer privacy protection which Congress passed in 1999 and compares it with other bills pending in Congress. This inquiry yields insights into some of the essential issues in making consumer privacy policy, and suggests the need for additional legislation to protect consumers while allowing business to flourish in a robust e-commerce environment.

Government regulators have been urging banks and other industries to post privacy policies on their Web sites, but have not provided guidance on what those policies should be. US Bank followed the regulators' advice, posted a policy, and made it a strong policy purporting to keep all consumer information confidential, whatever the source. The Minnesota Attorney General's lawsuit illustrates the perils of following this course of action. The article explores the strength of the Attorney General's case under the state's Consumer Fraud Act. Even assuming the bank violated its posted policy, it is questionable whether the state's law is adequate to force a company to comply with its posted policy. The consent agreement is analyzed, revealing a rather narrow remedy was achieved. Finally, the systemic limits of litigation are described. In light of the above, the article examines the need for legislation.

37. Gellman, *supra* note 2, at 195 (referring to remarks made by Alan Westin).

Federal agencies have issued several pronouncements, epistles of advice, reports, and guidelines on privacy, none having the force of law, but all admonishing businesses to watch their step. Their pronouncements suggest their ambivalence: acknowledging there is a significant potential problem which may well require action by regulatory agencies, but strong reluctance to take any action at this early stage for fear of unduly restricting a newly emerging medium for engaging in commerce. In short, they don't want to kill the goose that may be laying the golden egg, but are not sure how pure the gold in that egg is. Agency reluctance is understandable, but the result of their various statements is a lack of uniformity, consistency, and specificity. In addition, since none of the statements have the force of law, businesses lack a legal incentive to seriously examine and strengthen their privacy policies. It is doubtful that consumer preferences for privacy and public reactions to scattered media exposés are sufficient to ensure a satisfactory degree of privacy.

Litigation has a limited reach and regulatory agencies have refused to act. The Republican-controlled Congress is the last place many would have thought consumer privacy would find a sympathetic audience. Nevertheless, not only have several consumer privacy bills been submitted, but privacy played a central role in Congress' consideration of the legal restructuring of the entire financial services industry.[38] The result is important new legislation granting consumers a modicum of privacy when dealing with financial institutions. The article examines this landmark statute, compares it to the approaches taken in other pending bills and assesses the need for additional legislation to ensure consumer privacy. The new law and pending bills illustrate how difficult it is to identify industry's need and desire to collect and share information and consumers' need and desire to have their privacy protected. Even if these are properly identified, striking the proper balance among the competing interests presents difficulties as well. Nevertheless, the article recommends legislation to provide greater protection in certain areas.

I. *HATCH V. US BANK*: THE POSSIBILITIES AND LIMITATIONS OF AGENCY LAWSUITS

A. *The Complaint*

In June, 1999, Mike Hatch, the Attorney General of Minnesota, brought what was apparently the first lawsuit which alleged,

38. *See* Michael Schroeder, *Legislators Reject a Plan to Strengthen the Protections Involving Consumer Privacy*, WALL ST. J., Oct. 18, 1999, at A50.

inter alia, that a company had violated the law by violating a privacy policy which it had posted on its Web site. An examination of that litigation illustrates many of the potentialities of litigation brought by a state agency, and also the severe limitations attendant upon such actions.

According to the Complaint,[39] US Bank and its parent holding company US Bancorp, ("the bank") sold confidential information about their customers to MemberWorks. MemberWorks is a telemarketing company which sells memberships in a dental and health service.[40] The bank was paid $4 million plus a commission of 22 percent of net revenue based on MemberWorks' sales to the bank's customers. From January 1, 1996 to the filing of the Complaint, the bank provided information on 600,000 checking account customers and 330,000 credit card customers. Under agreements between the bank and MemberWorks, the bank provided MemberWorks with seventeen items of personal information, including social security numbers, account status and frequency of use, a "behavior score," a "bankruptcy score," gender, and marital status.[41] In its answers to the Attorney General's interrogatories, MemberWorks acknowledged receiving many of these items. The Complaint notes that some of the information provided to the telemarketer was based on information other than the bank's "first-hand experience with their customers."[42] The implication is that the bank may have received at least some of this information, such as the bankruptcy score and behavior score, from third parties.

The sharing of information did not end when MemberWorks received it; MemberWorks in turn passed the information on to telemarketing vendors whom they hired to conduct the actual sales calls. The Complaint alleges that MemberWorks and their vendor representatives used this information when making their calls as well as for bulk mailing solicitations.[43] Customers receiving the calls did not know the telemarketer already had their credit card numbers or checking account numbers. If the customer asked if the telemarketer had

39. Complaint, Attorney Gen. v. US Bank Nat'l Ass'n ND (visited Feb. 2, 2000) <http://ag.state.mn.us/home/files/news/pr_usbank_06091999.html> [hereinafter "Complaint"].

40. The program offered X-rays and oral exams free or for a nominal charge, discounts for dental services, and access to a network of participating dentists. *See id.* at ¶ 45 The Complaint also involves Coverdell & Company, a subsidiary of MemberWorks. *See id.* at ¶ 14.

41. *Id.* at ¶ 15.

42. *Id.* at ¶ 19.

43. *See id.* at ¶ 44.

the customer's account number, the caller was instructed to follow a script in which the customer was told; "No, I personally do not have your account number."[44]

Although the Complaint alleges various wrongful practices and violations of various statutes, of relevance to this article are the allegations relating to electronic commerce. The bank had posted the following privacy policy on its Web site:

> US Bancorp and its family of financial service providers understands that confidentiality is important to you and essential in our business. It is our policy that all personal information you supply to us will be considered confidential. This policy holds true no matter how we receive your personal information; over the phone, at our branches, through our ATMs or on-line at this Web site. (May 25, 1999).[45]

The Complaint alleges that the bank "created an expectation that its Minnesota consumers have a right to financial privacy."[46] Presumably, this expectation was created by the privacy policy posted on the Web. Despite this clear and sweeping privacy statement, credit card customers received notice that their privacy might not be all that sacred to the bank. The credit card agreement provided that the bank "share[s] information within our organization"[47] unless the customer wrote to say he or she did not want the information shared. In addition, "[p]eriodically we may share our cardholder lists with companies that supply products and services that we feel our customers will value . . . . You may request that your name and information not be given to these companies by writing."[48]

The Complaint alleges in Count II that the bank violated the Minnesota Prevention of Consumer Fraud Act and Deceptive Trade Practices Act (Minnesota Fraud Act). That law provides that the use of "any fraud, false promise, misrepresentation, misleading statement or deceptvie practice, with intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoinable as provided herein."[49] The Complaint then notes that the privacy statement on the Web site does not advise consumers that their confidential information will be

---

44. *Id.* at ¶ 26.
45. *Id.* at ¶ 4.
46. *Id.* at ¶ 39.
47. *Id.* at ¶ 41
48. *Id.*
49. MINN. STAT. ANN. § 325F.69 (1) (West 1995).

sold to third parties, nor that they may opt-in or opt-out of the sale of this information, or how the bank chooses to use the information. Whereas the credit card agreement provided information about affiliate sharing of information, "[b]y titling the paragraph 'Affiliate Sharing,' consumers are deceived and/or misled regarding the sale of information to unrelated, non-affiliated entities."[50]

The Complaint does not explicitly allege that all of the allegations in Count II, or in the preceding paragraphs of the Complaint which are incorporated into this count, amount to a violation of the Act. Rather, the Complaint alleges under this Count that the bank's "sale of personal, confidential *information obtained from consumers* in the course of a banking relationship"[51] is a deceptive and misleading act. What is not clear is whether the Attorney General also would regard the bank's sale of information about the consumer obtained from its own investigation or from third parties would be a deceptive and misleading act.

The paragraph in the Complaint alleging that the sale of information obtained from consumers is a deceptive and misleading act also alleges that the same conduct violates Minnesota consumers' common law right to privacy.[52] The Complaint cites *Lake v. Wal-Mart Stores, Inc.*, in support of this contention.[53] The Complaint then alleges that "[t]he systematic violation of Minnesota's common law right of privacy is a violation" of the Minnesota Fraud Act.[54]

In response to the Complaint, the bank denied the allegations that it violated consumer protection and privacy laws.[55] The bank admitted it had cooperative marketing agreements with MemberWorks and other companies. The bank touted its commitment to consumer privacy. "U.S. Bancorp takes customer privacy very seriously, and has strict poicies in place to protect that privacy."[56] Furthermore, the bank insisted that "[o]ur partners at no time have access to customer accounts."[57] Soon after the Complaint was filed, U.S. Bancorp announced it was termi-

50. Complaint, *supra* note 39, at ¶ 65

51. *Id.* at ¶ 68 (emphasis added).

52. *See id.*

53. *See id.* at 68, *citing* Lake v. Wal-Mart Stores, Inc., 582 N.W. 2d 231 (Minn. 1998).

54. Complaint, *supra* note 39, at ¶ 74.

55. *See* U.S. Bancorp News Release, *U.S. Bancorp Denies Minnesota Attorney General's Allegations* (visited Feb. 2, 2000) <http://199.230.69/cgi-bin/micro. . .-1999/0000960133&EDATE=JUn+9,+1999>.

56. *Id.*

57. *Id.*

nating contracts with companies that marketed non-financial products.[58] Bank of America and Wells Fargo also said they would end such agreements.[59]

B. *Critique of the Complaint*

An examination of the Complaint illustrates the types of benefits and disadvantages which litigation poses for both those using a lawsuit to promote consumer privacy and those businesses which are accused of violating that privacy where no federal or state statute specifically governs consumer privacy in electronic commerce. This examination demonstrates the need for a statute tailored to consumer electronic commerce which takes into account the needs of all of the affected parties.

One challenge for those drafting the Complaint for the Minnesota Attorney General must have been finding a legal basis for the allegations that posting a privacy policy on the Web while not following that policy in practice violated the law. The Complaint never comes right out and says the bank broke any law by doing such. Rather, as described above, the Complaint's specific allegation was that the sale of "personal, confidential" information the bank obtained from consumers "in the course of a banking relationship . . . is a deceptive and misleading act" and violated the common law right of privacy.[60]

One can only speculate why the Complaint is framed in this way, but it is instructive to examine the difficulties posed by attacking the bank directly for violating a policy posted on its Web site. The Attorney General might have argued that posting a policy on the Web and not following it is a breach of the bank's contract with its customers. This contention, however, would have required proving that the policy posted on the Web site is part of the contract between the customer and the bank. Although the Uniform Commercial Code's Article 2 does not apply to this case because it did not involve a "transaction in

58. *See* U.S. Bancorp, *A Letter from the Chairman, President and CEO, Usbancorp* (visited June 11, 1999) <http://www.usbank.com/customer_privacy/61199.html> ("Customer privacy is at the core of our business, and we did not misuse customer information . . . . There is nothing we value more than the trust you put in us. When that trust is called into question, it's something we take very seriously.").

59. *See* Tim Huber, *U.S. Bancorp, Minnesota Attorney General Settle Customer Privacy Suit*, KNIGHT-RIDDER TRIB. BUS. NEWS, *available in* 1999 WL 17353777; *Bank of America Announces Privacy Position Concerning Third-Party Marketers*, (visited Apr. 10, 2000) <http://www.bankamerica.com/news/news660.html>.

60. Complaint, *supra* note 39, at ¶ 68.

goods,"[61] the UCC's provisions for sales of goods provides us with the type of analysis courts typically use. The contract of the parties "means the total legal obligation which results from the parties' agreement as affected by this Act and any other applicable rules of law."[62] "Agreement" means "the bargain of the parties in fact as found in their language or by implication from other circumstances including course of dealing or usage of trade or course of performance."[63]

Whether the privacy policy became part of the contract between the parties may depend on whether the language in any written agreement between them contains language incorporating by reference the practices and policies of the bank. If such language was present, the Attorney General had a strong argument that the bank breached its contract.

If there were no such language, the Attorney General would have to rely on "other circumstances" such as usage of the trade, course of dealing, and course of performance. Presumably, nothing in the language of any written agreements between the bank and its customers referred to or incorporated by reference the bank's privacy policy as posted on its Web site. "Usage of trade" means a practice "having such regularity of observance . . . as to justify an expectation that it will be observed with respect to the transaction in question."[64] Although in the future the posting of privacy policies may come within this definition, in June of 1999, the Attorney General would have had difficulty proving a usage of trade. A course of dealing refers to previous transactions between the parties which establish a common basis of understanding.[65] A course of performance involves the parties' performance of the contract which the other party accepts or acquiesces in.[66] It is doubtful that the posted privacy policy comes within either of these two possible categories. If the posted privacy policy is not part of the agreement, then it is not part of the contract, the bank's legal obligation, unless some other law makes it so. From the information provided in the Complaint, it is unclear whether the posted policy became part of the contract between the bank and the consumer. If it did not become part of the contract, the bank did not breach any contract with the consumer. On the other hand, if it was not part of the contract and the policy contained limitations and qualifica-

61. U.C.C. § 2-102.
62. U.C.C. § 1-201(11).
63. U.C.C. § 1-201(3).
64. U.C.C. § 1-205(2).
65. *See* U.C.C. § 1-205(1).
66. *See* U.C.C. § 2-208(1).

tions of the circumstances under which it would protect the confidentiality of its information about the consumers, the consumer would not be bound by those restrictions. If the consumer could find a legal basis for arguing the bank's practices violated her right to privacy, the policy would not constitute a waiver or limitation of her right.

The Attorney General may have considered alleging common law misrepresentation. To succeed, however, he would have had to prove, inter alia, that consumers justifiably relied upon the misrepresentations in the posted privacy policy.[67] This would require the Attorney General to prove three things: that consumers went to the bank's Web site and read the privacy policy; that consumers relied on that privacy policy when entering into transactions with MemberWorks; and that such reliance was reasonable.

Instead of alleging that the bank breached its contract with consumers or engaged in common law misrepresentation, the Attorney General alleged violations of three Minnesota statutes. Each of these presented its own challenges and illustrate the need for legislation specifically designed to balance the privacy needs of consumers against the information sharing needs of industry. One of these statutes is the Minnesota Consumer Fraud Act. That law prohibits the employment of "any fraud, false promise, misrepresentation, misleading statement or deceptive trade practice."[68] A major advantage of proceeding under the Minnesota Fraud Act instead of breach of contract or misrepresentation is that it does not require the plaintiff to prove that "any person has in fact been misled, deceived, or damaged thereby."[69] The Attorney General, however, may have faced an obstacle in fitting the posted privacy policy within the scope of the statute. The Act applies to any of the above conduct which is committed "in connection with the sale of any merchandise."[70] The statute formerly defined "merchandise" as "any objects, wares, goods, commodities, intangibles, real estate, loans, or services."[71] In the *Boubelik* case, the Minnesota Supreme Court held that the Act did not apply to bank loans because the statute did not include such loans in its definition of "merchandise," and bank loans were not "intangibles" or "services."[72] The legislature

67. *See* Yost v. Millhouse, 373 N.W.2d 826 (Minn. Ct. App. 1985).
68. MINN. STAT. ANN. § 325F.69(1) (West 1995).
69. *Id.*; *see also* Lesage v. Norwest Bank, 409 N.W.2d 536 (Minn. 1987).
70. § 325F.69(1).
71. § 325F.68.
72. Boubelik v. Liberty State Bank, 553 N.W.2d 393, 403 (Minn. 1996).

responded by amending the statute to include loans.[73] *Boubelik* adopted a narrow interpretation of the statute which could have hindered the Attorney General. The court seemed to be saying that unless a product were specifically listed in the definition of "merchandise" or could be characterized as a service or intangible, it was not covered by the statute. Some of the consumers of U.S. Bank undoubtedly obtained loans from the bank. The Attorney General could have argued that the privacy policy was related to their bank loans and consequently the policy was subject to the Consumer Fraud Act. But it is not clear that the bank would be subject to the Act in regard to those consumers who had not taken out bank loans.

Boubelik is not the final word on the meaning of "merchandise" under the Act, however. In the *Force* case, a federal district court distinguished *Boubelik*.[74] The court pointed out that the *Boubelik* decision rested on the fact that the Act speaks in terms of the "sale of any merchandise" and a bank extending a loan is not "selling" money.[75] The *Force* court faced the question of whether the sale of insurance was covered by the Act. The court relied on another Minnesota case that found that the sale of investment contracts is governed by the statute because the definition of merchandise includes commodities and intangibles.[76] The court found the sale of insurance to be comparable to the sale of investment contracts. Holding more promise for the Attorney General, moreover, was the court's reference to a New Jersey decision in which the court felt free to include transactions not specifically listed in the statute because remedial statutes such as these cannot obtain their objectives if persons could evade them merely by devising new fraudulent schemes which the statute had failed to mention.[77] In litigating against U.S. Bank, the Attorney General may have found that the court sided with the approach taken by the *Force* court. He ran the risk, however, of the court favoring *Boubelik*'s narrow construction, and granting a motion to dismiss.

When the recently enacted federal Financial Institutions Modernization Act of 1999 becomes effective in November,

---

73. *See id.* at 403, n. 18.

74. *See* Force v. ITT Hartford Life & Annuity Ins. Co., 4 F. Supp. 2d 843 (D. Minn. 1998).

75. *Id.* at 858-59.

76. *See id.* at 859 (relying on Jenson v. Touche Ross & Co., 335 N.W.2d 720, 726 (Minn. 1983)).

77. *See id.*, (citing Lemelledo v. Beneficial Management Corp., 696 A.2d 546, 551 (N.J. 1997)).

2000,[78] U.S. Bank will have a duty to disclose its privacy policy. When the Attorney General brought his suit, however, the law had not yet been enacted, raising the question of whether the bank had a duty to disclose that it did not keep customer information confidential. If it did not have that duty, then arguably, it did not violate the Consumer Fraud Act by this failure to disclose. The *Boubelik* decision held that a company does not have a duty to disclose material facts about a transaction unless "special circumstances" are present.[79] *Boubelik* includes a nonexclusive list of examples of special circumstances:

> One who speaks must say enough to prevent his words from misleading the other party. One who has special knowledge of material facts to which the other party does not have access may have a duty to disclose these facts to the other party. One who stands in a confidential or fiduciary relation to the other party to a transaction must disclose material facts.[80]

U.S. Bank would seem to fall under the first two examples. Perhaps it had no duty to disclose anything about its privacy policy, but once it posted its privacy policy on the Web site, it had a duty not to mislead. In addition, the bank had "special knowledge" of its privacy policy and practices. Consumers had no access to information about that policy except for the disclosures made on the Web site. They had no information about the bank's practice of selling information to MemberWorks. The Attorney General may have run into problems, nevertheless, from court decisions stating that in a case relying on the "special knowledge" situation, there must be proof that the party with the special knowledge must know that the other party will rely on his erroneous beliefs.[81]

In addition, the Attorney General may have had a problem proving that the sale of "personal, confidential information"[82] violated the Minnesota Fraud Act. No cases decided under that statute involved sharing "personal, confidential" information. Furthermore, it is not clear how that phrase should be interpreted. "Personal" information presumably means what is typically referred to as 'personally identifiable information.' That is information which relates to an individual, not a person in a rep-

78. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

79. *See Boubelik*, 553 N.W.2d at 398.

80. *Id.*

81. *See* Rossbach v. FSB Mortgage Corp., 1998 WL 156303 (Minn. Ct. App. 1998).

82. Complaint, *supra* note 39, at ¶ 3.

resentative capacity or a person acting as part of an organizational or commercial enterprise. It is information which relates to that particular individual, not information in the aggregate such as the bank telling MemberWorks that 55% of its customers are male, 20% earn over $100,000, etc. The meaning of "confidential" information is more elusive. In this case, however, the Attorney General would have been helped enormously by the bank having defined the term in its privacy policy. "It is our policy that all personal information you supply to us will be considered confidential."[83] Therefore, for purposes of this case, personal information is confidential information if it is information the consumer supplied to the bank as contrasted with information the bank obtained from other sources. The statement in the posted privacy policy may explain why the Complaint's allegation of a deceptive and misleading act is limited to the sale of "information obtained from consumers." This raises the question of whether the Attorney General could have successfully argued that other types of information, such as information supplied by third parties, or information gathered by the bank itself could be regarded as confidential and protected even though not within the meaning of "confidential" included in the bank's privacy policy.

This inquiry also raises the issue of the degree to which a bank or other seller of goods or services can define the parameters of liability by clever wording of its privacy statement. It is reasonable to assume the average consumer, reading the bank's privacy statement, has the impression that the bank will protect her privacy, and will fail to understand that information gleaned from third parties and from the bank's own investigation is not protected.

On the other hand, at the time of the lawsuit, no law required banks or other sellers to have privacy policies, much less to post them on Web sites. U.S. Bank went out on a limb by adopting a policy and posting it for all to see. In doing so it was dutifully complying with the recommendations, but not the legal requirements, of its regulators. In the absence of specific statutes establishing requirements, the bank can argue it could not reasonably anticipate that its posted policy violated the Minnesota Fraud Act or the common law right of privacy, neither of which explicitly contemplate the situation at issue.

83. U.S. Bancorp, *U.S. Bancorp Privacy Policy* (visited March 16, 2000) <http://usbank.com/privacy.html> ("It is our policy that all personal information you supply to us will be considered confidential. This policy holds true no matter how we receive your personal information; over the phone, at our branches, through our ATMs, or online at this Web site.").

The Attorney General might have alleged a violation of the Minnesota Fraud Act even if the bank had not posted a privacy policy on the Web. The Complaint states that the bank's customer agreement does not inform consumers of the sale of confidential information,[84] and claims that the credit card agreement is deceptive and misleading because it talks about selling information in a paragraph titled "Affiliate Sharing," even though information is sold to non-affiliated parties.[85] Perhaps that would be sufficient to prove a violation of the statute even if there had been no posting on the Web.

The Complaint goes further than merely alleging that the site does not inform customers that the bank will sell confidential information to third parties.[86] In addition, in the count alleging a violation of Minnesota's Consumer Fraud statute, the Complaint notes that the site does not advise customers of whether or how they might opt-in or opt-out of the sale of information about them to third parties.[87] Furthermore, that count states that the Web site does not give the consumer an option as to how the bank "choose[s] to use" information about the consumer.[88] This raises the question whether the Attorney General was claiming that a site would violate the statute unless it not only advised customers the bank would sell information about them to third parties, but also gave them these options.

The Complaint also alleges a violation of the Minnesota Deceptive Trade Practice Act. The sections of this statute provide that a person engages in a deceptive trade practice when he represents that goods or services have characteristics, uses, or benefits that they do not have,[89] or engages in conduct which "creates a likelihood of confusion or of misunderstanding."[90] To prove a claim under those provisions, the Attorney General would have to show either that U.S. Bank had knowledge of the deceptive trade practice or that the bank had a financial interest in the goods or services deceptively offered for sale.[91] The Attorney General could prove that the bank knew of the deceptive trade practice by showing that it had entered into the alleged business arrangement whereby the bank shared information

84. *See* Complaint, *supra* note 39, at ¶ 64.
85. *See id.* at ¶ 65.
86. *See id.* at ¶ 61.
87. *See id.* at ¶ 62.
88. *See id.* at ¶ 63.
89. MINN. STAT. ANN. § 325D.44(5) (West 1995).
90. *See* § 325D.44(13).
91. *See* Aequitron Med., Inc. v. CBS, Inc., 964 F. Supp. 704 (S.D. N.Y. 1997) (citing § 325D.46(1)(a)).

about consumers with MemberWorks while posting a privacy policy claiming that information would be confidential. The Attorney General could prove that U.S. Bank had a financial interest in the services offered for sale by proving its allegations that the bank received four million dollars plus a twenty-two percent commission of the revenue from MemberWorks' sales to bank customers.

The Attorney General alleged the bank violated the Minnesota Deceptive Trade Practices Act by representing that its services had characteristics and benefits they do not have. Presumably, the Attorney General could prove this by arguing that the privacy policy represented that bank services had the characteristic and benefit of information confidentiality, while in fact their services did not have that characteristic or benefit. The success of that argument might have depended upon the court's willingness to regard the privacy policy as part of the contractual obligation of the bank. The bank likely would have argued that its contractual obligations were defined by those matters specifically contained in its written agreement with each consumer and any matters incorporated by reference in that agreement. The lack of a specific statute providing for consumer privacy creates uncertainty in regard to the legal status of the privacy policy.

The Attorney General also alleged the bank violated the Deceptive Trade Practices Act by engaging in conduct which creates the likelihood of confusion or misunderstanding.[92] Presumably the Attorney General could have proven this by showing that consumers reading the representations in the privacy policy would reasonably believe information would not be shared with third parties, and therefore had a misunderstanding of the true nature of the bank's information practices. The bank may have argued, however, that there was no nexus between the posting of the privacy policy and any particular transaction between the bank and its customers. That is, posting the privacy policy was done merely to inform customers, and was not done in connection with any transaction with the consumer; consequently, it could not create the likelihood of confusion or misunderstanding.

The Attorney General's final count under Minnesota statutes alleged a violation of the false advertising law. That statute provides that a corporation which publishes an advertisement which contains representations which are "untrue, deceptive, or misleading" is guilty of a misdemeanor and the advertisement

92. *See* § 325D.44(13).

may be enjoined.[93] In a civil action, the Attorney General would have to prove:

1. Intent to sell merchandise or services;
2. Publication;
3. A false or misleading advertisement; and, if seeking a civil recovery;
4. Damages.[94]

It is not clear that the Attorney General would have been able to convince a court that the privacy policy was an advertisement covered by this statute. As to the first requirement, the bank's posting of its privacy policy was arguably done merely to inform its customers of its policy, rather than as part of its strategy for selling products or services. In regard to the second requirement, there seems to have been publication by posting the privacy policy on the Internet. The statute, however, lists many types of media, but does not mention the Internet.[95] Furthermore, the listing is not precluded by—"including, but not limited to"—the standard language indicating a listing is not exclusive. A privacy statute drafted with Internet transactions in mind would preclude the types of legal challenges which U.S. Bank might have raised. In regard to the third requirement, it is not clear that the posted privacy policy qualifies as an advertisement. As explained above, the bank's intent may have been to inform rather than to use the privacy policy as part of its marketing strategy to sell products. In addition, in a case brought under the Minnesota Deceptive Trade Practice Act, one court noted that one of the factors in typical advertisements is that the representations are commercial speech.[96] It is not clear that the bank's privacy policy qualifies as commercial speech under Minnesota law.[97] The Attorney General's case would be buttressed,

93. MINN. STAT. ANN. § 325F.67 (West 1995).

94. *See* Lenscrafters, Inc. v. Vision World, Inc., 943 F. Supp. 1481, 1491 (D. Minn. 1996).

95. § 325F.67 provides that the publication or dissemination appears "[I]n a newspaper or other publication, or in the form of a book, notice, handbill, poster, bill, label, price tag, circular, pamphlet, program, or letter or over any radio or television station, or in anything so offered to the public . . . ."

96. *See* Medical Graphics Corp. v. SensorMedics Corp., 872 F. Supp. 643, 650 (D. Minn. 1994).

97. *See, e.g.*, State of Minn. v. Casino Mktg. Group, 491 N.W.2d 882, 886 (1992) (commercial speech is that "which 'does no more than propose a commercial transaction.'") (quoting Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976)); *cf.* Central Hudson Gas & Elec. v. Public Serv. Comm'n, 447 U.S. 557, 561 (1980) (commercial speech is "an expression related to the economic interests of the speaker and its audience.") (cited in Casino Mktg. Group, 491 N.W.2d at 886).

however, by an FDIC pronouncement that every Web home page constitutes an advertisement.[98]

The Complaint also alleges a violation of Minnesota's common law right to privacy.[99] To support that allegation, the court cites the *Wal-Mart* case.[100] In that 1998 case, the Minnesota Supreme Court for the first time recognized the tort of invasion of privacy. Although refusing to put its imprimatur on the privacy tort known as "false light," the court recognized intrusion upon seclusion, appropriation, and publication. The Complaint alleges a violation of all three of these torts.[101] Given its recent vintage, the appellate courts in Minnesota have not had the occasion to apply it to any facts.[102] It is not clear, however, that the Attorney General would have prevailed. The privacy tort of intrusion upon seclusion "occurs when one 'intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another in his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person.'"[103]

As applied to this case, one of the fundamental issues is whether the bank intruded upon the consumers' private affairs or concerns. This is not a situation where a telemarketer, unbeknownst to the consumer, secretly gathers information about the consumer and uses it to sell a product to a consumer who never even asked the telemarketer to call. Rather, U.S. Bank's customers had willingly supplied information to the bank in order to obtain its services. Nevertheless, the bank has a problem because the bank published a privacy policy which promised confidentiality. Because of that policy, the Attorney General could have argued that consumers were misled when they voluntarily supplied personal information to the bank. They did so expecting

98. *See* Walter Effross, *Logos, Links, and Lending: Towards Standardized Privacy and Use Policies for Banking Web Sites*, 24 OHIO N. U. L. REV. 747, 755 (1998).

99. Complaint, *supra* note 39, at ¶ 68.

100. Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998).

101. Complaint, *supra* note 39, at ¶¶ 69-71.

102. In *Wal-Mart*, the court reversed the lower court's dismissal of the complaint for failure to state a claim upon which relief may be granted. The court did not opine on the merits except to say that a Wal-Mart employee's distribution of a picture of two naked young women is a type of privacy "worthy of protection" because "[o]ne's naked body is a very private part of one's person and generally known to others only by choice." *Wal-Mart*, 582 N.W.2d at 235.

103. *Id.* at 233 (citing RESTATEMENT (SECOND) OF TORTS, § 652B (1977)). The complaint alleges that the sharing of consumer information was an "intentional intrusion upon the private affairs or concerns . . . [which was] highly offensive to a reasonable person." Complaint, *supra* note 39, at ¶ 69.

that the bank would adhere to its own policy and keep it confidential.

A harder case would arise if the bank did not publish a privacy policy, or published one that was ambiguous or equivocal. In those instances, the Attorney General could not argue that consumers relied on any bank promise. The question in these situations is whether the law should regard personally identifiable information collected and shared in consumer transactions as "a very private part of one's person" like the pictures of naked women in *Wal-Mart*,[104] and subject to the consumer's control even if consumers did not rely on any bank promise of confidentiality. Businesses can be expected to contend that the type of information involved in consumer transactions should be regarded as a commercial commodity, the control of which the consumer relinquishes when she voluntarily supplies it to the bank.[105] In Minnesota, the Attorney General could have found some support in case law, which holds that "a bank is generally under a duty not to disclose the financial condition of its depositors."[106] The disclosure of the personal information in the U.S. Bank case was not the same as information about the consumer's financial condition. Nevertheless, the case law supports the general notion that selling customer information to third parties may constitute intruding upon seclusion.

C. *The Settlement: Sachet or Saccharin?*

Less than one month after the Complaint was filed, the bank and the Attorney General signed a "Stipulation of Settlement" (Settlement).[107] The Settlement and accompanying proposed Final Judgment illustrate the opportunities provided by a state Attorney General, rather than an individual consumer, suing under general law such as the Minnesota Consumer Fraud Act and the common law right of privacy.[108] If instead, Minnesota had enacted a specific law aimed at consumer privacy and the Attorney General had based its claims on it, that statute would

104. *Wal-Mart*, 582 N.W.2d at 235.

105. See text *infra* accompanying note 12 (Intro discussion of Lessig).

106. Richfield Bank & Trust Co. v. Sjogren, 244 N.W.2d 648, 651 (Minn. 1976).

107. Stipulation of Settlement, State of Minnesota v. US Bank, Court File No. 99-872 (D. Minn. June 30, 1999) [hereinafter Settlement].

108. The complaint also alleged violations of specific provisions of various statutes such as the Fair Credit Reporting Act and Minnesota's deceptive trade practice act as well as a provision creating liability for false advertising. Nevertheless, as discussed below, the Settlement's remedies are not directly related to remedies in these statutes.

likely contain a specific provision on remedies which would not authorize some of the innovative types of remedies in the consent order in this case.[109] At the same time, the Settlement and Final Judgment contain serious limitations, demonstrating the restrictions which result from negotiated settlements which require each party to compromise. If the Attorney General had been able to rely on a consumer privacy statute, he might not have needed to accept some of these limitations.

One of the major weaknesses of the Settlement is the lack of any legally binding adjudication, admission, finding, or conclusion that anything the bank did violated any law. Therefore, in a strictly legal sense, the case accomplished nothing in terms of precedent.[110] While the Complaint requested the court to declare the bank's actions violated several statutes, the Settlement provides: "Nothing in this Stipulation constitutes, and nothing herein shall be construed to mean or imply, that Defendants have engaged in any wrongdoing or violations of law, or that they have made any express or implied admission of any wrongdoing or violation."[111]

Under the terms of the Settlement, the bank agreed to make refunds to all Minnesota customers who apply for a refund of any fees they paid to any "Unaffiliated Third Party" in connection with the sale of a non-financial product or service since June 1, 1997 as long as the bank shared "Customer Data"[112] with that third party and the customer did not use the program or services. On the one hand, this is a sweeping remedy. The Settlement defines "Unaffiliated Third Party" as "any person who is not an Affiliate of U.S. Bancorp." It is not known if there were other third parties besides MemberWorks, but the Settlement nevertheless is notable in ostensibly enlarging the protected class of consumers far beyond the original lawsuit.

The Settlement also resolves the problem of determining what items constitute personal information entitled to protection by listing twenty-three types of information. This raises the question of whether a statute can ever adequately fulfill this role. The

109. The statute could overcome this limitation by including a phrase such as: "The court may order such other legal and equitable remedy as is appropriate to the case and which furthers the purposes of the Act."

110. As described above, the litigation produced immediate results, including the announcement by two major financial institutions that they would no longer enter into joint marketing arrangement for non-financial products such as that between the bank and MemberWorks.

111. Settlement, supra note 107, at ¶ 5.

112. The settlement includes a definition of "Customer Data" which lists twenty-three items. *See id.* at ¶ 8.

list in the Settlement was drafted in light of the specific transactions involved and the types of information which the Attorney General, through discovery, learned were shared with MemberWorks.[113] Other types of information may be relevant to other transactions. In addition, in the future, businesses will develop new products and marketing strategies, and new forms of payment devices will be used. Therefore, a consumer privacy statute may not sufficiently describe the types of information covered. This can be partially ameliorated by including in the statute a provision such as: "The personally identifiable information protected under this Act includes, but is not limited to . . . The Attorney General shall have the authority to promulgate additional types of personally identifiable information as appropriate to effectuate the purposes of the Act and to clarify its application."

On the other hand, this part of the Settlement is quite restricted in extending relief only to Minnesota customers. US Bank is a national bank doing business in several states[114] and US Bancorp, US Bank's parent, is a multistate bank holding company.[115] Consumers in other states can obtain relief from the bank's practices only if the Attorneys General of those states or consumer class actions are successfully brought. The success of actions in those other states will depend upon the presence and strength of statutory grounds and common law rights in those states. Thus, even if the Minnesota case had not been settled and a court had adjudicated the bank in violation of Minnesota law, the bank's conduct could have been found entirely lawful if and when lawsuits are filed in other states. This situation, requiring lawsuits in every state where the bank does business, fails to ensure that consumers will be protected. In addition, banks and other e-commerce businesses are faced with a confusing variety of laws, making it difficult to plan business strategies. This concern would be solved by passing a federal statute, thus imposing uniform rules on all banks. Uniform rules ease the banks' problem of having to comply with the laws of many different jurisdictions. Consumers are highly mobile, often changing residence from state to state. Uniform rules also would reduce consumer confusion; once the consumer learns one set of rules, she can be confident they apply wherever she moves.

Other provisions of the Settlement provided for the bank to pay $500,000 to the State of Minnesota, $1,500,000 to Minnesota

113. *See* Complaint, supra note 39, at ¶ 16.
114. *See id.* at ¶ 7.
115. *See id.* at ¶ 9.

chapters of Habitat for Humanity, as well as $1,043,000 to regulated charities or public bodies in states other than Minnesota. The total amount represents the bank's total revenue, without any deduction for expenses, from sharing customer information for purposes of marketing non-financial products.[116] In addition, a provision of the Settlement is designed to prevent non-Minnesota customers from receiving more in similar litigation brought in other states. Such innovative remedies may well have been impossible if the Attorney General had been acting pursuant to a specific privacy statute.

The Final Judgment and Order for Injunctive and Consumer Relief (Judgment) provides that the bank and its affiliates shall not share customer data with unaffiliated third parties for the purpose of marketing *non-financial* products or services of unaffiliated third parties.[117] The definition of "nonfinancial products or services" is crucial. The Judgment, however, does not define this term. Rather, it defines "financial products or services."[118] Presumably, every product or service which does not come within this definition qualifies as a "nonfinancial product or service."

This is a sweeping order, affecting the bank's practices, not only in relation to the third party involved in this case, MemberWorks, but also to all other present and future third parties who market such products or services. The Judgment, however, raises but does not answer several related questions. For instance, can US Bank share information with unaffiliated third parties for purposes unrelated to marketing non-financial products or services, but related to other purposes? For example, can U.S. Bank share information with XYZ company where XYZ does not use the information for marketing such products or services, but instead sells the information to ABC, Inc., which does market these products? Another question is how the Judgment affects other Minnesota banks. Does the Judgment stand as a warning that all banks doing business in that state are in violation of Min-

116. *See* Settlement, *supra* note 107, at ¶ 14(d).

117. *See* Judgment, State of Minnesota v. US Bank, Court File No. 99-872 (D. Minn. June 30, 1999) [hereinafter Judgment]. The bank also is required to "maintain all data bases in a manner that allows their separation in the event of divestiture and the preservation of confidentiality of Customer Data in such event." *Id.* at ¶ 15.

118. *Id.* at ¶ 10. "Financial Products or Services" are defined as regulated securities or insurance products or services, making loans or extending credit and related services, leasing and trust and asset management services. The refund provision of the Settlement is included in the judgment. *Id.* at ¶ 18.

nesota laws if they share information with marketers of non-financial information?

What if another Minnesota bank provides consumers with an opt-in opportunity? That is, the bank will share information with marketers of non-financial information only if the consumer affirmatively notifies the bank that the bank has the consumer's permission to do so. Assume the bank also clearly discloses this practice in its written brochures and contracts and on its Web site. Would the Attorney General regard that as violating state law? It would be contrary to the U.S. Bank Judgment in allowing sharing with these third parties, but may not be regarded by the Attorney General as violating state law because this hypothetical bank uses a substantially different procedure than was present in the U.S. Bank case.

The Judgment includes several mandatory disclosures. The bank is required to disclose its privacy policy "conspicuously and clearly, in written communications."[119] The disclosure must be made when the customer purchases a product and annually. Disclosures must "clearly list each category of information" the bank proposes to share with affiliates for direct marketing purposes or third parties for purposes of marketing that third party's financial products or services. In addition, the bank must disclose "the specific purpose for the sharing of information." Finally, customers must be given a method for opting-out of the bank's sharing of customer data with affiliates and unaffiliated third parties when they engage in the above types of marketing activities.[120] If a customer exercises the option to opt-out, the bank must remove the customer's name from its direct marketing lists and lists it provides to third parties for purposes of marketing financial products.

Implicit in the Judgment's provision requiring disclosure of its privacy policy is the requirement that the bank have a privacy policy. Also significant is the provision applying the opt-out, not only to the bank's sharing information with third parties, but also with its affiliates. This was a matter of major contention in the battle over federal privacy legislation governing financial institutions.[121]

It is not clear whether other banks doing business in Minnesota also must follow these disclosure and opt-out requirements or risk action by the Attorney General. As discussed above,[122] the

119. *Id.* at ¶ 19.
120. *See id.*
121. *See infra* text accompanying notes 274-76
122. *See supra* text accompanying note 105.

Richfield case's[123] holding that banks are under a general duty not to disclose the financial condition of their customers establishes a legal precedent for consumer privacy. In effect, the Judgment permits banks to violate this privacy when the consumer consents under an opt-out procedure. The issue which then arises is whether opt-out makes it too easy for the bank to avoid the privacy duty, and whether opt-in should be required instead.

Another opt-out provision in the Judgment applies to customers opening a credit card or depository account.[124] Customers must be provided a notice of the opportunity to opt-out of the bank's cross-marketing activities by electing not to permit the bank to share customer data. This applies both to sharing data with affiliates for direct marketing, and to third parties for purposes of marketing financial products or services. The notice also must be provided annually.

These opt-out provisions raise the issue of what happens if the consumer chooses to opt-out. May the bank refuse to do business with that consumer? Is that a valid reason for refusing to extend credit or to refuse to open a depository account? May the bank terminate current customers if they opt-out? In the alternative, since those consumers who opt-out are less profitable to the bank, may the bank charge higher fees to those consumers or refuse to offer certain services such as free checks?

Other provisions permit modification of the terms of the Judgment under specified conditions. For example, the Office of the Comptroller of the Currency (OCC) may modify the Order "if it deems so appropriate in respect to the ability of Defendants to conduct their business relative to the use or disclosure of Customer Data in a manner comparable to that of other national banks."[125] In addition, the bank can petition the court for a modification which may be granted if it can show it is at a "competitive disadvantage to other national banks" because of the Judgment's restrictions on the use or disclosure of customer information. Furthermore, certain key provisions will not be binding on a successor organization if the bank merges and the transaction value at the time of the merger's announcement is equal to twenty-five percent of the pre-announcement market capitalization of U.S. Bancorp. Finally, the bank may seek a modification if new federal statutes or regulations applicable to

123. Richfield Bank & Trust Co. v. Sjogren, 244 N.W.2d 648, 651 (Minn. 1976).

124. *See* Judegment, *supra* note 117, at ¶ 14. An exception is made for co-branded and affinity credit card programs. The bank is allowed to share customer data in regard to these programs. *See id.* at ¶ 21.

125. *Id.* at ¶ 24(A).

national banks are enacted which the bank believes requires modification of the Judgment. Now that Congress has enacted a new federal law, U.S. Bank may take advantage of this provision to seek a substantial revision of the Judgment.

These provisions illustrate the very fluid environment in which financial institutions operate today. The Judgment takes into account the variety of authorities to which U.S. Bank is subject. Because U.S. Bank is a national bank, the Judgment had to take into account the OCC's possible future exercise of its regulatory powers. In addition to the Attorney General's continuing monitoring of the bank, the court is still a participant: the bank can petition the court for modification of the Order, and the Attorney General can go back to the court if it believes the Order is not being followed. The Judgment recognizes that the bank operates in an era of constant mergers and acquisitions, and that federal statutes and regulations affecting the Judgment may be enacted. These provisions also provide lessons for possible legislative action. State privacy legislation may have a different impact from bank to bank depending on whether an institution is a state chartered institution, a national bank, a thrift, or a credit union. Depending on what type of institution it is, the bank will be subject, not only to the state law, but also to various federal laws and regulations, some of which may preempt the state law. In addition, because of the rapidly changing nature of financial institutions and the marketplace, both common law and statutes run the risk of not being suitably adapted to new conditions.

The Judgment is deficient in not providing adequate protection in the sharing of information to those using it to market financial products. The Fair Information Practices principles adopted by the federal government and a European Union Directive include requiring companies to give individuals access to the information the company has about the individuals.[126] Furthermore, the individual has some control over the quality of the information. The principles allow the individual to correct erroneous and incomplete information. It is understandable that the Judgment does not include provisions guaranteeing consumer access and control, given the lack of statutory basis for requiring these. This illustrates, however, the inadequacy of reliance on current law to adequately protect consumer privacy.

Finally, despite the fact that the Complaint was based, in part, on the bank's failure to comply with the privacy policy it posted on the Web, the Judgment fails to take electronic com-

126. *See* SWIRE & LITAN, *supra* note 6, at 29.

merce into account. For instance, the Judgment requires the bank to disclose its privacy policy to its customers "in written communication" at various times.[127] May the bank satisfy this requirement by posting the policy on its website if in its paper communication devices, brochures and contracts, it clearly notifies consumers the policy is on the Web? Does "written communication" include text on a website? Many states recently have enacted laws providing that electronic records have the same legal validity as paper documents.[128] Should posting privacy policies on the Web be satisfactory at least for consumers who have signed home banking agreements whereby they directly express their desire to do their banking on the Web? What is the effect of posting a privacy policy on the Web? The Judgment would have been more effective if it had included a provision indicating that the bank would take steps to ensure that the policy posted on the Web accurately reflects actual bank practice and procedure. Further, the Judgment could have stated that if the bank made changes to its privacy policy, it would notify its customers in paper communications of those changes, as well as on its Web site.

Perhaps the most important lesson of the U.S. Bank case is that the lack of consumer privacy law does not provide banks and others with immunity. A determined state official, and possibly a determined consumer, may be able to fashion a viable cause of action out of current statutory and common law. Moreover, even if the plaintiff does not win by obtaining a court determination that the company violated the consumers' privacy rights, the firm may well lose the most important battle of all: it may lose the public's trust.

II. THE FEDERAL GOVERNMENT'S AMBIVALENT POSITION

The federal government has issued various reports and pronouncements about consumer privacy on the Internet for several years.[129] Although expressing concern and detailing potential privacy and security problems and the tremendous harm to consumers they could cause, until Congress enacted privacy legislation in October, 1999, government agencies contended that for the time being, the preferable approach is to trust that industry will adopt adequate self-regulation, making legislative action unnecessary. Even though Congress has passed legislation, federal agencies will play a major role issuing regulations and

127. Judgment, *supra* note 117, at ¶ 19.
128. *See, e.g.*, GA. CODE ANN. §§ 10-12-1 to 10-12-5 (1994).
129. *See* Budnitz, *supra* note 6, at 860-68.

enforcing the law.[130] In addition, that legislation is limited in scope. Therefore, agencies will have to decide what further action on their part is appropriate in regard to matters not covered by the law. As a result, it is instructive to examine their approach to consumer privacy prior to passage of the new statute.

Ira Magaziner, formerly President Clinton's adviser on Internet policy, articulated the Administration's opposition to privacy legislation, in part, by pointing out agencies' inability to police cyberspace:

> [E]ven if you passed a thousand pages of privacy protection, on the Internet, you can't enforce it. Because there is no government agency that is going to be able to monitor the 10,000 Web sites that are formatted every week. So essentially you are making a false promise [of protection] to your citizens.[131]

Magaziner assumes that if Congress were to pass privacy legislation which included authorizing a government agency to enforce the law, Americans would regard that as a guarantee that the agency would be able to ensure complete compliance with that law. Therefore, because it is impossible to ensure even close to 100% enforcement of an Internet privacy law, we should not enact any legislation.

If Magaziner's reasoning were followed, Congress should repeal all consumer and investor protection laws, because it is impossible to guarantee perfect enforcement of those laws. His conclusion that no laws should be enacted is based on the assumption that when a statute empowers a government agency to enforce a law, the public takes that as a promise by the government that the agency can protect them whenever they engage in conduct for which the statute provides protection. It is unreasonable to believe consumers have such an optimistic view of the effectiveness of government agencies in a free democratic society. Moreover, Magaziner assumes the only possible enforcement mechanism is through government agencies. A statute which includes a private right of action with statutory damages, punitive damages, attorney's fees and class actions would provide an additional source of potential enforcement.

Magaziner's reluctance to provide government agencies with an explicit statutory mandate to ensure consumer privacy is shared by the agencies themselves. In May, 1999, the Office of

130. *See infra* text accompanying note 207.

131. Ira Magaziner, *Magaziner: Momentum is Shifting, in* GOVERNMENT TECHNOLOGY, E-COMMERCE 42 (1998).

the Comptroller of the Currency (OCC) issued "guidance" to national banks in the matter of Web site privacy.[132] The guidance provides examples of practices and procedures banks have implemented. The OCC stressed the critical nature of consumer privacy in explaining why it issued the guidance. The OCC pointed out that "a fundamental component of the bank/customer relationship is a customer's trust in the institution to respect the privacy and confidentiality of that relationship."[133] Citing survey evidence, the OCC stressed that it is even more important to reassure consumers about their privacy in an online environment. The OCC not only describes consumer expectations of privacy and security, but categorizes them as "legitimate expectations."[134]

After building its argument that Internet consumer privacy is of crucial importance, the OCC then explains that national banks are not required to adopt any of the practices or procedures described in the guidance. "These examples are not examination standards, do not impose new regulatory requirements on banks, and are not intended to be an exclusive description of the various ways banks can devise and communicate effective privacy policies."[135] In other words, ensuring consumer privacy and security on the Internet is something national banks should definitely should be doing, but it's entirely up to those banks whether or not to actually do it.

The OCC then describes various ways in which banks currently communicate their privacy policies to consumers, procedures employed to develop an effective privacy policy, methods to ensure that third parties act consistently with the bank's privacy policy, and mechanisms for dealing with consumer complaints and inquiries. The memorandum fails to distinguish among practices and procedures which are sound and should be followed in all situations, and those for which banks should always have flexibility because of the different sizes and types of national banks and the various types of reasonable alternative methods of achieving the same objectives. In failing to make these distinctions, the guidance fails to provide meaningful guidance and demonstrates just how gun-shy the OCC is about consumer privacy.

---

132. Julie L. Williams, *Guidance to National Banks on Web Site Privacy Statements*, (visited May 4, 1999) <http://www.occ.treas.gov/ftp/advisory/99-6.txt>.

133. *Id.*

134. *Id.*

135. *Id.*

For example, the guidance does not require banks to have a privacy policy, nor to post a privacy policy if they have one. The OCC's reluctance to require banks to have a policy is understandable in the absence of a statutory mandate. It would not seem unduly brash, however, to suggest that the OCC could have at least strongly recommended that, if a bank has adopted a privacy policy, it should make that policy known to its customers. The guidance is somewhat confusing in encompassing general bank privacy policy although the focus is ostensibly on bank Internet sites.[136] The confusion arises, for example, in its discussion of how banks that choose to communicate their privacy policy go about doing so. The OCC notes that some banks post their privacy policy only on their Web sites, whereas others provide paper copies of the policy. The OCC should have opined that a bank should always have a paper copy of their privacy policy for those consumers who do not have accounts that can be accessed through the Web, or who have accounts that can be accessed either at a physical site or on the Web, but who choose not to use the Web option.

The memorandum also describes various ways of satisfying the OCC's recommendation that privacy policy be made in disclosures that are "clear, prominent, and easy to understand."[137] Illustrations include placing links on the bank home page and putting the policy on transaction pages where they are automatically displayed once the consumer chooses what type of transaction he or she wants to engage in. It is appropriate for the OCC to provide examples rather than lay down rigid rules: banks need flexibility in deciding how to disclose their privacy policy. However, it is essential that a bank's actual practices be consistent with the official privacy policy it has disclosed. Rather than coming right out and stating this as a given, the OCC states the following: "Banks with effective privacy policies also take steps to ensure that their internal policies and procedures are consistent with and support stated privacy promises."[138]

Another example of the OCC's disconcerting failure to state what should be regarded as a necessary bank practice relates to a bank's relationship with third parties. Some banks have a privacy policy which promises that any information shared with unaffiliated third parties is subject to the same confidentiality protec-

136. *See id.* ("Although this guidance is targeted at banks that operate Web sites, the examples of practices and procedures for developing and implementing privacy policies are pertinent to any national bank considering establishing or revising a privacy policy and related procedures.").

137. *Id.*

138. *Id.*

tions as when the information is in the possession of the bank. It should follow that banks with such a privacy policy should take steps to ensure that those third parties are complying with the representations made in the bank's policy. The OCC, however, refuses to state the obvious, instead merely noting that several banks require third parties to enter into confidentiality agreements and agree to limit use of information they receive from the bank, and that some banks monitor the third parties for compliance with these agreements or provide consumers with the opportunity to opt-out of information sharing. While it is understandable that the OCC would hesitate to mandate specific procedures, by not even recommending that banks implement any procedures to assure themselves that third parties are adhering to the bank's policy, the OCC leaves the impression that banks can merely post a policy promising the confidentiality of information shared with third parties, and then do nothing to monitor compliance. The problem with such a practice is that consumers reading the policy statement will reasonably assume that the bank is doing something to make sure its promises in regard to confidentiality of information are monitored and enforced.

The OCC's guidance instead merely describes two alternative bank practices: one is for the bank to monitor compliance, and the other is to provide consumers with the opportunity to opt-out. Presumably, the OCC is suggesting banks have these two options: either monitor third party compliance, or allow consumers to opt-out. For the consumer opt-out to be a meaningful choice, the bank should be required to disclose the following to consumers: "Although the bank promises in its privacy policy that information shared with unaffiliated third parties is subject to the same confidentiality guarantee as that information when in the possession of the bank, the bank does not monitor compliance by those third parties. Because the bank does not monitor compliance, you have the opportunity to opt-out and thereby prevent the bank from sharing information about you."

Noticeably absent from the OCC's discussion is any hint that banks that share information with third parties and do nothing to ensure the confidentiality of that information when in the hands of third parties should disclose that crucial fact to consumers. Also absent is any recommendation that banks make certain their employees understand the bank's privacy policy, or that banks institute procedures to deter employees from violating the policy. The OCC does not recommend banks construct firewalls so only employees with a need to know have access to the information. Finally, the OCC fails to recommend that banks estab-

lish mechanisms for dealing with consumer complaints or questions about privacy. Instead, the OCC merely describes practices and procedures which some banks have adopted in regard to these items.

This examination of the OCC's 1999 guidance suggests several ways in which financial institutions can protect consumer privacy. As regulatory agencies, including the OCC, draft regulations pursuant to the privacy provisions of the recently enacted Financial Institution Modernization Act, they may find these suggestions helpful.

In July, 1999, the Federal Trade Commission (FTC) issued a report entitled *Self-Regulation and Privacy Online: A Report to Congress.*[139] That Report nicely illustrates three distinct views of whether there is a need for privacy legislation for consumers in electronic commerce. The Report also demonstrates the markedly different perceptions of reality which well-informed persons occupying major policy-making, regulatory and enforcement roles can have when evaluating identical data. The FTC voted 3-1 to issue the Report. Commissioner Sheila Anthony concurred in part and dissented in part. Commissioner Orson Swindle issued a concurring statement.

The Report noted that the need to protect privacy was recognized and practices and procedures to accomplish that were developed over twenty-five years ago, in 1973.[140] That was the year when the Department of Health, Education, and Welfare developed fair information practice principles which have since been adopted by government agencies in the United States, Canada, and Europe.[141] The Report was the latest of many FTC privacy projects; the FTC has been "deeply involved in addressing online privacy issues"[142] since 1995.[143] The Report found that while "[i]n some areas there has been much progress,"[144] the vast majority of commercial Web sites have not implemented all four of the fair information practice principles applicable to private companies.[145] The Report examined "seal" programs in which

139. FEDERAL TRADE COMM'N, SELF REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS (1999) [hereinafter REPORT TO CONGRESS].

140. *See id.* at 3.

141. *See id.* The five principles are: "(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress." *Id.*

142. *Id.*

143. *See id.* at n.16.

144. *Id.* at 6.

145. *See id.* The FTC did not apply the principle of "Security/Integrity" to private industry. The FTC commended IBM, Microsoft, and Disney for their

independent organizations, including the Better Business Bureau, issue privacy standards, and permit companies which follow those standards to display the organization's seal of approval on their Web site.[146] The FTC viewed seal programs as a positive development, for they allow consumers to identify companies which have agreed to follow specific standards established by a third party.[147] The FTC found, however, that "[o]nly a small minority of commercial Web sites" had become members of seal programs.[148] Despite finding industry failure to adhere to basic privacy principles or to participate in seal programs, the FTC concluded: "Based on these facts, the Commission believes that legislation to address online privacy is not appropriate at this time."[149]

Commissioner Swindle voted to submit the FTC Report "reluctantly" because he felt it did not reflect reality.[150] He believed industry had made "substantial progress," and "significant progress," considering the FTC had "articulated the elements of these four practices in detail just one year ago."[151] He faulted the Report for not giving sufficient prominence to a 1999 Georgetown University study. That study found that a majority of frequently visited sites implemented one of the fair information principles, "Notice/Awareness," by informing consumers of "at least some of their information practices."[152] Swindle also faulted the Report for not emphasizing its conclusion that no legislation was necessary. Instead, the Report mentions its conclusion at the end of the Report "as if the recommendation is some trivial afterthought."[153]

Commissioner Sheila F. Anthony concurred in part and dissented in part. While Swindle cited the Georgetown study as evidence of the substantial progress industry had made, Anthony was "dismayed" by both that study and a study commissioned by the Online Privacy Alliance (OPA study).[154] Anthony interpreted these studies as showing that there is "an enormous gap between" the collection of data online and the protection of that

policy of refusing to advertise on Web sites that do not follow fair information practices. *See id.* at 12-13.

146. *See id.* at 9-12.

147. *See id.* at 9.

148. *Id.* at 12.

149. *Id.*

150. *Id.* (Separate Statement of Commissioner Orson Swindle).

151. *Id.*

152. *Id.* at 8.

153. *Id.*

154. *Id.* (Statement of Commissioner Sheila F. Anthony Concurring in Part and Dissenting in Part).

data through implementation of the four principles. Only ten to twenty percent of the sites in the survey followed all four of the principles. Anthony, in sharp contrast to Swindle, found industry progress "far too slow" considering the FTC had been urging compliance with fair information practices since 1996. She concluded that "the time may be right for federal legislation to establish at least baseline minimum standards."[155] While Swindle feared the "likely adverse unintended consequences" of legislation,[156] Anthony believed legislation was necessary because the lack of a federal statute "will undermine consumer confidence and hinder the advancement of electronic commerce and trade."[157]

It is understandable that the Report seemed to have buried its conclusion that no legislation was necessary, given that its findings of fact would seem to point to the opposite conclusion. In addition, the Report's superficial examination of seal programs and its complete failure to acknowledge the inherent limitations of self-regulation[158] reflect either the refusal to come to grips with crucial issues, or the recognition that the only way to obtain the votes necessary for the FTC to approve a report required by Congress was to pretend these issues do not exist.

The Report found the emergence of seal programs "[a]n encouraging development,"[159] and it described the ways in which they establish standards, require licensees to comply with the standards, and employ various methods to monitor compliance. The Report avoids closely scrutinizing the programs, however, ignoring obvious systemic deficiencies which have significant implications for whether they can play a meaningful role in obviating the need for any privacy legislation. For example, the Report does not analyze in detail the agreements which licensees are required to sign. In describing a program operated by TrustE, the Report notes that licensees must "follow the standards for notice, choice, access and security" developed by the Online Privacy Alliance (OPA).[160] The OPA is described by the FTC as "a coalition of industry groups,"[161] raising the issue of whether it is the appropriate organization to determine privacy standards for the industry rather than a coalition consisting of

155. *Id.*
156. *Id.*
157. *Id.*
158. *See* Budnitz, *supra* note 6, at 874-77.
159. REPORT TO CONGRESS, *supra* note 139, at 9.
160. *Id.* at 10.
161. *Id.* at 8.

industry, privacy advocates and government representatives.[162] More importantly, the Report does not compare the details of the OPA standards with the accepted fair information practices standards developed by HEW or those established by the Organization for Economic Development and Cooperation (OECD) in Europe.[163]

The Report also describes other seal programs, such as that operated by the Better Business Bureau.[164] As with its treatment of TrustE, the Report is entirely superficial, and does not examine the merits of any of these programs. At the least, it would have been helpful for the FTC to compare the distinguishing features of each program to one another. The Report also could have compared who is eligible for membership in each program to determine if there are certain types of businesses who could not qualify even if they were willing to comply with the standards. For example, the membership fees may be too high for mom and pop businesses to be able to afford. Analysis and comparison also is needed of the membership agreements' definitions of what data is covered, whether sharing of information with affiliates is proscribed in any way, and how the term "affiliates" is defined. Are the licensing standards set in stone for all time, or may they be changed? If they are changed, will consumers be alerted? And if they do change, what the seal meant yesterday may be different from what it means today and will mean tomorrow. For example, TrustE has changed its agreement and some licensees are subject only to the prior agreement.[165]

The importance of the details of the agreement became evident when Microsoft launched Windows 98. During the online registration process, Microsoft collected from the consumers' computers "global unique identifiers."[166] This was done without informing consumers,[167] even where consumers had specifically informed Microsoft they did not want to have this type of proce-

162. The OPA Web site lists the businesses and associations which belong to the OPA. The author was not able to identify any privacy advocacy organizations among its members. *See* Privacy Alliance, (visited Jan. 31, 2000) <http://www.privacyalliance.org/who>.

163. *See* SWIRE & LITAN, *supra* note 6, at 23-25.

164. *See* REPORT TO CONGRESS, *supra* note 139, at 10. *See also* BBBOnline, *A Better Business Bureau Program* (visited Jan. 31, 2000) <http://www.bbbonline.com>.

165. *See* REPORT TO CONGRESS, *supra* note 139, at 19 n.47.

166. Rachel Chalmers, *TrustE Lets Microsoft Off on a Technicality*, COMPUTERGRAM INT'L, Mar. 24, 1999, *available in* 1999 WL 8110353.

167. *See* Lisa Guernsey, *Can They Cut It? Privacy Seals Don't Mean It's a Lock That a Web Site Will Keep Your Information Confidential*, CHICAGO TRIB., June 11, 1999, *available in* 1999 WL 2882191.

dure performed.[168] TrustE publicly acknowledged that Microsoft had "compromise[d] consumer trust and privacy,"[169] but refused to invoke its authority under its seal agreement with Microsoft to conduct an independent audit or to revoke its seal.[170] TrustE explained that its agreement covers only the Microsoft.com Web site. Because the unique identifiers were not collected pursuant to interaction with that site, the agreement was not violated and there was no basis on which to revoke the seal. One may question whether consumers will understand the limited scope of the seal's protection, even if they read the company's privacy policy and explanation of the seal program.

The Microsoft incident caused many to question the relationship between the members who had qualified for the seal and the company which approved their membership and decides whether they have complied with the terms for continued display of the seal. Microsoft and nine other companies, in addition to membership fees, are also sponsors of TrustE, contributing $100,000 each year.[171] Microsoft has joined the Better Business Bureau board of directors,[172] and several companies who are sponsors of TrustE have offered to sponsor BBBOnLine as well.[173] This has led to the charge that there is a conflict of interest between the "independent" organizations awarding the seals and the companies applying for the seals.[174]

TrustE and other programs do not want to "dictate specific practices" to companies who join the program.[175] This is reasonable, since TrustE wants to have one-size-fits-all rules and standards, rather than different requirements depending upon whether the site offers financial services, an auction format, or sells prescription drugs. That means, however, that hundreds of companies display the same seal, but have very different privacy policies.[176] In addition, contrary to reasonable consumer expectations, the mere presence of the seal in no way guarantees that

168. *See* Chalmers, *supra* note 166.

169. *Id.*

170. *See* Jeri Clausing, *On-line Privacy Group Decides Not to Pursue Microsoft Case*, N.Y. TIMES, Mar. 23, 1999, *available in* 1999 WL 9876310.

171. *See* Helen Dancer, *Can we trust in TrustE?*, ABIX, May 11, 1999, *available in* 1999 WL 2293496. Other sponsors include America Online and Netscape. *See also* Guernsey, *supra* note 167.

172. *See Microsoft Joins BBBOnLine Board of Directors*, M2 PRESSWIRE, Dec. 9, 1998, *available in* 1999 WL 16539604.

173. *See* Guernsey, *supra* note 167.

174. *See id. See also* Dancer, *supra* note 171.

175. Guernsey, *supra* note 167.

176. *See id.*

the site operator will not sell the consumer's personal information.[177]

In addition, there are certain systemic deficiencies in any self-regulation seal program. Memberships are voluntary. Companies which do not follow fair information practices are the least likely to join a program.[178] Programs have a variety of mechanisms to monitor compliance with the membership agreement.[179] But a company which desires a seal and is unwilling to undergo stringent monitoring, can simply join a program with less rigorous requirements. If the free market works, enterprising firms will offer such programs if there is sufficient demand. It then becomes a matter of consumers, not only remembering to examine each Web site to see if it contains a privacy seal, but also learning to distinguish weak seal programs from strong ones. Rather than even alluding to any of the above, the FTC Report merely acknowledges that "[i]t may be appropriate, at some point in the future, for the FTC to examine the online privacy seal programs and report to Congress on whether these programs provide effective protections for consumers."[180]

While seal programs have much merit and should be one part of industry self-regulation, it is questionable that they should be regarded as a justification for not enacting privacy legislation. As noted above there can be wide variations in the extent to which such a program actually protects consumer privacy. No matter how good some seal programs are, it will take years before consumers are sufficiently knowledgeable about seal programs and the differences among them, to be able to intelligently decide which sites to avoid based on which seals they display. Finally, given the tens of thousands of Web shopping sites, and the marginal status and questionable longevity of many mom and pop Web enterprises, it may unrealistic to assume that even the majority of Web businesses will join seal programs.

In addition to its superficial treatment of seal programs, the FTC Report fails to confront the essential systemic deficiencies of all types of self-regulation. Chief among these is the absence of the fifth HEW principle "Enforcement/Redress."[181] As discussed

177. *See id.*

178. *See* Budnitz, *supra* note 6, at 875.

179. TrustE periodically reviews licensees' compliance with their agreement, uses a technique known as "seeding" to test whether consumers' opt-out decisions are honored, requires members to provide consumers with a way to express concerns and ask questions, and employs third party auditors. *See* REPORT TO CONGRESS, *supra* note 139, at 10.

180. *Id.* at 13.

181. *Id.* at 3.

above,[182] even a state Attorney General might have trouble proving a case of privacy invasion absent legislation specifically tailored to deal with that conduct. A consumer would face major hurdles arguing that the consumer has a cause of action against a company violating standards set by voluntary self-regulation.

III. FEDERAL LEGISLATION

A. *General Considerations*

While federal agencies and others continued to debate whether privacy legislation is necessary to protect consumers and to provide them with a level of comfort which will ensure necessary e-commerce volume, in 1999, Congress considered a number of consumer privacy bills. In the closing days of the first session of the 106th Congress, it enacted the Gramm-Leach-Bliley Financial Services Modernization Act (Modernization Act) which contains significant provisions on consumer privacy.[183] The Modernization Act, the bills which were not enacted, and the preceding examination of the Minnesota case and federal agency response illustrate that, even if there is consensus that federal legislation is needed, the task of drafting satisfactory legislation is a difficult one for two reasons. First, there are a great many facets to consumer privacy, and hard decisions must be made as to which facets require legislation. Second, within each facet, it is hard to know how to attain a satisfactory balance between the consumer's reasonable expectation of privacy and the industry's need to collect, analyze, use and share information about consumers.

The following list of issues is suggested by a consideration of the Minnesota case, the legislative bills, the Modernization Act, as well as two European documents. One is the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organization of Economic Cooperation and Development (Guidelines).[184] The other is the European Union Directive on Data Protection (Directive).[185] As will be apparent from the discussion below, the Modernization Act deals with few of the issues

182. *See supra* text accompanying notes 59-127.

183. Gramm-Leach-Bliley Financial Modernization Act, P.L. 106-102, 113 Stat. 1338 (1999). Unless otherwise indicated, references to the Modernization Act are to Title V, Subtitle A (Disclosure of Nonpublic Personal Information).

184. Organisation for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (visited Jan. 31, 2000) <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> [hereinafter Guidelines].

185. *See* SWIRE & LITAN, *supra* note 6, at 213 (reproducing European Union Directive on Data Protection) [hereinafter Directive].

on the following list. While all of the issues on the list are important, the mandates of the Directive are particularly crucial because, unless the United States enacts privacy protections comparable to those of the Directive or otherwise reaches an accommodation with the European Union, companies in Europe will not be permitted to share information with companies in the United States.[186]

Among the issues which are relevant to consumer privacy and therefore which Congress should consider are the following:

> 1) Should all companies be required to follow certain privacy practices or should the law be restricted to certain industries such as financial institutions and the direct marketing industry?
>
> 2) Consumer privacy likely attracted Congress' attention largely because of the perceived heightened risks of consumers engaging in e-commerce. Should new privacy laws be restricted to those companies doing business with consumers in e-commerce or should it apply to all consumer transactions?[187]
>
> 3) If companies are required to follow certain practices, should those companies also be required to adopt a formal privacy policy to implement the law's required practices?
>
> 4) If companies are required to follow required privacy practices and adopt a privacy policy, should they be required to publicize that policy by informing their customers of the policy?[188] Should e-commerce companies be required to post the policy on their Web sites?
>
> 5) Should legislation provide that failure by a business to follow its privacy policy renders the company liable to government enforcement agencies and consumers?

---

186. *See id.* at vii.

187. The Guidelines and the Directive cover both non-electronic and electronic commerce. *See* Guidelines, *supra* note 184; *supra* note 185, at art. 3. They apply both to automated and nonautomated processing of consumer data. The Guidelines justify the decision to include both types of commerce by explaining that it is sometimes difficult to distinguish between the two; some companies use mixed systems, and some companies might evade being subject to the Guidelines' requirements by using nonautomated systems to process the information they wanted to keep from the consumer. *See, e.g.*, Citibank Corp., *Your Privacy* (visited Jan. 29, 2000) <http://www.citibank.com/privacy/privacy.htm> (containing general privacy policy and additional policy applicable to Internet transactions).

188. The Directive requires disclosures to the "data subject" both when the company collects information from the subject and when it obtains information from another source. *See* Directive, *supra* note 185, at arts. 10-11.

6) What types of information about consumers should the law require a company to keep private?[189]

7) Should the law require disclosure of a company's information collection, use, and sharing? If the law does require those disclosures, how detailed should the law be in regard to those disclosures? Data collected for e-commerce transactions may be far more extensive than for traditional purchases. For example, should the law require a company to disclose whether the company uses cookies or comparable devices?[190] Should the statute require the company to specifically list all the types of personally identifiable information it collects? Must the company detail what types of transactional data it collects? Should disclosure requirements vary depending upon whether or not the information was collected from the consumer?[191]

8) Should the law require companies to provide consumers with access to the information it has obtained about the consumer?[192]

9) Should the law permit the consumer to correct erroneous information and submit additional information to make the company's data base more complete?[193]

10) Should the law require disclosure of whether or not the company uses systems to ensure the security of trans-

189. The Guidelines subject "personal data" to its requirements. That term is defined as "any information relating to an identified or identifiable individual (data subject)." Guidelines, *supra* note 184. The Directive applies to "personal data," which is defined as "any information relating to an identified or identifiable natural person . . .; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Directive, *supra* note 185, at art. 2(a).

190. Many sites voluntarily make this disclosure. *See, e.g.*, Amazon.com, *Your Privacy* (visited Jan. 21, 2000) <http://www.amazon.com/exec/obidos/subst/misc/policy/privacy.html>; *American Express Customer Internet Privacy Statement About Cookies* (visited Jan. 31, 2000) <http://home3.americanexpress.com/corp/consumerinfo/privacy/about_cookies.asp>.

191. The Directive makes this distinction. *See* Directive, *supra* note 185, at arts. 10-11.

192. The Guidelines provide consumers with access as part of its "Individual participation Principle." Guidelines, *supra* note 184. *See also* Directive, *supra* note 185, at art. 12.

193. The Guidelines provide consumers with the right to challenge data and have it "erased, rectified, completed or amended." Guidelines, *supra* note 184. The Directive also provides the consumer with the right to correct data. *See* Directive, *supra* note 185, at art. 12(b).

mission of data online and to authenticate transactions, systems such as SSL and SET?[194]

11) Should the law require that companies implement systems which assure adequate internal protection of consumer information?[195]

12) Should a company be required to disclose, not only that it shares information with affiliates and third parties, but also list the types of business those affiliates and third parties engage in?

13) Should the law require giving the consumer a choice to opt-out of the company's information-sharing practice?[196] Should the law require opt-in, where the company could share its information with others only if the consumer gave the company specific individualized permission to do so after being fully informed of who would receive the information, and for what purpose?

14) Should the law only restrict privacy practices where the company shares information with third parties, and not restrict sharing with affiliates?

15) If the law applies only to financial institutions, should it restrict all information it shares with third parties? In the alternative, should the law, like the Settlement in the Minnesota case, govern only information sharing with third parties when they market non-financial services to consumers? The rationale apparently is that information obtained from or about consumers by the bank should be shared only when used by third parties to market services compa-

194. Secure Socket Layer (SSL) technology ensures that only the merchant with whom the customer is communicating over the Web has access to the information being sent. *See* Marc Holt, *How to Ensure Your Credit Card is Secure in Cyberspace: Commonsense Goes a Long Way*, BANGKOK POST, Jan. 26, 2000, at 4, *available in* 2000 WL 4680757; Stuart McClure & Joel Scambray, *Security Watch: Hacking Frenzy Shows Network Security Breaches are not About to go out of Fashion*, INFOWORLD, Jan. 24, 2000, at 64, *available in* 2000 WL 8732439. Secure Electronic Transactions (SET) is a technology developed by credit card companies which provides protection for transmission of credit card information. *See* LESSIG, *supra* note 8, at 40. The Guidelines provide that "[p]ersonal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data." Guidelines, *supra* note 184. The Directive contains detailed requirements in regard to the security of systems. *See* Directive, *supra* note 185, at art. 17. *See also* American Express, *Security Q & A* (visited Jan. 31, 2000) <http://home4.americanexpress.com/cust_serv//docs/cs-security.shtml>.

195. The Guidelines contain such a provision. *See* Guidelines, *supra* note 184. The Directive also contains detailed requirements in this regard. *See* Directive, *supra* note 185, at art. 17.

196. *See* Directive, *supra* note 185, at art. 17.

rable to those the bank offered (financial services) when it obtained the information from and about the consumer. The assumption is the consumer's expectation of privacy is only that the information will not be used for selling nonfinancial purposes, but may be used, even by others, for selling financial services. Is that assumption about consumer expectations reasonable?

16) Should the law establish a privacy agency to promulgate regulations pursuant to whatever statute is enacted?[197] Should an existing agency (i.e., the FTC, the FRB, or Commerce Department) be delegated that task?

17) Should consumers be given the right to sue for violations of the law, or should enforcement be left entirely to a government agency?[198] Instead of a government agency, should all enforcement be left to consumer lawsuits?

B. *The Financial Services Modernization Act*

As a result of the growing public interest in consumer privacy, the Republican-controlled first session of the 106th Congress experienced a flood of privacy bills.[199] The privacy provision which ultimately became law was contained in a most unlikely piece of legislation. The Modernization Act[200] restructures the entire financial services industry, permitting banks to engage in types of businesses previously forbidden by merging with insurance companies and brokerage firms.[201] Congress has considered this restructuring for many years, and in the past consumer privacy was never anywhere on the radar screen. In 1999, however, the House Commerce Committee approved a version of the bill which ultimately became the basis of the bill which became law. That bill contained a remarkably strong privacy sec-

197. *See id.* at art. 28 (requiring each Member State to delegate to one or more public authorities the responsibility for monitoring the application of the Directive, conducting investigations, intervening, and bringing legal proceedings).

198. Item #5 is far more limited than this item. Item #5 addresses only the failure of a company to follow its privacy policy. This item would provide a remedy for any violation of a consumer privacy statute and regulations, which might include required notices, opt-out disclosures, security procedures, etc. The Directive provides for enforcement actions by both individuals and government agencies. *See* Directive, *supra* note 185, at arts. 22 & 28(3).

199. *See infra* text accompanying notes 314-47.

200. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (to be codified at 15 U.S.C. § 6801).

201. *See At a Glance: Gramm-Leach-Bliley Act of 1999*, AM. BANKER, Nov. 12, 1999, at 4.

tion.[202] The bill ultimately enacted is considerably weaker, but given industry opposition, the fact it contained any privacy provision at all is notable. The enactment of the privacy provisions demonstrates the extent to which the seriousness of consumer privacy concerns have been successfully communicated to Congress.

The description, analysis, and evaluation which follows raise many issues. Some are fundamental, while others are technical in nature. Many questions which arise because of holes and ambiguities in the statute will be answered in forthcoming regulations.[203] But many questions undoubtedly will remain. Moreover, the discussion which follows should provide a basis for judging the regulations.

The Modernization Act begins by making a bold and sweeping policy statement. The Modernization Act states that it is Congress' policy that financial institutions have "an affirmative and continuing obligation to respect the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information."[204] This policy statement may guide agencies drafting regulations when deciding how broadly to define terms[205] and how extensively to expand exemptions.[206] It may influence courts interpreting the many vague terms and provisions of the Modernization Act.[207]

This policy is then effectuated in three principal ways. First, each of the agencies or authorities with enforcement powers under the Modernization Act is required to establish appropriate standards relating to administrative, technical, and physical safeguards:

> (1) to insure the security and confidentiality of customer records and information;

---

202. *See* Dean Anason, *Privacy Issue Might Push Reform Bill Vote Past July 4*, AM. BANKER, June 24, 1999, at 2.

203. *See* Gramm-Leach-Bliley Financial Modernization Act § 504.

204. *Id.* § 501(a). The Act becomes effective six months after regulations are issued. *See id.* § 510. Regulations are to be promulgated six months after the date of enactment. *See id.* § 504(3). Because the date of enactment was Nov. 12, 1999, regulations must be issued by May 12, 1999, and the Act becomes effective Nov. 12, 2000. The regulations, however, can specify that the Act will become effective at a later date. *See id.* § 510.

205. For example, section 509(4)(B) requires the crucial term "publicly available information" to be defined by regulation.

206. *See* Gramm-Leach-Bliley Financial Modernization Act § 504(b).

207. *See, e.g., id.* § 509(4)(A)(iii) (providing that nonpublic personal information includes "financial" information "otherwise obtained"). The Act does not define either of the quoted terms.

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[208]

The second way in which congressional policy is effectuated is by requiring the institution to disclose its privacy policy to "consumers" with whom it has established a "customer relationship" (the privacy policy disclosure).[209] Third, the institution must notify the consumer before sharing nonpublic personal information about the consumer to nonaffiliated third parties, and must provide consumers the opportunity to opt-out of such information sharing (opt-out notice).[210] Institutions also are prohibited from disclosing account numbers, access numbers and access codes under many circumstances.[211] Various federal agencies are authorized to issue regulations applicable to the institutions subject to their jurisdiction.[212] Those agencies are empowered to enforce the Act and regulations issued pursuant to it.[213] There is no provision authorizing a private right of action which would enable a consumer to sue for violation of the Act.[214] Finally, the Treasury Department is required to conduct a study of information sharing among financial institutions' affiliates;[215] those affiliates are exempted from the Act's notice and opt-out requirements.[216] There also are numerous other excep-

208. *Id.* § 501(b).

209. *Id.* § 503.

210. *See id.* § 502.

211. *See id.* § 502(d). Other than disclosing these codes and numbers to consumer reporting agencies, institutions may not disclose this information "to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer." *Id.*

212. *See id.* § 504. *See also* Privacy of Consumer Financial Information, 65 Fed. Reg. 8770 (2000) (to be codified at 12 C.F.R. pts. 40, 216, 332, 573 (proposed Feb. 22, 2000)) (regulations proposed by the Office of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision) [hereinafter Proposed Regulations].

213. *See* Gramm-Leach-Riley Financial Modernization Act § 505.

214. However, state attorneys general and consumers may be able to sue pursuant to state unfair and deceptive trade practice statutes and the common law. *See* David W. Roderer, *Privacy Provisions of New Financial Services Law Likely to Ensnare the Unwary*, 73 BANKING REP. (BNA) 854, 855 (1999).

215. *See* Gramm-Leach-Bliley Financial Modernization Act § 508.

216. The opt-out notice provisions of section 502 only apply to nonaffiliated third parties, a term which does not include a financial institution's affiliates. *Id.* § 509(5).

tions and exemptions.[217]

While industry hailed the Modernization Act for providing important and far-reaching protection for consumers,[218] others, including President Clinton, decried what they claimed were substantial weaknesses in those provisions.[219] The criticism was not confined to the "usual suspects," the privacy advocates who would be expected to criticize any law which failed to provide very expansive consumer privacy protection.[220] Others also questioned the effectiveness of the law.[221] For example, columnist Jane Bryant Quinn condemned the law in the strongest terms. "*Privacy.* Consumers lost it all . . . You've been sold out."[222] A detailed analysis of the Modernization Act reveals that while consumers did not lose everything, they did not receive anywhere near the safeguards which they need to be adequately protected.

Crucial to understanding the scope of the provisions of the Modernization Act is the statute's definitions of key terms. The Modernization Act makes a major distinction between nonaffiliated third parties and affiliates, exempting affiliates from its restrictions on information sharing. The terms "affiliate" and "nonaffiliated third-party" are defined in the Modernizaion Act, largely based on whether one company controls another.[223]

---

217. *See, e.g., id.* at § 502(e).

218. The Consumer Bankers Association "hailed" the Act and proclaimed it to be pro-consumer. *See Financial Modernization Crosses the Finish Line*, CBA REP., Nov. 1, 1999, at 1, *available in* 1999 WL 20345608.

219. *See* Roderer, *supra* note 214, at 854 (President Clinton stated: "I do not believe that the privacy provisions go far enough.").

220. *See* Ed Mierzwinski, *New Bank Laws May Increase Threats to Consumers' Privacy*, 15 U.S. PIRG 4, Fall 1999 (stating that the Act "may have made things worse," and deeming the opt-out provision "meaningless").

221. *See, e.g.*, William Safire, *Privacy Fire Walls About to Tumble*, ATLANTA J.CONST., Nov. 2, 1999, at A13 (criticizing law for failure to provide protection from affiliate information sharing); Schroeder, *supra* note 38, at A50 ("A diverse group of critics including consumer activist Ralph Nader, conservative Phyllis Schlafly, AARP, and a number of conservative Republicans and liberal Democrats in the House and Senate" opposed the bill's exclusion of affiliates from the privacy protection afforded against nonaffiliated third parties. Nonetheless, the exclusion was retained in the law as enacted).

222. Jane Bryant Quinn, *The Megabucks Marts Arrive*, NEWSWEEK, Nov. 8, 1999, at 52; *see also* Roderer, *supra* note 214.

223. A nonaffiliated third party means an entity that is not an affiliate of the financial institution, and an entity that is not "related by common ownership or affiliated by corporate control with . . . the financial institution." Gramm-Leach-Bliley Financial Modernization Act § 509(5). An "affiliate" is "any company that controls, is controlled by, or is under common control with another company." *Id.* § 509(6). This definition is similar to that used in the Fair Credit Reporting Act. *See* 15 U.S.C. § 1681a(d)(2)(A)(iii) (1999) ("related by common ownership or affiliated by corporate control").

The Modernization Act differentiates between the "consumer" and the consumer with whom the institution "establish[es] a customer relationship."[224] The provisions requiring the opt-out notice apply to the consumer. "Consumer" is defined in the same manner as it is defined in other federal consumer protection statutes.[225] The section requiring the privacy policy disclosure applies to the consumer with a customer relationship. The Modernization Act does not define "customer" or a "customer relationship."[226] Perhaps what Congress intended was to distinguish persons who obtain products or services only one time or occasionally, from persons who have an ongoing relationship. Examples of the former might be a person who occasionally uses an ATM owned and operated by a bank with whom the person has no account. Or a person who occasionally cashes a check at a bank with whom the person does not have an account. Examples of the latter would be a person who has a savings or checking account at a bank, obtained a loan from the bank, or uses a credit card issued by the bank. This interpretation is implied from the use of the word "relationship." In addition, the privacy policy disclosure must be made to the consumer annually. It would impose an unfair burden on the institution to have to make this disclosure to one-shot users or persons occasionally using its services or products. It would be very expensive and require the institution to get the address of every consumer who uses any product or service. On the other hand, the institution has the address of persons who have accounts with it. Finally, this interpretation is supported by the Modernizations Act's requiring the privacy policy disclosure to include policies and practices in regard to "persons who have ceased to be customers of the financial institution."[227] This implies that a customer with a relationship includes a temporal component, a consumer who has had an ongoing, continuing relationship.

---

224. Gramm-Leach-Bliley Financial Modernization Act § 502(a).

225. "The term 'consumer' means an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." *Id.* § 509(9).

226. Another portion of the Act, dealing with fraudulent access to financial information, defines "customer" as "any person (or authorized representative of a person) to whom the financial institution provides a product or service, including that of acting as a fiduciary." *Id.* § 527(1). This definition does nothing to further an understanding of the difference in the privacy section of the Modernization Act between a consumer and a consumer who is also a customer.

227. *Id.* § 503(a)(2).

The Modernization Act restricts an institution's sharing of "nonpublic personal information," which means "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[228] The term therefore includes what is referred to as "data privacy" as well as "transaction privacy."[229] Use of the phrase "otherwise obtained" seems to cast a wide net, meant to include all information which comes within the definition of nonpublic personal information. Examples which might come within this category are information obtained from credit reporting agencies and from companies which gather data about the consumers who view the advertisements which financial institutions have on their Web sites.[230] The only information which is protected, however, is "financial information."[231] Although the term is not defined in the Modernization Act, it would not include "nonfinancial demographic data or depersonalized information used by a bank or business for analytical purposes."[232] "Nonpublic personal information" must be distinguished from "publicly available information." The Modernization Act does not restrict an institution's sharing of publicly available information. Obviously, the definition of publicly available information therefore is very important. Unfortunately, the term "publicly available information" is not defined; instead, it is to be defined by regulations issued under the statute.[233] Nevertheless, the Modernization Act does provide

228. *Id.* § 509(4).

229. CARAT GUIDELINES, GUIDELINES FOR CONSTRUCTING POLICIES GOVERNING THE USE OF IDENTITY-BASED PUBLIC KEY CERTIFICATES 95 (Sept. 1999) [hereinafter CARAT GUIDELINES]. *See also* Richard Fischer & Clarke Dryden Camper, *Reform Law and Privacy: A Road Map*, AM. BANKER, Nov. 19, 1999, at 6. Data privacy refers to personal information about a consumer, such as his Social Security number, address, and age. Transactional privacy refers to information about a consumer's business transactions such as the stores where the consumer shops and what items the consumer purchases. The CARAT guidelines, developed by the National Automated Clearing House Association's Internet Council Certification Authority Rating and Trust Task Force, also defines transactional privacy as information that a subject may not realize is being collected about himself. See CARAT GUIDELINES, *supra*. The guidelines state that the subject has the same expectation of privacy regardless of whether the subject knowingly provides data to an entity or the information is collected without his knowledge. *See id.*

230. *See* Alan Zeichick, *Ad Serving Explained*, RED HERRING, Jan. 2000, at 216-17.

231. Gramm-Leach-Bliley Financial Modernization Act § 509(4)(A).

232. Fischer & Camper, *supra* note 229, at 6.

233. *See* Gramm-Leach-Bliley Financial Modernization Act § 509(4)(B).

that some types of publicly available information are included within the meaning of nonpublic personal information.[234]

A major limitation of the Modernization Act is its application only to financial institutions[235] and other persons and entities who are involved in information sharing directly or indirectly related to nonpublic information possessed by the financial institution.[236] Therefore, it imposes no duties upon Web businesses that are not themselves financial institutions as defined by the Modernization Act or that do not share information with financial institutions. The Modernization Act does include a broad definition of "financial institution," however, which includes not only traditional depository institutions such as banks, but also broker-dealers, investment companies, investment advisers, and insurance companies.[237] Moreover, its coverage may also include businesses which do not come within the common understanding of what constitutes a financial institution.[238]

Despite the broad definition of financial institution, it may nevertheless be underinclusive given the overlapping nature of e-commerce, which often involves financial institutions and other businesses. For example, a consumer may engage in home bank-

234. Nonpublic personal information includes "any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable information other than publicly available information." *Id.* § 509(4)(C)(i).

235. The Act defines "financial institution" as "any institution the business of which is engaging in financial activities or activities that are incidental to financial activities, as described in section 4(k) of the Bank Holding Company Act of 1956." *Id.* § 509(3)(A). The term does not include persons or entities subject to the jurisdiction of the Commodity Futures Trading Commission, the Federal Agricultural Mortgage Corporation, or any entity chartered under the Farm Credit Act of 1971, or institutions chartered by Congress to engage in transactions described in section 502(e)(1)(C) of the Modernization Act, as long as they do not sell or transfer nonpublic personal information to a nonaffiliated third party. *See id.* §§ 509(3)(B)-502(e)(1)(C). Section 502(e)(1)(C) applies to secondary market institutions.

236. For example, the Modernization Act also applies to nonaffiliated third parties with whom the financial institution shares information. *See id.* § 502(d) (stating that a financial institution may not disclose account number information for marketing purposes to nonaffiliated third parties). In addition, restrictions are placed on these third parties sharing with "fourth parties." *See id.* § 502(c) (restricting the reuse of information by third parties).

237. *See id.* § 509(3)(A); *Privacy and the Gramm Leach Bliley Act*, KPMG Memorandum (Nov 12, 1999) (unpublished, on file with author) [hereinafter KPMG Memorandum]. Under certain circumstances it also may include travel agents and automobile dealers. *See* Roderer, *supra* note 214, at 855.

238. "This definition [of financial institution] could include . . . a merchant or manufacturer that extends credit or a nonbank that issues stored value cards or sells money orders." Fischer & Camper, *supra* note 229, at 6.

ing from her PC, transferring funds from her savings account to her checking account. At the same sitting she may use the bank's electronic bill-paying service to pay bills resulting from transactions with both Web-based and bricks-and-mortar stores, which she charges on her present credit card account. After paying those bills she may apply for an additional credit card from the bank. Immediately thereafter, she may use her credit card account to purchase items from Web sellers. The consumers' privacy concerns and expectations in regard to her credit card account will not be significantly different whether she is conducting transactions with a financial institution or with the Web sellers. Nevertheless, presumably the Web seller is not considered a financial institution unless that seller has itself issued the credit card.[239]

As discussed below,[240] it is expected that many states will enact privacy laws to expand the coverage of privacy protection beyond the scope of the Modernization Act. That may result in state laws which include non-financial institutions. If that happens, the industry likely will urge Congress to enact a new law or an amendment to the Modernization Act to cover non-financial institutions and to preempt state law. Presumably, industry will urge language more limited in scope than what states have enacted. Even if it is not more limited than state law, it will be advantageous to industry in being uniform nationally, rather than the variation which occurs when each state enacts its own version. If Congress enacts legislation to cover non-financial institutions, the possibility arises that this legislation could impose obligations upon non-financial institutions and provide protections to consumers which are different from those in the Modernization Act. This would result in confusion for consumers as they receive different disclosures and notices depending on with which type of business they are dealing.

In addition, consumers may confuse the protections of one law with those of another law, believing they have more protection than they actually have, and engaging in transactions they otherwise would avoid. This confusion has already occurred in regard to debit cards. The law provides consumers with far less protection for debit cards than for credit cards,[241] but consumers

239. *Cf. id.* (opining that a merchant who extends credit may be considered a financial institution under the Modernization Act).

240. *See* text *infra* accompanying note 301.

241. For example, the maximum consumer liability for unauthorized use of a credit card is $50. *See* 15 U.S.C. § 1643(a)(1)(B)(1994). The liability for debit cards ranges from $50 to whatever amount the consumer has in her

do not understand the difference.[242] On the other hand, the confusion caused by having two different laws may lead consumers to wrongly believe they have less protection for debit cards than the law actually provides. As a result, consumers may avoid transactions they would willingly enter into if they realized they were protected.

Turning from the scope of the Modernization Act to its substance, the Modernization Act requires a privacy policy disclosure. Financial institutions must disclose their "policies and practices" in regard to certain matters.[243] In using that phrase, the Modernization Act recognizes that there is a difference between an institution's policies and its practices. Whereas a "policy" is "a principle or course of action chosen to guide decisionmaking,"[244] a "practice" is the "[a]ctual performance."[245] This requirement should be viewed in connection with another section of the Modernization Act which requires enforcement agencies to establish standards for institutions which "insure the security and confidentiality of customer records and information."[246]

The Modernization Act requires the institution to inform consumers with whom it has established a customer relationship of its policies and practices in regard to the following:

> 1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 502, including the categories of information that may be disclosed;
>
> 2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and
>
> 3) protecting the nonpublic personal information of consumers.[247]

This privacy policy disclosure requirement is limited to disclosure of policies and practices in regard to nonpublic personal infor-

---

account, depending upon when the consumer notifies the card issuer. *See* 15 U.S.C. § 1693(g) (1994).

242. *See Debit Cards Still Confuse Many Consumers*, PALM BEACH POST, Mar. 15, 1999, at 15 (reporting on a survey by the National Consumers League which showed that consumers did not understand their liability when using debit cards).

243. *See* Gramm-Leach-Bliley Financial Modernization Act § 503(a).

244. WEBSTER'S II NEW RIVERSIDE DICTIONARY 540 (1984).

245. *Id.* at 548.

246. Gramm-Leach-Bliley Financial Modernization Act § 501(b)(1).

247. *Id.* § 503(a). The reference to § 502 is to the section that requires notice of sharing with third parties and opportunity to opt-out.

mation. As noted above,[248] this presents problems of application because the Modernization Act contains no definition of "public personal information." Whereas the Modernization Act contains a major loophole in exempting sharing information with affiliates from the notice and opt-out requirements of section 502, the privacy policy disclosure provision requires the institution to disclose its policies, not only in regard to sharing information with nonaffiliated third parties, but also with its own affiliates. The disclosure must be made "[a]t the time of establishing a customer relationship with the consumer."[249] The apparent objective of requiring disclosure at this early time is to ensure that the customer is alerted to the risk to his privacy at a meaningful time. The consumer who objects to the institution's policies and practices of sharing information with affiliates could avoid having information about himself shared with non-affiliates by refusing to do business with the institution before any information is shared. The Modernization Act requires the institution to inform the consumer of its policies and practices, not only while the consumer is a customer of the institution, but also after the consumer is no longer a customer of the institution. This is a significant provision because it is likely that at the beginning of a relationship with an institution many consumers would not think about what may happen to personal information when the consumer's relationship with the firm has terminated.

The disclosures must describe both the "categories of persons to whom information is or may be disclosed,"[250] and "the categories of nonpublic information that are collected by the financial information."[251] Consumers would receive a more informative disclosure if the Modernization Act required the institution to provide the names of the persons or entities to whom information is disclosed and to describe the nonpublic information that it collects, rather than merely listing categories. To require that, however, would present problems if the law also required the institution to notify the customer whenever there was a change in the information disclosed. Since the institution must notify the customer annually, however, the law could

248. *See supra* text accompanying note 232.

249. Gramm-Leach-Bliley Financial Modernization Act § 503(a). The disclosure must also be given at least annually thereafter. *See id. See also* Proposed Regulations, *supra* note 212, at 8775 (requiring that notice be provided prior to the time a customer relationship is established).

250. Gramm-Leach-Bliley Financial Modernization Act § 503(b)(1)(A).

251. *Id.* § 503(b)(2). *See also* Proposed Regulations, *supra* note 211, at 8776 (providing that information can be categorized according to source and giving examples).

require that once a year the institution compile a list of companies to whom it may disclose information and a list of the specific nonpublic information it collects. The disclosure to the customer would explain that the list may not be entirely accurate because it is updated only once each year. Such a requirement would give the customer the information she needs without unduly burdening the institution. At the very least, the institution should be required to name the affiliates with whom it shares information. Because the term "categories" is not defined in the Modernization Act, regulations may provide a definition. The requirement of describing categories will be practically meaningless if an institution, for example, can describe categories of persons to whom information may be disclosed merely as "affiliates of the institution who sell insurance products." The consumer needs to know that the financial institution will share information with affiliate XYZ Insurance Company which is in the business of selling life health insurance. That type of disclosure will alert the consumer who has life, disability, or health insurance from XYZ Insurance Company that if she requests a loan from the financial institution, its insurance affiliate may share medical information it has collected about the consumer.

Finally, the institution must disclose how it protects its nonpublic personal information. Although not absolutely clear, that requirement most likely is explained by a provision later in the section which states that the required disclosures must include "the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information."[252] The requirement thus refers to both privacy safeguards and the closely related area of security.[253] Banks already make disclosures which may satisfy some of the Modernization Act's requirements. For example, U.S. Bancorp used to inform consumers that all of its employees must follow a Code of Ethics under which they must keep customer information confidential, an obligation which continued even after they no longer worked at

252. Gramm-Leach-Bliley Financial Modernization Act § 503(b)(3). *See also* Proposed Regulations, *supra* note 212, at 8777-78 (stating that the institution can satisfy the confidentiality and security requirements by explaing who has access and how they may obtain access).

253. *See* Roderer, *supra* note 214, at 855 ("[U]nheeded by most is the persistent reference to security throughout the title as a separate and equal value under the new law. The regulatory and ultimately legal standards for security to which financial institutions might be held accountable will likely only unfold in time-and through litigation.").

the bank.[254] U.S. Bancorp also notifies customers of their security measures.[255]

Requiring the institution to disclose its policies and practices presents risks for the institution. It must be sure its disclosures accurately state its policies and practices or it may encounter difficulties similar to those U.S. Bank faced in Minnesota. This may require monitoring the conduct of its employees to ascertain what their actual practices are. If the institution changes its policies and practices, it must be sure those changes are accurately reflected in its disclosures. The Modernization Act does not spell out the institution's duties when it adopts such changes. For example, it is not clear whether the institution is required to promptly notify all of its customers of the changes, or whether it can wait until the mandated annual notice to do so.

The disclosure of privacy policy must be "clear and conspicuous," and the institution can provide the required disclosure either in writing or in electronic form.[256] In case there may be some other acceptable manner of providing notice that Congress had not thought of, the Modernization Act gives federal agencies the authority to issue regulations which permit notice in other formats. This raises the possibility that regulations could allow notice to be made orally. Oral notice is problematic. If the institution chooses that alternative, it is inviting claims by consumers that the disclosures were never made, or that they were not made clearly and conspicuously. The allowance of electronic notice also is problematic. For example, could an institution make electronic disclosures even if the consumer was not informed that the institution had chosen that method, and even if the consumer did not agree to that form of disclosure?[257] Could the

254. The bank's privacy page was revised to state instead, "Employees' access is restricted to their need to know such information for business reasons. All employees are trained to respect customer privacy, and those who violate our Privacy Pledge will be subject to discipline." USBancorp, *US Bankcorp Privacy Policy* (visited Jan. 28, 2000) <http://www.usbank.com/privacy.html>.

255. The bank uses Secure Sockets Layer to encrypt transmissions. *See id.*

256. *See* Gramm-Leach-Bliley Financial Modernization Act § 503(a). *See also* Proposed Regulations, *supra* note 212, at 8771 (defining clear and conspicuous); Will Roger, *Privacy Isn't Public Knowledge: Online Policies Spread Confusion With Legal Jargon*, USA TODAY, May 1, 2000, at 3D (stating many sites' privacy policies are difficult to understand).

257. *See, e.g.*, 63 Fed. Reg. 14548 (1998) (proposed March 25, 1998, proposing a rule amending Reg. Z to permit creditors to use electronic communication). *See also* Proposed Regulations, *supra* note 212, at 8775 (stating that oral notice alone is not sufficient and permitting notice via electronic mail to a consumer who obtains financial products or services electronically and notice on a Web page if the consumer is in the process of conducting a transaction over the Internet).

institution choose that method even it had no reason to believe the consumer owned or had access to a computer? Even if the institution obtained a signed agreement from the consumer consenting to electronic disclosure, the institution would have to be careful to maintain systems capable of proving to regulatory authorities and others who might challenge the institution's compliance that the mandates of the Modernization Act had been followed in regard to the timing and contents of the notice. The Modernizatin Act seems to require agencies to issue regulations pursuant to the section containing the disclosure provisions.[258] Hopefully, those regulations will answer the preceding questions.

In addition to requiring the disclosure of the institution's privacy policy, the Modernization Act requires the institution to provide a notice to the consumer prior to sharing information, either directly or through an affiliate, with unaffiliated third parties.[259] The information must "clearly and conspicuously" inform the consumer that nonpublic personal information may be disclosed to "such third party."[260] By using this latter language rather than merely requiring the disclosure of categories of persons as is required for the privacy policy disclosure,[261] the Modernizatin Act seems to require the institution to specifically name the third party, rather than merely notify the consumer of the type of third parties, for example, telemarketers, with whom information would be shared.[262] The notice may be either in writing or in electronic form or other form allowed by regulation, raising the same issues as discussed above in regard to the privacy policy disclosure.[263]

In addition to informing the consumer that it may share nonpublic personal information with nonaffiliated third parties, the institution also must give the consumer the opportunity "to direct" that the information not be disclosed to the third party.[264] In the parlance of privacy protection, this is known as an "opt-out." The institution must provide the opt-out before it

258. Section 503(a) provides: "Such disclosures shall be made in accordance with the regulations prescribed under section 504." Gramm-Leach-Bliley Financial Modernization Act § 503(a).

259. *See id.* § 502(a).

260. *Id.* § 502(b)(1)(A).

261. *See id.* at § 503(b)(1)(A).

262. Contrast the language of section 503(b)(1)(A), which requires merely the disclosure of the "categories of persons to whom the information is or may be disclosed." *But see* Proposed Regulations, *supra* note 211, at 8778 (permitting the institution to identify categories).

263. *See supra* text accompanying note 256.

264. Gramm-Leach-Bliley Financial Modernization Act § 502(b)(1)(B).

initially discloses nonpublic personal information. In addition, the institution must explain to the consumer how she can exercise the nondisclosure option.[265] The Modernization Act does not contain any specifics on how the consumer can opt-out. The question arises whether the method of opt-out is entirely up to the institution. If the institution can choose any method it wants, it could require the consumer to opt-out by sending an e-mail message to the institution. This would be unfair if the consumer did not have access to e-mail. Even if the consumer has access to e-mail, she may prefer to exercise the option in writing and send it by mail. The Modernization Act does not indicate whether she would be able to do so, regardless of whether the institution sought to require opt-out only via e-mail.

Whereas the disclosure of the institution's privacy policy must be provided annually,[266] there is no such explicit requirement for the opt-out notice. That raises the issue of whether the institution can impose a time limit on the consumer's ability to opt out, after which the consumer forever loses her ability to ever opt-out.[267]

The significance of certain portions of the Modernization Act can be better understood when they are contrasted with the Settlement between U.S. Bank and Minnesota. The scope of the Modernization Act is broader than the Minnesota Settlement in applying to all types of third parties, including those selling financial products.[268] It is narrower than the Settlement, however, in not prohibiting the sharing of information with third parties,[269] but merely requiring disclosure and the opportunity to opt-out. Therefore, financial institutions could continue to share information with third parties selling nonfinancial products, but only after consumers are fully informed that would be done and the consumers failed to opt-out. Arguably, having been informed and not opting-out, the consumer no longer has an expectation of privacy in regard to that sharing. Privacy advo-

265. *See id.* § 502(b)(1)(C).

266. *See id.* § 503(a).

267. "A colloquy between Sens. Phil Gramm and Michael Crapo during Senate consideration of the bill confirms that this notice and opt-out opportunity only has to be given once; in other words, it does not have to be provided separately for each disclosure of covered information or for each nonaffiliated entity to which such information may be provided." Fischer & Camper, *supra* note 229, at 6. *See also* Proposed Regulations, *supra* note 212, at 8778 (stating that the consumer always has the right to opt-out).

268. The Minnesota Settlement applies only to unaffiliated third parties marketing nonfinancial products or services. *See* Settlement, *supra* note 107, at ¶ 11.

269. *See id.*

cates, however, favor an opt-in procedure as necessary to ensure consumers truly intend to surrender their privacy.[270] Failure to opt-out is passive; the consumer may not have paid attention to the disclosure, may have intended to opt out but forgot to, may have a limited understanding of English, etc. If the forthcoming regulations allow the institution to require the consumer to exercise opt-out by sending an electronic message, the meaningfulness of the option is even more doubtful. Opt-in requires an affirmative act, providing much stronger proof of the consumer's actual intention not to protect her privacy.

The Settlement provides that if the consumer exercises the option to opt-out, the bank must remove his name from the lists it provides to third parties.[271] The Modernization Act is silent, merely requiring the consumer to "direct" that the information not be disclosed to third parties, but not saying what the bank is required to do when the consumer exercises his option. In addition, although the law requires the bank to explain to consumers how they can exercise opt-out, it does not provide any standards or procedures. For example, can the bank require that the consumer's opt-out be in writing, or be in electronic form if the bank's disclosure is in electronic form? Can the bank require the consumer to exercise opt-out within five business days or forever relinquish his right to opt-out? The Modernization Act does, however, provide for the situation where the consumer does not exercise opt-out, the information is consequently shared with a third party, and the third party in turn shares it with a "fourth" party. The third party may not disclose nonpublic personal information to a "fourth" party unless that disclosure would be lawful if the financial institution had made the disclosure directly to the "fourth" party.[272]

The scope of the Modernization Act also is narrower than the Settlement in excluding from coverage under the opt-out section an institution sharing information with its affiliates. The Settlement provides that the consumer can opt out of the bank's

270. *See* Gramm-Leach-Bliley Financial Modernization Act § 508(a)(8) (directing federal agencies to conduct a study, *inter alia*, of the feasibility of an opt-in procedure); Sovern, *supra* note 5, at 1074-78 (describing problems consumers have had opting out of mailing lists); Lisa Fickenscher, *States Expected to Tighten Reform's Privacy Provisions*, AM. BANKER, Nov. 19, 1999, at 11; Richard Wolf, *Privacy is a Priority With Voters, State Legislators Say*, USA TODAY, Jan. 19, 2000, at A3 (reporting that privacy proponents advocate giving consumers control, while bankers claim opt-in would be disastrous because consumers will not take the time to opt-in).

271. *See* Settlement, *supra* note 107, at ¶ 20.

272. *See* Gramm-Leach-Bliley Financial Modernization Act § 502(c). The third party's affiliate is subject to the same restriction. *See id.*

sharing information with affiliates.[273] Whether or not to include affiliates in the Modernization Act's coverage was a major point of contention. The House Commerce Committee's bill had included affiliates.[274] Small banks contended that, if privacy legislation were enacted, it should include affiliates in order to ensure a level playing field.[275] According to the smaller banks, they have to use third parties to perform many operations, whereas the big banks have affiliates for many tasks. Therefore, the big banks would seldom or never have to comply with the statute's restrictions on sharing with third parties, whereas the smaller banks would constantly be subject to it. The larger banks won that battle, contending that the ability to cross-sell products from affiliate to affiliate was often a primary objective in a merger among different types of financial institutions.[276]

The Modernization Act contains significant exceptions to its third party notice requirements. The disclosure of nonpublic personal information is not prohibited if it is "necessary to effect, administer, or enforce a transaction requested or authorized by the consumer."[277] The disclosure of such information also is not prohibited if the consumer consents to it.[278] It is not clear what might constitute consent which meets the requirements of the Modernization Act. Institutions might be tempted to insert consent clauses into agreements in a format unlikely to be noticed and phrased in legalese. These should not pass muster. It has been suggested that the institution must obtain "informed consent" and "a clear and conspicuous notice of such sharing above a signature line" would be sufficient.[279] In addition, disclosure is not prohibited if it is necessary to administer a transaction, or to

273. *See* Settlement, *supra* note 107, at ¶ 20.

274. *See* Anason, *supra* note 202, at 2.

275. *See* Dean Anason, *Gramm: Privacy Safeguards May be Essential Concession for Financial Reform Passage*, AM. BANKER, Oct. 5, 1999, at 2 (Senator Gramm opposed excluding affiliates which would give diversified holding companies a competitive advantage over community banks); Stephen Labaton, *Lawmakers Reject Clinton Changes to Finance-Overhaul Bill*, N.Y. TIMES, Oct. 19, 1999, at 13 (house defeats Congressman Markey's amendment to apply the third party notice to affiliates); Norbert McCrady, *Personal Data Firewall Remains an Illusion*, AM. BANKER, Sept. 3, 1999, at 6 (opining that excluding affiliates puts small banks at an unfair disadvantage); Schroeder, *supra* note 38, at A50 (Republican Senator Richard Shelby sponsored an unsuccessful amendment to apply the third party notice to affiliates).

276. *See* Schroeder, *supra* note 38, at A50.

277. Gramm-Leach-Bliley Financial Modernization Act § 502(e)(1). This sweeping exclusion is defined at great length. *See id.* § 509(7).

278. *See id.* § 502(e)(2).

279. *See* L. Richard Fisher & Clarke Dryden Camper, *Exceptions to Reform's Privacy Obligation*, AM. BANKER, Dec. 3, 1999, at 8.

service or process a product or service.[280] Although sharing information with third parties who service or process a product or service is permitted, those third parties must comply with the information confidentiality requirements which apply to the institution for which it is doing the servicing or processing.[281] Disclosure is allowed when its purpose is to protect the confidentiality or security of the institution's records, to protect against fraud, for risk control or to resolve consumer disputes or inquiries.[282] Information may be disclosed to insurance rate advisory organizations,[283] credit reporting agencies,[284] and to a person acting as the fiduciary of the consumer.[285] Disclosure may also be made to law enforcement agencies.[286] The third party disclosures need not be made in connection with maintaining a consumer's account with another entity as part of a private label credit card program or any other credit extension of credit on behalf of that entity.[287]

There are sound reasons for many of these exceptions. The problem is that the statute does not require the institution to disclose those exceptions to the consumer. As a result, absent regulatory action, the institution may make the required disclosures to consumers informing them of the institution's privacy policy, describing how generally the information will be kept confidential, may make the required third party notice, but then add the standard phrase, "except where otherwise permitted or required by law." The consumer will have no inkling how extensive the exceptions are unless they are described in the notice. As an alternative, in the notice, the institution could inform the consumer that there are many exceptions allowed by law and provide the consumer with an easy method for obtaining a detailed description of those exceptions.

There also are exceptions which apply specifically to the opt-out provision. The opt-out provision does not prevent an institu-

280. *See* Gramm-Leach-Bliley Financial Modernization Act § 502(e)(1). This would apply to third parties which process or administer pay which are made by consumers paying by check, credit card, or debit card.

281. *See* Fisher & Camper, *supra* note 280, at 8.

282. *See* Gramm-Leach-Bliley Financial Modernization Act § 502(e)(3).

283. *See id.* § 502(e)(4).

284. *See id.* § 502(e)(6)(A).

285. *See id.* § 502(e)(3)(E).

286. *See id.* § 502(e)(8).

287. *See id.* § 502(e)(1)(B). This exception was inserted "without a full conference-committee debate . . . The exemption applies to retailers who offer credit cards issued and serviced by third-party firms, such as GE Capital and Household International, Inc." Michael Schroeder, *Congress Passes Financial-Services Bill*, WALL ST. J., Nov. 5, 1999, at A2.

tion from sharing information with a nonaffiliated third party where that party performs functions for the institution or functions on behalf of the institution.[288] Consequently, a third party can use the institution's information about consumers to market the financial institution's own products or services. In addition, a third party can perform services for two or more institutions pursuant to joint agreements between the institutions as long as each institution "fully discloses" that it is providing information to the third party.[289]

The types of entities excepted under these provisions of the Modernization Act may actually increase beyond those listed in the statute. The federal banking agencies are authorized to promulgate regulations.[290] While this provides the opportunity for filling in the holes discussed above, the Modernization Act also permits the regulations to include additional exceptions which are "deemed consistent with the purposes" of the law.[291] That is a rather vague standard, and the industry may be expected to try to gain further exceptions to ameliorate the effect of the law. Therefore, absent regulatory clarification, there will be great uncertainty regarding the scope of the statute.

A statute is not worth the paper it is printed on unless it provides an effective means for enforcing its provisions. The Modernization Act contains a major defect in regard to enforcement. Federal and state agencies are given the authority to enforce the statute.[292] Banks are subject to enforcement by the agency having jurisdiction over them. Financial institutions not subject to the jurisdiction of any other agency are subject to enforcement by the Federal Trade Commission. Federal and state consumer protection laws recognize that there is no way that government agencies can possibly enforce these laws effectively, given their many other enforcement duties, their need to

288. *See* Gramm-Leach-Bliley Financial Modernization Act § 502(b)(2).

289. *Id.* § 502(b)(2). The institution is required to enter into an agreement with the third party requiring that party to keep the information confidential. "Joint agreement" is defined in section 509(10). This provision "address[es] a potential imbalance between the treatment of large financial services conglomerates and small banks or credit unions." Roderer, *supra* note 214, at 854-55. It has been suggested that the "fully discloses" language means the disclosure must conform to the "clear and conspicuous" requirement of section 502(b)(1)(A). *See* Fisher & Camper, *supra* note 280, at 8.

290. *See* Gramm-Leach-Bliley Financial Modernization Act § 504(a).

291. *Id.* § 504(b).

292. *See id.* § 505(a).

prioritize, and limited resources.[293] In addition, they are subject to congressional pressures which influence their setting of priorities.[294] Therefore, these laws provide for a private right of action so consumers can sue.[295] Moreover, they contain provisions for statutory damages, attorney's fees, and class actions in order to encourage consumers to act as "private attorneys general."[296] The Modernization Act, however, does not authorize a private right of action for consumers. Consumers, consequently, are unable to sue directly for violation of the statute. They may, nevertheless, be able to sue under statutes such as state Unfair and Deceptive Practice laws, arguing that a violation of the federal privacy law is an unfair or deceptive practice.[297] That avenue does not afford consumers with as effective a remedy as a private right of action under the Modernization Act, however, because many state UDAP statutes contain various types of restrictions and limitations which place obstacles in the way of consumer's seeking redress.[298]

The industry's successful effort to restrict the reach of the Modernization Act's privacy provisions may backfire. The Modernization Act provides that it preempts only state law that is inconsistent, and then only to the extent of the inconsistency.[299] In addition, a state law is not considered inconsistent if the FTC determines that it provides consumers with greater protection

293. *See Complaints Rise, But Not Complaint Agency Budgets*, CFA NEWS, Dec. 1999-Jan. 2000, at 4 (stating that complaints to state and local consumer agencies rose 49% from 1996 to 1998, but agencies had the same budgets).

294. *See generally* Mark E. Budnitz, *The FTC's Consumer Protection Program During the Miller Years: Lessons for Administrative Agency Structure and Operation*, 46 CATH. U. L. REV. 371 (1997).

295. *See, e.g.*, Truth in Lending Act, 15 U.S.C. § 1640 (1998).

296. *Id. See also* Kronebusch v. MVBA Harvestore Sys., 488 N.W.2d 490 (Minn. Ct. App. 1992) (allowing recovery of costs and attorney's fees for violation of statute prohibiting misleading advertising in order to encourage lawyers to bring cases where nominal damages would otherwise preclude such actions); JONATHAN SHELDON & CAROLYN L. CARTER, UNFAIR AND DECEPTIVE ACTS AND PRACTICES 513-82 (4th ed. 1997) (discussing consumer remedies under state unfair and deceptive trade practice laws); Emily Heller, *Junk Fax Ads Irritate Consumers but May Yield Windfall for Lawyers*, FULTON CO. DAILY REP., Jan. 12, 2000, at 1 (quoting plaintiff's lawyers, who stated that while an individual consumer case is not financially attractive because so little money is involved, a class action is).

297. *See* Roderer, *supra* note 214, at 855.

298. *See* SHELDON & CARTER, supra note 297, at 47-111, 465-80 (discussing the scope of state consumer statutes and preconditions to bringing private actions); Donna S. Shapiro, *The Georgia Fair Business Practices Act*, 9 GA. ST. U. L. REV. 453 (1993) (discussing the restrictions courts have imposed upon consumer actions under Georgia's UDAP statute).

299. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102 § 524(a), 113 Stat. 1338 (1999) (to be codified at 15 U.S.C. § 6801).

than the Modernization Act.[300] Twenty-five states and some municipalities have been considering privacy legislation which would provide greater protection than that afforded by the Modernization Act.[301] State laws requiring the more consumer-friendly opt-in rather than the Modernization Act's opt-out are a principal issue attracting attention.[302] If these bills are enacted, financial institutions operating in many states would have to comply with many different state privacy laws.[303] The Comptroller of the Currency urged banks to try to halt this trend by voluntarily providing more protection than required by the Modernization Act in order to show that new state law is unnecessary.[304]

C. *Congressional Privacy Bills*

It is instructive to compare the Modernization Act with other privacy bills which were before the first session of the 106th Congress in order to further evaluate the strengths and weaknesses of the Modernization Act. Several bills would regulate Internet transactions. They would cover some of the same areas as the Modernization Act which applies both to Internet and traditional modes of conducting business with financial institutions. At the same time, they would have a broader scope than the Modernization Act because they would apply to all types of companies doing business on the Internet, not just financial institutions.

Consumers may be confused about the scope of the Modernization Act, incorrectly believing it covers all electronic commerce. The enactment of new privacy legislation could lessen that confusion. Financial institutions increasingly are offering online banking services. Many traditional banks offer such services,[305] and several exclusively Internet banks have been estab-

300. *See id.* § 524(b).

301. *See* Dean Anason, *Consumer Privacy Laws May be Set to Spread Like Wild Fire in States*, AM. BANKER, Dec. 6, 1999, at 1, 6 (reporting on activities in states and municipalities). States were actively considering bills even before enactment of the federal law. *See* Martha Kessler, *Privacy Bill Could Have Sweeping Impact on Banking Industry, State Bankers Warn*, BANKING REP. (BNA), Aug. 2, 1999, at 168 (describing Massachusetts privacy bill); Laura Mahoney, *California Senators Eye State Law Protecting Privacy of Bank Customers*, BANKING REP. (BNA), July 19, 1999, at 88 (describing testimony on bill to regulate banks' sale of personal information to telemarketers); Gerald Silverman, *Package of Privacy Bills Approved by New York State Assembly*, BANKING REP. (BNA), June 7, 1999, at 10, 13 (describing New York privacy bills).

302. *See* Anason, *supra* note 302, at 6.

303. *See* Fickenscher, *supra* note 270 (quoting Christine Varney, an attorney, as saying "The worse scenario is 50 different privacy regimes.").

304. *See* Anason, *supra* note 302, at 6.

305. *See, e.g.*, Citibank, *Online Financial Solutions* (visited Feb. 2, 2000) <http://www.citibank.com>.

lished.[306] Surveys have indicated that consumers are very concerned about their privacy when dealing with financial institutions, and worried about invasions of their privacy when doing business on the Internet.[307] The Modernization Act requires financial institutions to have a privacy policy and to disclose that policy to consumers.[308] It requires notice of the bank's practices regarding disclosure of nonpublic personal information to third parties.[309] Presumably, as a result of these privacy measures, consumers will become less worried about possible privacy intrusions and will do more banking online. In addition, they may engage in other types of business as well, wrongly believing the full panoply of privacy rights contained in the Modernization Act applies to every type of Internet transaction.

The Modernization Act permits banks, insurance companies and brokerage firms to merge. As described above,[310] the Modernization Act provides far less privacy protection in regard to information sharing among these affiliates. Consumers, however, may not realize the protection they lose when they do business with the insurance company or brokerage firm that is affiliated with their bank as opposed to an independent insurance company or brokerage, and will increase their online business with these companies as well. The fact that the Modernization Act applies, not only to banking, but to the sale of insurance and securities, may confuse consumers into believing that the Modernization Act's coverage is broader than it actually is. They may believe the Modernization Act covers all types of transactions, including the sale of goods and services on the Web. The likelihood of this confusion is probably increased by the very fact that many Web sellers voluntarily post privacy policies and official-looking privacy seals on their sites.[311] Consumers may think Web sellers do this in compliance with some legal requirement. Because there is no law establishing minimum requirements, however, Web sellers' voluntary privacy policy may

306. *See, e.g.*, Security First Network Bank (visited Oct. 31, 1999) <http://www.sfnb.com>.

307. *See* Fickenscher, *supra* note 270, at 11 (reporting on a Louis Harris survey in which consumers said they did not trust companies that gather information online).

308. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102 § 503(a), 113 Stat. 1338 (1999) (to be codified at 15 U.S.C. § 6801).

309. *See id.* § 502(a).

310. *See supra* text accompanying notes 282-288.

311. *See, e.g.*, Land's End, *Home Page* (visited Feb. 2, 2000) <http://www.landsend.com/cd/frontdoor>.

not offer any meaningful protection,[312] and there may not be any way to enforce the posted policy. Consumer misunderstanding of the extent to which the law protects their privacy will be lessened by the enactment of new statutes which broaden that protection to areas not covered by the Modernization Act.

A major loophole in the Modernization Act is its exclusion of affiliates from the third party notice and opt-out.[313] House Bill 1339 would close that loophole by imposing notice requirements which apply to affiliates as well as other third parties.[314] The bill offers greater protection to consumers than the Modernization Act by providing for an opt-in procedure rather than the Modernization Act's opt-out.[315] Finally, whereas the Modernization Act requires disclosure of an institution's policies and practices in regard to disclosing personal information at the time the customer relationship is established and annually thereafter,[316] this bill requires the institution to inform its customers "whenever . . . financial information is being collected that pertains to such customers."[317]

Senate Bill 809, the Online Privacy Protection Act of 1999, applies to operators of Web sites and online services. It requires the FTC to promulgate regulations which would, inter alia, require covered businesses to give consumers who have provided personal information to the business "a description of the specific types of personal information collected by that operator that was sold or transferred to an external company" upon the consumer's request for that information.[318] This goes beyond the Modernization Act which requires only a disclosure of the categories of persons to whom information may be disclosed and

312. *See* Guernsey, *supra* note 167, at 1, *available in* 1999 WL 2882191 (stating that the posting of a seal on a site does not mean the Web merchant displaying the seal will not sell your personal information to others).

313. *See supra* text accompanying notes 274-276.

314. *See* H.R. 1339 § 2, 106th Cong. (1999). In May, 2000, President Clinton announced that he will introduce legislation extending the opt-out to affiliates.

315. *See id.* § 2(a) (An institution would not be permitted to share information except "upon the affirmative written request, or with the affirmative written consent, of the customer to whom the information pertains").

316. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102 § 503, 113 Stat. 1338 (1999)(to be codified at 15 U.S.C. § 6801).

317. H.R. 1339 § 2.

318. S. 809 § 2(b)(1)(B)(i), 106th Cong. (1999). "Personal information" is defined to include the consumer's first and last name, her home and other physical address, e-mail address, social security number, telephone number, any other identifier that the FTC determines identifies an individual, or information "that is maintained with, or can be searched or retrieved by means of, data described" in the above five categories. *Id.* § 8(8).

types of information collected.[319] In addition under Senate Bill 809, the operator must provide the consumer with a reasonable means "to obtain the personal information."[320] This is an important provision because it provides an ingredient regarded by many as essential to consumer privacy, that is, access to information about the consumer. The Modernization Act does not grant consumers the right to access.[321]

Finally, Senate Bill 809 contains an interesting provision acknowledging the role which self-regulation could play. Representatives of the marketing and online industries, as well as many others, are encouraged to draft their own guidelines. If they are approved by the FTC, a person who complies with them would be deemed in compliance with the regulations issued by the FTC.[322]

Whereas Senate Bill 809 grants consumers the right of access, House Bill 313, the Consumer Internet Privacy Protection Act takes the next crucial step by also giving the consumer the right to correct any error in the information maintained by the computer services covered by the bill.[323] The Modernization Act, by not granting the consumer access to her information, obviously also does not provide a right to correct the institution's information about the consumer.[324]

The bill also contains two other important provisions. First, it improves on Senate Bill 809 by not only granting access, but also providing that the company cannot charge a fee for making the requested information available. This may be seen as an acknowledgment that the consumer has some type of legal interest in information about herself, and that it would be unfair to charge the consumer a fee for that information. Finally, the bill prohibits disclosure of personal information unless the consumer supplies "prior informed written consent."[325] The Mod-

319. *See* Gramm-Leach-Bliley Financial Modernization Act §§ 503(b)(1)(A), 503(b)(2).

320. S. 809 § 2(1)(B)(ii). There are exceptions when this requirement does not apply. *See id.* § 2 (b)(2)(3).

321. Both the Guidelines and the Directive provide consumers with access to their information. Guidelines, *supra* note 184; Directive, *supra* note 185, at art. 12.

322. *See* S. 809 § 3.

323. *See* H.R. 313 § 2 (C)(1)(C), 106th Cong. (1999). The bill covers "interactive computer services" defined as "any information service that provides computer access to multiple users via modem to the Internet." *Id.* §4(1).

324. Both the Guidelines and the Directive permit the consumer to correct inaccurate and incomplete information. Guidelines, *supra* note 184; Directive, *supra* note 185, at art. 12(c).

325. H.R. 313 § 2.

ernization Act permits disclosure to third parties "with the consent or at the direction of the consumer."[326] The bill contains much stronger language to protect the consumer by requiring that the consent be in writing and be "informed." Moreover, the bill provides that where the consumer has given her consent, she can revoke it at any time.[327] Presumably, this is also true under the Modernization Act, but it does not say this explicitly.

House Bill 3320 was drafted in order to expand the coverage of the Modernization Act by amending provisions of that Act.[328] The bill would strengthen a consumer's privacy protection in several significant respects. In regard to the notices triggered by an institution's sharing information with others, the bill changes the opt-out notice to an opt-in notice, and extends its coverage to affiliates.[329] The Modernization Act provides consumers with protection in regard to disclosure of account number information to nonaffiliated third parties; the bill would extend protection in regard to disclosures to affiliates as well.[330] The bill would apply to nonfinancial products[331] as well as the financial products or services covered by the Modernization Act. Whereas the Modernization Act applies only to the disclosure of financial information,[332] the bill applies both to disclosure of the information and making "unrelated use" of the information.[333] The institution can share information with others if the consumer affirmatively consents, but the bill also explicitly recognizes the consumer's right to withdraw that consent.[334] The institution is prohibited from denying a consumer any financial product or service if the consumer refuses to consent.[335] The exceptions

326. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-112 § 502(e)(2), 113 Stat. 1338 (1999) (to be codified at 15 U.S.C. § 6801).

327. *See* H.R. 313 § 2(a)(2).

328. The title of House Bill 3320 is, "To amend the privacy provisions of the Gramm-Leach-Bliley Act." H.R. 3320, 106th Cong. (1999).

329. *See id.* § 502(b).

330. *See id.* § 502(d). As in the Modernization Act, the bill's restrictions on account numbers applies to prohibiting disclosure when the information is to be used for telemarketing, direct mail marketing, or electronic mail. It adds the new category of "other electronic means." *Id.*

331. *See id.* § 502(b)(2)(B). The Modernization Act applies to financial products or services.

332. The provisions on the disclosure of privacy policy and opt-out apply to nonpublic personal information. *See* Gramm-Leach-Bliley Financial Modernization Act §§ 502(a), 503(a). The Modernization Act defines nonpublic information to mean financial information. *See id.* § 509(4)(a).

333. *See* H.R. 3320 § 502(a).

334. *See id.* § 502(b)(1)(B).

335. *See id.* § 502(b)(3).

under the bill are more limited than under the Modernization Act.[336]

An important gap in the Modernization Act is its failure to provide consumers with access to information and the opportunity to correct inaccuracies in it. The bill grants consumers the right to examine all nonpublic personal information that has been disclosed to any person or entity besides an employee or agent of the institution.[337] Furthermore, the consumer can dispute the accuracy of that information.[338]

In regard to the institution's requirement to notify customers of its privacy practices and policies, the bill would add several important requirements. In addition to disclosing its policies about sharing information with others, the institution also must disclose its policies about how it makes unrelated uses of that information,[339] including who is permitted to make unrelated uses of the information.[340] The institution must inform consumers of their right to examine the institution's nonpublic personal information about them,[341] and its practices and policies regarding the consumer's ability to examine the information and dispute its accuracy.[342] The enforcement agencies are required to design forms for the required notice of an institution's privacy practices and policies.[343] The forms must be designed so that a consumer can compare the practices and policies of one institution to another. Finally, the enforcement agencies are instructed to prescribe rules which will prohibit unfair or deceptive acts or practices in connection with an institution's disclosure of nonpublic personal information and its making unrelated uses of that information.[344]

House Bill 3320 strengthens the privacy protection provisions of the Modernization Act in many significant ways. Nevertheless, privacy advocates may still find it inadequate. First, there is no private right of action, so enforcement is subject to the whims, political considerations, priorities, and resource limitations of the agencies with enforcement authority. Second, like the Modernization Act, only financial institutions are within its

336. For example, there is no exception for private label credit card programs. *See* Gramm-Leach-Bliley Financial Modernization Act § 502(e)(1)(B).

337. *See* H.R. 3320 § 502(c)(1)(A), 106th Congress (1999).

338. *See id.* § 502(c)(1)(B).

339. *See id.* § 503(a)(2).

340. *See id.* § 503(a)(2)(A).

341. *See id.* § 503(a)(5).

342. *See id.* § 503(a)(4).

343. *See id.* § 503(b).

344. *See id.* § 503(a).

scope. Matters of less importance also may cause concern. Although the bill would guarantee consumers access to the institution's nonpublic information about them, unlike House Bill 313,[345] there is no prohibition against the institution charging a fee to discourage consumers from exercising their access rights. The bill permits consumers to dispute the accuracy of an institution's information. This should be expanded to allow the consumer to dispute the completeness of the information as well.[346] Finally, the bill would expand disclosures to include an institution making unrelated uses of personal information, but the bill does not define that term.

This examination of bills in Congress enables one to identify major weaknesses in the Modernization Act's protection of consumers' privacy. The Modernization Act is an important substantive and symbolic step forward. The pending legislation indicates ways in which the law needs to be improved by filling major gaps in the Modernization Act. The bills, however, are deficient in granting rights but providing no remedy for those directly injured by violation of those rights. This should be rectified by adding a private right of action.

CONCLUSION

1999 was a momentous year for privacy protection. Despite the lack of an aggressive response from federal agencies,[347] the actions of the Minnesota Attorney General and Congress resulted in significant legal protection for consumers. Perhaps as important, those actions have encouraged others to act. In the aftermath of the Minnesota case, attorneys general from more than thirty states began to investigate whether banks were violating federal or state law in their information sharing practices.[348] Concerned with the limits in the Modernization Act's protection,

345. *See supra* text accompanying note 328.

346. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681i(a)(1)(A) (1998) (permitting consumer to dispute the "completeness or accuracy of any item of information" in the consumer's file).

347. *See supra* text accompanying notes 134, 148. Agencies have continued to be involved in considering privacy issues since enactment of the Modernization Act. *See FTC, Online Privacy Committee Members Named* (visited Jan 27, 2000) <http://ftc.gov/opa/2000/01/asrev.htm> (FTC named members of a committee to advise the FTC on the costs and benefits of implementing fair information practices of access and security online on January 21, 2000).

348. *See* R. Christian Bruce, *Working Group of Attorneys General Investigating Banks' Privacy Practices*, 68 U.S.L.W. 2199, Oct. 12, 1999. *See also* Michael Gormley, *Bank, Internet Firm Agree to Curbs*, ASSOC. PRESS, Jan. 25, 2000, *available in* 2000 WL 9750970 (reporting that New York's Attorney General reached a settlement with Chase Manhattan in which the bank agreed to stop sharing per-

bills were submitted to Congress[349] and state legislatures[350] to provide greater protection.

In the coming years of this new millennium, we will see how far state legislatures and Congress are willing to go to ensure consumers have adequate privacy protection. The study mandated by the Modernization Act[351] may provide an important impetus for new legislation, or may put a damper on new efforts. If Congress refuses to act, the states may push forward on their own. This may take the form of new legislation or further lawsuits brought by state attorneys general. Consumers may seek to take advantage of these legislative developments to bring lawsuits. As discussed in this article, if legislators are serious about promoting privacy protection, they will enact legislation granting consumers a private right of action so they can enforce their privacy rights. Meanwhile, companies may voluntarily guarantee additional protection in order to bolster consumer confidence and stave off further legislation.

While the above is occurring, there will be new technological developments.[352] Some will improve industry's and consumers' ability to protect privacy.[353] Others will provide opportunities for further invasions of privacy. Electronic commerce will undoubtedly increase, posing new types of invasions through that medium.[354] The Modernization Act will encourage companies to enter into new types of business combinations with significant implications for privacy as affiliates share financial, health, and investment information about their customers. Other combinations not involving financial institutions also pose

---

sonal information with an e-mail marketing company in violation of the bank's privacy policy).

349. *See supra* text accompanying notes 314-47.

350. *See supra* text accompanying note 301.

351. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102 § 508, 113 Stat. 1338 (1999)(to be codified at 15 U.S.C. § 6801).

352. *See, e.g.*, Chris Farnsworth, *Sell Phones Technology: BuyNow.com Will Use the Internet to Turn Cell Phones Into Buying Devices*, ORANGE COUNTY REG., Jan. 25, 2000, at C1(describing a new product in which consumers using Web-enabled cell phones will be able to purchase goods from those phones).

353. The World Wide Web Consortium has developed a *Platform for Privacy Preferences* which enables users to specify their privacy preferences so that their computer knows what sites provide the level of privacy the consumer desires. *See* World Wide Web Consortium, *Platform for Privacy Preferences* (visited Oct. 4, 1999) <http://www.w3.org/P3P>.

354. *See, e.g.*, Mark Clothier, *Software to Let Companies See Who Visits Sites*, ATLANTA J.-CONST., Feb. 2, 2000, at D6 (reporting on a new product allowing companies to track the conduct of consumers who visit their Web sites).

a privacy threat to consumers.[355] These new developments may be accompanied by privacy invasions which are so vast in scope or injurious to those affected that there will be demands for new laws.[356] Overreaction by legislators and government enforcers of the law could impede the flow of information which businesses need in order to efficiently market and sell goods and services. Failure to act could expose consumers to great harm which balanced new legislation and responsible enforcement actions would have prevented. These are the public policy choices which will always confront legislators and enforcement agencies.

Change will continue as technology improves and businesses develop new products and marketing methods.[357] This change will present new opportunities to erode consumer privacy. As long as there is change, there can be no magic legal bullet which will halt this endless cycle which requires constant reevaluation of the need for new legal initiatives. But there are things which can be done to ameliorate the present state of affairs. This article has pointed out the deficiencies in our present laws and the restrictions under which those who enforce those laws must operate. Moreover, the article has suggested how our laws should be improved in the immediate future to provide the necessary level of privacy protection.

---

355. *See generally* Deborah Kong, *E-tail Troubles Cloud Future of Consumer Data*, CHI. TRIB., Jan. 31, 2000, at 10 (quoting Marcelo Halpern, an attorney specializing in e-commerce, as saying, "I think there will eventually be acquisitions that are based on consumer data, where the primary asset that's being bought is the consumer data. . . . Consumer data right now is the currency of e-commerce in a lot of ways."); Steven Levy, *The Two Big Bets*, NEWSWEEK, Jan. 24, 2000, at 38, 42 (reporting that the announced merger of AOL and Time Warner has raised fears about their combined database with information about "everything from your reading habits to your day-trading logs"); .

356. Given the sensitivity of health and medical information, privacy invasions involving those types of data may provide the trigger for a demand for far stronger and more comprehensive laws. *See* Jeri Clausing, *Health Web Sites Fail to Keep Personal Data Private, Study Finds*, N.Y. TIMES, Feb. 2, 2000, at A19 (reporting on a study by the California Health Care Foundation that found that 19 of the 21 surveyed health sites had privacy policies, but most do not follow their policies).

357. Marketing may involve structuring transactions in new ways in which consumers voluntarily surrender their privacy in order to gain a benefit. *See, e.g., Newest Net Gimmick: Cash for Reading E-mail*, ATLANTA J.-CONST., Feb. 2, 2000, at D1 (describing company that pays consumers $30 per month if the consumer surfs for 50 hours each month, provides the company with personal information, and agrees to allow the company to monitor the consumer's surfing).