South Carolina Law Review

Volume 49
Issue 4 *SYMPOSIUM: CONDUCTING BUSINESS OVER THE INTERNET*

Article 7

Summer 1998

Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate

Mark E. Budnitz
Georgia State University College of Law

PRIVACY PROTECTION FOR CONSUMER TRANSACTIONS IN ELECTRONIC COMMERCE: WHY SELF-REGULATION IS INADEQUATE

MARK E. BUDNITZ*

"The future is in electronic commerce" . . . .
All that's holding it up is "this privacy thing."[1]

---

* Professor of Law, Georgia State University College of Law. The author thanks Georgia State for the financial support that made this article possible.

1. Joshua Quittner, *Invasion of Privacy*, TIME, Aug. 25, 1997, at 35 (quoting Ira Magaziner). Magaziner is a senior advisor for domestic policy to President Clinton and is responsible for overseeing administration policy on the Internet. John Mintz, *Firing Clinton Aide: $285,864 Question*, ATLANTA J.-CONST., Dec. 28, 1997, at B1.

I. INTRODUCTION

In 1997, trade associations representing companies marketing electronic commerce[2] services to consumers made a concerted effort to co-opt consideration of statutory privacy protection by voluntarily adopting privacy guidelines. Government agencies approve of the industry's embrace of self-regulation.

This Article evaluates the guidelines and the government's acceptance of industry self-regulation. The Article examines consumers' perceived and actual need for privacy protection and explores whether the government should establish guidelines to satisfy that need. The Article questions the adequacy of the industry's guidelines and self-regulation as a method of dealing with consumers' privacy needs. The Article reviews government reports, studies, and investigations and criticizes the government's response to calls for privacy protection for consumers in electronic commerce. The Article argues that consumers engaged in electronic commerce with the private sector need statutory protection. Without laws granting privacy protection, consumers face the risk of major assaults on their privacy. Moreover, industry needs such laws because without them, large numbers of consumers will refuse to participate in electronic commerce, thereby depriving the industry of the volume it needs to generate profits. Thus, both industry and consumers need statutory privacy protection.

In addition, the Article recommends that the public sector be subject to statutory privacy protection for consumer electronic commerce. Privacy protection should be applied to the public sector because government agencies are increasingly requiring their employees to participate in electronic commerce. Furthermore, the government insists that the public conduct some transactions with it only via electronic commerce.

Finally, the Article proposes a model for privacy legislation. The proposal seeks to provide basic consumer protection through general standards and procedures. However, this legislation does not commit the industry to any particular technological fix, anticipate future technological or product developments, or address every issue. Consequently, even if legislatures enact the proposal, the industry would have additional opportunities for voluntary self-regulation.

II. THE PRIVACY CONCERNS OF CONSUMERS: PERCEPTION AND REALITY

Surveys demonstrate that consumers highly value their privacy. In addition, consumers believe that electronic commerce systems are capable of invading their privacy and that unauthorized persons are able to penetrate these systems to steal

---

2. The term "electronic commerce" as used in this Article includes transactions in which electronic means of communication predominate, as well as access and payment devices. Electronic communication predominates in Internet shopping and electronic fund transfer payment systems such as Internet banking, direct deposit, and pre-authorized bill payment. The access and payment devices include credit cards, debit cards, ATM cards, and stored value cards.

information. This is a significant factor in consumers' resistance to substantial participation in electronic commerce. Moreover, consumers' perceptions about the vulnerability of electronic commerce to privacy invasions have some basis in fact. Electronic commerce remains vulnerable to security breaches and invasions of consumer privacy.

A. Surveys of Consumers' Privacy Concerns

Consumers are concerned about their privacy when engaged in transactions with financial institutions in general and particularly when engaged in electronic commerce. Surveys indicate that 89% of consumers are concerned about threats to their privacy in relation to financial services.[3] Eighty-one percent "believe that 'consumers have lost all control over how personal information about them is circulated and used by companies.'"[4] About 25% of the public want to keep personal information private. These "Privacy Fundamentalists" are not willing to trade information in return for benefits. About 20%, the "Privacy Unconcerned," have no strong interest in safeguarding their privacy, while the remaining 55% or so, known as "Privacy Pragmatists," are willing to trade information, depending upon the benefits they will receive in return, the privacy policy of the company, and whether they trust the company to follow its privacy promises.[5] Consumers are most concerned about medical records and financial information possessed by banks and credit card companies, and trust banks more than credit card companies. The majority prefer self-regulation to new laws "if meaningful voluntary policies are widely adopted and enforced."[6] Other studies document the importance consumers attach to privacy and how consumers' concern about privacy has increased over the years.[7]

In regard to consumer attitudes toward online transactions, a 1997 Harris survey found that the majority of consumers engaging in online activities and Internet transactions are worried about the confidentiality and security of these systems, including their purchases of goods and services.[8] Consumers do not trust online and Internet service companies, and they do not trust the voluntary policies of the companies selling those goods and services. Fifty-six percent of online users and forty-seven percent of Internet users believe government should enact laws

---

3. *Prepared Testimony of Dr. Alan F. Westin, Professor Emeritus of Public Law and Government, Columbia University; Publisher Privacy and American Business Before the House Banking and Financial Services Committee Financial Institutions and Consumer Credit Subcommittee*, Electronic Payment Systems, Electronic Commerce, and Consumer Privacy, Federal News Service, Sept. 18, 1997, *available in* LEXIS, News Library, Federal News Service File.

4. *Id.*(quoting the survey).

5. *Id.*

6. *Id.* On the feasibility of enforcing voluntary self-regulation, see *infra* Part IV.

7. NATIONAL TELECOMM. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION 2 (Oct. 1995).

8. *Westin, supra* note 3.

governing the collection and use of information on the Internet. Consumers want companies to post notices disclosing their collection and use policies on their web sites, and consumers want to be able to opt out of personal information being used for any purpose beyond that needed for the specific transaction.

Consumers in these surveys assert that they will not engage in many transactions in electronic commerce unless privacy rules and practices are strengthened. According to a survey conducted by the Boston Consulting Group, 86% of consumers want to be able to control personal data and 81% believe web sites do not have the right to resell information about them to third parties. Moreover, 70% said that concerns about their privacy were the primary reason they do not register at web sites.[9] Over 70% of consumers are more concerned about giving information over the Internet than over the phone or through the mail, and over 75% are concerned about companies monitoring consumer browsing on Internet sites. Forty-two percent of consumers refuse to provide information on sites requesting that consumers register because of privacy concerns.[10] Even when consumers do provide information, it often is not accurate. Twenty-seven percent provide false information because of privacy concerns.[11] One of the authors of the Boston Consulting Group study commented that consumer willingness to provide information "depends on trust and making it worth their while."[12] That trust is "earned when consumers know and consent to a company's use of their information."[13]

Events outside the context of electronic commerce indicate that consumers are willing to act on their belief in the importance of privacy. In 1990, New York Telephone disclosed in its billing statements that it intended to sell customer telephone listings to third parties. Eight hundred thousand customers told the company to remove their names from the list. Bell Atlantic's 1995 plan to sell its white pages directory met similar massive consumer opposition.[14]

These survey findings are crucially important to the success of electronic commerce. So far, electronic commerce on the Internet has not been profitable.[15] However, the Internet presents a huge potential market. The percentage of American households connected to the Internet has doubled in the past two years; it is now almost twenty percent. The amount of time consumers spend on the

---

9. Drew Clark, *Worries About Privacy Rain on Net Commerce Parade*, AM. BANKER, July 3, 1997, at 14.

10. Joanna Smith Bers, *Secrets for Sale*, FUTUREBANKER, Aug. 1997, at 40.

11. *Id.*

12. *Id.*

13. *Id.*

14. NATIONAL TELECOMM. & INFO. ADMIN., *supra* note 9, at 7.

15. *See* Michael E. Kanell, *Net Providers Busy but Beleaguered*, ATLANTA J.-CONST., Sept. 28, 1997, at G1; Steve Weber, *Picking Winners Is Still an Art, Online Veterans Say*, ONLINE BANKING NEWSLETTER, Dec. 15, 1997, at 1; Thomas E. Weber, *Red Flags from Leading Web-Ad Seller*, WALL ST. J., Dec. 18, 1997, at B1.

Internet has doubled in only one year, to an average of 12.8 hours every week.[16] Despite this promising potential market, if consumers do not trust companies to protect their privacy, the companies will not generate the volume of transactions essential for consumer electronic commerce to be profitable.

One could conclude from this that government regulation is unnecessary because self-interested companies will agree to adequate self-regulation in order to ensure the continuation of their electronic commerce ventures.[17] On the other hand, one could argue that companies should enthusiastically support privacy legislation. If such legislation imposes no more than reasonable requirements on firms and is consistent with what consumers demand to ensure their trust, it can only help companies.[18]

B. Factual Support for Consumer Concerns: The Vulnerability of Systems to Privacy Invasions and Security Breaches

Regardless of consumer concerns, legislation is not justified if it merely calms consumers' irrational fears. Therefore, it is necessary to examine whether any basis exists for consumers' privacy concerns. Consumers' privacy is invaded by "insiders," persons that work for legitimate companies, but gain unauthorized access to the company's information system, as well as "outsiders," interlopers that break into computer systems operated by legitimate companies. Moreover, scam artists invade consumers' privacy by establishing web sites and using fraud to obtain information and money. Finally, legitimate companies invade consumers' privacy by using computer systems to gain marketing information about consumers, often without their knowledge or consent.

One example of an outsider who hacked into a system is Kevin Mitnick. In 1995, Mitnick was arrested after being suspected of breaking into a computer network and stealing, among other things, thousands of credit card account numbers.[19] In 1997, a group of hackers broke into Equifax, one of the major national credit reporting agencies, stealing information from 176 credit reports including credit card numbers.[20] Another hacker stole credit reports from Experian, another national credit reporting agency.[21] In Seattle, a hacker obtained access to a hotel's computerized reservation system and stole the credit card numbers of the hotel's guests.[22] Security defects have appeared at least twice in Netscape

16. Kanell, *supra* note 15, at G1.

17. *See infra* Part IV.

18. *See infra* Part V.

19. *Cyberspace Raider to Get Plea Bargain*, ATLANTA J.-CONST., July 2, 1995, at A5.

20. Jon Jefferson, *Deleting Cybercrooks*, A.B.A. J., Oct. 1997, at 72.

21. Charles Haddad, *A Few Bad Apples Are Making Internet Privacy a Big Issue*, ATLANTA J.-CONST., Sept. 28, 1997, at G5. At the time of the theft, Experian was known as TRW.

22. Jefferson, *supra* note 20, at 72. Persons have gained unauthorized access to America Online and obtained members' credit card numbers, using them to make purchases. Jared Sandberg, *Hackers Find AOL Users Easy Pickings*, ATLANTA J.-CONST., Jan. 6, 1998, at C7.

Navigator, an Internet browser. The defects allowed thieves to collect personal information, including credit card numbers.[23] Scam artists already have adapted to cyberspace by using web sites to engage in various consumer frauds such as fake lottery clubs targeting the elderly[24] and pyramid schemes.[25] Hackers temporarily shut down over 3,000 web sites operated by one of the largest web service providers during the pre-Christmas shopping season.[26] London banks may have paid more than half-a-billion dollars to persons who threatened to use "logic bombs" which would have caused errors affecting the banks' computer systems.[27] The president of the National Association of Securities Dealers has asserted that Internet stock fraud is a major problem, especially because of the "'anonymity of the medium.'"[28] Unchartered and unlicensed companies posing as banks are soliciting deposits, signing up consumers for Visa cards, and promoting off-shore tax shelters.[29]

A favorite device of legitimate companies for obtaining marketing information is the "cookie."

> Cookies collect information as a user travels around the Web and feeds the information back to a Web server. A Web site sends a cookie to the user's computer, where it serves as a digital tag that notifies the site each time the user enters. The information can be used, for example, to automatically supply a password for a subscription-only site or to collect information about an online shopper's preferences so that electronic marketers can target their offerings to that individual.[30]

A 1997 survey of the 100 most frequently visited web sites found that twenty-four used cookies. None of the sites disclosed to the consumer that cookies were being

---

23. *Netscape Flaw*, ATLANTA J.-CONST., Aug. 30, 1997, at E3.

24. *Four Arrested in Lottery Scam*, ATLANTA J.-CONST., Dec. 11, 1997, at B5.

25. *Pyramid Scams Head Web Users' List of Complaints*, ATLANTA J.-CONST., Oct. 10, 1996, at E4. A new scam involves business opportunity schemes whereby 330 web sites offer to train consumers how to charge fees for obtaining government refunds for other consumers. HUD does not authorize third parties to engage in such practices. *HUD to Refund $70 million to Consumers: Refunds Are Fertile Ground for Scam Artists*, CONSUMER FIN. SERVS. L. REP., Dec. 26, 1997, at 2.

26. *A Computer Attack*, ATLANTA J.-CONST., Dec. 17, 1996, at E5.

27. *Warning Shot*, ATLANTA J.-CONST., Oct. 3, 1997, at B2.

28. Rob Chambers, *NASD Promises New Crackdown on Stock Fraud*, ATLANTA J.-CONST., Sept. 26, 1997, at F2 (quoting Mary L. Shapiro).

29. *Phony Banks Multiply on Internet*, FUTUREBANKER, Aug. 1997, at 21. The promoter of some of these banks claims they are sanctioned under the common law, a favorite assertion of "militia-type groups." *Id.*

30. Janet Kornblum, *Browser Users to Watch Cookies* (last modified Mar. 13, 1997) <http://www.news.com/News/Item/0,4,8770,00.html>. *See also* Hanan Sher, *Net Income*, JERUSALEM REP., Aug. 7, 1997, at 37 (explaining that ZapitPro hardware and software registers the time a consumer spends looking at each advertisement on the Internet, and how long the cursor spends on a specific portion of the ad. "It's something like having a salesman watch you sit at the computer screen, recording not only what you say or do but observing involuntary actions as well.")

placed in the consumer's computer system.[31]

Financial institutions are using computer systems to gather more information than ever and using it in new ways, activities which suggest that the nature of these institutions may be undergoing a fundamental change with dire consequences for consumer privacy. The traditional banker lived in a culture that valued the confidentiality of customers' financial information.[32] Now, however, banks are hiring people who specialize in target marketing to efficiently market services through "data mining" and "data warehousing."[33] These terms refer to software systems that produce a rich harvest of information about consumers which allows marketers to concentrate on those who are most likely to buy a product. In addition, this information enables the bank to most effectively appeal to the consumers who are targeted because the systems produce profiles based not only on traditional data such as information from consumer applications and transactions, but also "lifestyle, demographic, and psychographic information—both actual and implied—usually purchased from third-party database sources and then overlaid into the company's customer marketing databases."[34]

All of this is done without the consumer's knowledge or consent. A survey of fifty bank web sites found that thirty allowed consumers to bank online, and thirty-nine requested that consumers provide personal and sensitive information.[35]

---

31. Electronic Privacy Info. Ctr., *Surfer Beware: Personal Privacy and the Internet* (visited Apr. 29, 1998) <http://www.epic.org/reports/surfer-beware.html>.

32. *Westin, supra* note 3. First National Bank of Omaha tried to protect the confidentiality of its customers, but was thwarted by the third party to whom it provided the information. The bank sold the data to Trans Union Corp., a national credit reporting agency. The bank and Trans Union entered into a contract in which Trans Union agreed not to sell the names of the bank's customers to other credit card issuers. The bank's motive was to prevent other issuers from stealing its customers, but it also had the effect of restricting the dissemination of personal information. However, Trans Union mistakenly sold the information to other issuers, and a jury awarded the bank $23 million. Lisa Fickenscher, *Credit Bureau Socked by $23M Verdict for Revealing Bank Customers' Names*, AM. BANKER, Sept. 12, 1997, at 1, 14.

33. *Westin, supra* note 3; *see also* Stuart Elliott, *New in Ad Sales Cyberspace, the Softbank Network Will Cover Topics from Sports to Travel*, N.Y. TIMES, Sept. 15, 1997, at C14 (writing that the Softbank Network allows "advertisers to reach their core audiences across many [web] sites . . . [and also] offers . . . certain targeting capabilities, by day of week, time of day, continent, country, state or operating system").

34. *Westin, supra* note 3. See Drew Clark, *Fleet Puts Muscle into Building a Huge Warehouse*, AM. BANKER, Aug. 20, 1997, at 12, noting that

> The real value of data warehousing in the financial industry, most experts agree, is its capacity for analyzing customer behavior and tailoring marketing strategies appropriately.
>
> . . . . Fleet found that warehousing was essential to dig deeper in understanding and potentially even predicting customers' behavior . . . .
>
> ". . . .Because we are beginning to collect a massive amount of information, we have to be very conscious about how to ensure the privacy of information we collect."

Id. (quoting Randall B. Grossman).

35. *Westin, supra* note 3.

> [N]ot one of the web sites for banks we visited displays a privacy button or a link to a web site privacy notice on its home page . . . . [O]nly three banks we sampled . . . informed consumers of the right to opt out of marketing and third party disclosure lists or said such lists were not utilized by the company.[36]

Some new industry practices have gone awry and others have raised privacy concerns. For example, Experian, one of the major credit reporting agencies, made its credit reports available online in August, 1997, but had to abandon the effort after a technical problem misdirected 2,000 reports.[37] Experian also developed an "anti-spam" product which threatens to encroach upon consumers' privacy. Experian sells this product to Internet service providers, who in turn sell it to persons using the Internet. The service providers can share in the subscription fee paid by the consumer if the service provider encourages its current customers to provide their names and e-mail addresses for listing in Experian's online directory. In addition, new subscribers must be automatically registered in the directory. Although the anti-spam product is touted as reducing unwanted e-mail, privacy advocates charged it would result in more unwanted e-mail that would be generated by the addresses in the directory.[38]

Microsoft and First Data Corporation have developed an electronic bill presentment and payment service. In a pilot project, the service will enable Wells Fargo employees to receive and pay their credit card bills online. Some banks have voiced concerns that the service may pose a threat to consumer privacy because nonbank participants in the system might keep information which should stay within the bank.[39] United Parcel Service requests that customers write their signatures on equipment that captures the signature electronically. As a result, shippers can obtain the customer's signature, and the fear is that the signature could be sold to commercial databases.[40]

A Harvard University study found that gambling disorders have risen more than

---

36. *Id.* A Federal Trade Commission survey of 126 Web sites conducted on October, 14, 1997, found that many Internet sites collect personal information from children. These sites did not request parental consent prior to collecting the information. *FTC Survey Says Most Sites Collect Data on Kids*, ATLANTA J.-CONST., Dec. 16, 1997, at E5.

37. Art Kramer, *"Spam" Slam: Junk E-Mail Plan Raises Suspicion*, ATLANTA J.-CONST., Aug. 29, 1997, at F1.

38. *Id.* "Spam" refers to unsolicited e-mail. In 1997, a group purporting to represent small Internet businesses threatened to make public the e-mail addresses of 5 million persons who subscribe to America Online (AOL) because AOL blocked the businesses from sending unsolicited e-mail advertisements to its subscribers. *Group Threatens AOL Over "Spam" Ban*, ATLANTA J.-CONST., Jan. 1, 1998, at C9. The group later withdrew the threat. *E-Mail Group Withdraws Threat*, ATLANTA J.-CONST., Jan. 6, 1998, at C7.

39. *Wells Fargo, KeyCorp to Pilot Microsoft Billpay Service*, ONLINE BANKING NEWSL., Dec. 15, 1997, at 6.

40. Lauren Weinstein, *Your Signature for Sale?* PRIVACY F. DIG. 1 (last modified Jan. 17, 1997) <http://vortex.com/priv-sig.html>.

50% over the past twenty years and are now at about the same level as drug abuse (this study includes those who gamble in casinos).[41] Meanwhile, Harrah's is marketing a Visa card which gives its gambling customers credit for their purchases. At the same time, the card provides data on customers by recording their gambling and purchasing choices.[42] Casinos also buy information from the data bases developed by others, such as the "Compulsive Gamblers Special."[43] This information allows the casinos to build their own databases and direct their marketing toward those most likely to spend large amounts of money at casinos. Critics have attacked this practice, not only for the alleged invasion of privacy, but also for the socially harmful effects of preying upon compulsive gamblers.[44]

The government also has been involved in activities that invade consumer privacy. In March 1997, the Social Security Administration established a web site seeking to enable persons to obtain their Personal Earnings and Benefit Estimate Statement. After a storm of protest by many who pointed out that it would be easy for persons other than the holder of a Social Security number to gain access to an individual's earning statement, the site was removed from the Internet.[45]

Other government agencies, however, are eagerly using personal, but public, information as a lucrative source of new revenue. Illinois raises $10 million annually from the sale of public records, and Rhode Island takes in almost as much solely from the sale of motor vehicle records.[46] Twenty-four companies, including

---

41. *Study Shows Increase in Gambling Disorders*, ATLANTA J.-CONST., Dec. 5, 1997, at A14.

42. S.C. Gwynne, *How Casinos Hook You*, TIME, Nov. 17, 1997, at 69; *see also* Mike Fish, *Shifting Sands of Legalities*, ATLANTA J.-CONST., Dec. 28, 1997, at E9 (observing that some off-shore companies operating Internet gambling operations in the Caribbean are reportedly run by persons with criminal records who make fraudulent credit card charges); Mike Fish, *U.S. Frets About Potential to Launder Money*, ATLANTA J.-CONST., Dec. 28, 1997, at E8 (noting that "'because a casino provides an array of financial services, they're just as vulnerable to money-laundering activity as a bank would be .... Some of the Internet outfits are specifically encouraging activity drawn against credit cards.'" (quoting Peter Djinis, associate director of the Treasury Department's Financial Crimes Enforcement Network)).

43. Gwynne, *supra* note 42, at 69.

44. *Id.*

45. *The Social Security Administration and Online Privacy* (visited Dec. 11, 1997) <http://www.epic.org/privacy/databases/ssa/>. Several months later, the Social Security Administration put its service back on the Internet with stronger safeguards against unauthorized use. *Social Security Plans to Go Back Online* (CNN Newsnight television broadcast, Sept. 5, 1997), *available in* LEXIS, News Library, CNN File. A private company, Lexis-Nexis, also has run into opposition in regard to the disclosure of Social Security numbers. The company stopped including Social Security numbers in its P-Trak Person Locator Service after it received complaints that release of the number would give subscribers to the Lexis service access to confidential financial information. *On-Line Service Ends Use of Social Security Numbers*, DES MOINES REG., June 14, 1996, at 7.

46. Nina Bernstein, *On Line, High-Tech Sleuths Find Private Facts*, N.Y. TIMES, Sept. 15, 1997, at A20. The Driver's Privacy Protection Act of 1994, 18 U.S.C.A. §§ 2721-25 (West Supp. 1998), prohibits states from disclosing or otherwise making available personal information which the state has obtained in connection with a motor vehicle record. *Id.* § 2721(a). Although the Act became effective on September 13, 1997, *id.* § 2721 historical and statutory notes, *in* Condon v. Reno, 972 F. Supp. 977 (D.S.C. 1997), the Act was held unconstitutional. *Id.*

credit reporting agencies and direct selling marketers, pay the United States Postal Service $80,000 each year in return for the information from change of address cards.[47] In addition to public information sold to legitimate companies, the *New York Times* reported that confidential information also is being sold to private investigators who formerly worked for the government agencies from whom they now seek information.[48]

Employees who sold information from the Social Security Administration and the National Crime Information Computer databases have been prosecuted for unauthorized sale of information.[49] Outsiders gain information illegally over the phone simply by assuming the identity of a person about whom the caller seeks information.[50] First, the government clerk willingly provides the information because the caller can provide data, such as a Social Security number, which leads the clerk to believe the caller is the person he or she pretends to be. The caller has often obtained that Social Security number through his or her access to computer systems.[51] Second, the clerk is willing to provide the information because it is not onerous to do so; if it is in the agency's computer system, it can be retrieved quickly and easily.

Directly related to invasions of privacy is the security of electronic commerce systems. To the extent that these systems lack adequate security, privacy invasions are possible. Outside hackers pose a constant threat to electronic commerce sites. Netsolve, Inc., conducted a study which analyzed 556,464 security alarms from May to September of 1997. The study found that

> every one of its electronic commerce customers suffered at least one serious network attack per month . . .
>
> . . . .
>
> The attacks stem from external sources seeking to gain root access to a site's network. Once they gain that access, they possibly could download customer lists, change files, access new product information, destroy data or transfer funds from the finance system. . . .[52]

---

47. Susan Headden, *The Junk Mail Deluge*, U.S. NEWS & WORLD REP., Dec. 8, 1997, at 42.

48. Bernstein, *supra* note 46, at A20.

49. *Id.*

50. *Id.*

51. Once an interloper has the Social Security number and other easily obtainable public information, the interloper has the ability to gather a great deal of confidential information. For example, Internal Revenue Service auditors made 109 telephone calls to the IRS armed only with a name, address, and Social Security number. In ninety six instances, they were able to obtain confidential information. Ralph Vartabedian & Alan Miller, *IRS Service by Phone Poses Risk to Privacy*, ATLANTA J.-CONST., Nov. 3, 1997, at A8. "'In a few hours, sitting at my computer, beginning with no more than your name and address, I can find out what you do for a living, the names and ages of your spouse and children, what kind of car you drive, the value of your house and how much taxes you pay on it.'" Quittner, *supra* note 1, at 33 (quoting Carole Lane).

52. *E-Commerce Sites Under Heavy Attack from Hackers*, REPORT ON SMART CARDS, Dec. 8, 1997, at 5.

According to Stephen Katz, Chief Information Officer at Citibank, the greatest threat to security is from insiders.[53]

> They have the availability, access, and knowledge to compromise or shut down systems and networks. However, . . . we do not have the mechanisms available to thoroughly and openly check the backgrounds and employment history of current and potential employees.
>
> We don't have anything that even remotely resembles the type of background check used by the government for security clearances. This risk is further exacerbated by the lack of information available about contractors, consultants and outsource vendors.
>
> . . . .
>
> . . . It's extremely difficult to catch someone in the act. Then there is the challenge of tracking and locating the person causing the problem.[54]

Experts in the industry have warned of the risks involved in handling debit and credit cards. One expert warns that banks who market off-line debit cards do not employ adequate safeguards, such as neural networks, to protect themselves from security breaches.[55] Another warned that credit card numbers should not be transmitted over the Internet, even if cryptography is employed, because credit cards are "self-identifying," and cryptography is not a "silver bullet."[56] A vice president of the New York Federal Reserve Bank warned that home banking and electronic commerce pose major threats to banks and bank customers because of the risk of hackers intercepting messages, changing instructions, and inserting viruses.[57]

In addition to the threat to financial institutions from insiders, the President's Commission on Critical Infrastructure Protection took a global perspective, looking at threats to the operation of the entire financial system. The Commission found

---

53. *Stephen Katz: Our State of Security*, ONLINE BANKING NEWSL., Nov. 24, 1997, at 7.

54. *Id.* The President's Commission on Critical Infrastructure Protection stated that it would recommend that the federal government make available to the private sector the government's tools used to check the backgrounds of employees and issue security clearances. *Robert Marsh: Managing Risk in a New Information-Based World*, ONLINE BANKING NEWSL., Nov. 3, 1997, at 7; *see also Report of the President's Commission on Critical Infrastructure Protection*, ONLINE BANKING NEWSL., Nov. 17, 1997, at 6 (observing that "[a]t the institutional level . . . , the most persistent security threat is the insider. . . . [T]he knowledgeable insider dedicated to corruption is difficult to stop."); *see, e.g.*, *Technician Accused of Sabotaging Forbes Inc.*, ATLANTA J.-CONST., Nov. 25, 1997, at D1 (reporting that a temporary computer technician erased data from the internal network of Forbes, Inc. after he was fired). Additionally, viruses pose security threats. For example, a virus shut down the computer system at National City Bank in Cleveland. Michael E. Kanell, *When Computer Disaster Strikes . . .*, ATLANTA J.-CONST., Sept. 18, 1997, at E3.

55. Jeremy Quittner, *Fraud Changing Fast, and Systems Must Too, Experts Say*, AM. BANKER, June 14, 1996, at 12.

56. *Id.*

57. Jaret Seiberg, *To Stem Computer Piracy, New York Fed Begins Major Review of Banks' Precautions*, AM. BANKER, Nov. 8, 1996, at 3.

that:

> The major current threats to the overall operation of the financial system are largely physical in nature, consisting either of natural disasters or a direct coordinated attack on the system's more vulnerable points. These are aggravated by the more open availability on the Internet of the kind of information needed to plan such attacks, increasing reliance on global outsourcing of core operations, and the consolidation of bank and other operations centers as a result of merger and acquisition activity.
>
> . . . .
>
> There is also the evolving threat of a larger scale cyber attack by a sovereign adversary or organized terrorists with the aim of inflicting serious damage on key elements of the US financial system. The current probability of this threat is estimated to be low but growing, and one of its more troubling features is that its source may be undetectable and the attack itself might be masked as a series of lesser intrusions. . . .
>
> Based on the sector profiles developed by the Commission, the nation's core payment systems (FedWire, CHIPS, SWIFT) and the organized securities and commodities exchanges seem to present a serious physical vulnerability within the financial system. This is so not because they have failed to take extensive precautionary measures, but rather because there is substantial cross sector dependence on the services they provide, and few if any alternatives available to provide those services in the event of a disabling catastrophe.[58]

As demonstrated above, privacy concerns are an important factor influencing consumer reluctance to participate in electronic commerce. In addition, a legion of reported privacy invasions, the acknowledgment by industry officials of serious problems, and the findings of government studies, provide abundant evidence that consumers' fears of privacy invasions are justified.

C. Types of Privacy Invasions

As a result of the vulnerability of electronic commerce systems, consumers risk several different types of privacy invasions. One type is often referred to as "identity theft." In this situation, a thief gains access to a consumer's vital information which then allows the thief to impersonate the consumer and purchase goods and services which are billed to the consumer. Additionally, the thief may be able to transfer payments out of the consumer's deposit account.[59] For example, if a thief learns the

---

58. *Report of the President's Commission on Critical Infrastructure Protection,* ONLINE BANKING NEWSL., Nov. 17, 1997, at 5-6.

59. BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD 18 n.14 (Mar. 1997) [hereinafter

credit card number and expiration date of the consumer's card, the thief can shop on the Internet and charge purchases to the consumer's account. With information about a consumer's ATM card and PIN, the thief can withdraw funds from the consumer's account.

In contrast to identity theft, which involves criminal activity, another type of privacy invasion ordinarily involves legal conduct by legitimate electronic commerce businesses which obtain information about the consumer's purchasing and banking habits. For example, many companies with web sites on the Internet request that customers register with the company by providing personal information. Some sites decline to offer their services to those who refuse to register. Consumers who highly value their privacy can simply refuse to register; however, consumers who do register may erroneously believe the information will be used by the company only for purposes related to the instant transaction. In reality, the company may use the information for other purposes and sell it to third parties.[60]

Companies also collect information from consumers surreptitiously. Every time a consumer visits a web site on the Internet, the company operating the site can deposit a cookie, an electronic device that records the consumer's activities on the site.[61] The company can then use this information to target-market the consumer and sell the information to others. Additionally, consumers using electronic payment devices are exposed to invasions of privacy. By using their credit cards, debit cards, and smart cards, consumers may be subject to having their shopping and banking practices tracked, recorded, and sold.[62]

Taking advantage of advances in technology, companies are establishing vast databases on consumers, collecting from sources never used before, and aggregating and manipulating the data in unique ways.[63] Much of this is being done in a manner which is hidden from consumers. Consumers do not know information is collected, how it is used, or to whom it is sold. As a result, consumers' privacy is invaded without their knowledge, consent, or control. In addition to the privacy invasion, if that information is inaccurate or incomplete, consumers may be denied many benefits for which they would qualify if the information were accurate.[64]

FRB REPORT]. The report was sent to Congress on April 2, 1997. *Privacy: Fed Report Outlines Consumer Privacy Issues, Discusses Information Sources and Usage* 68 BANKING REP. (BNA) 639 (Apr. 7, 1997); *see* Gene Tharpe, *Identity Theft Scams Start With Social Security Numbers*, ATLANTA J.-CONST., Nov. 30, 1997, at H7; Ed Mendel, *What Others Know Can Hurt You*, COPLEY NEWS SERVICE, May 15, 1997, at 2, *available in* LEXIS, News Library, Current News File.

60. Professor Westin found that out of the fifty banks he surveyed, only three told consumers they had the right to opt out of marketing and third-party disclosure lists, or informed consumers the bank did not use such lists. *Westin*, *supra* note 3.

61. *See supra* text accompanying notes 30-31.

62. *Westin*, *supra* note 3; Quittner, *supra* note 1, at 32; DONALD I. BAKER & ROLAND E. BRANDEL, THE LAW OF ELECTRONIC FUND TRANSFER SYSTEMS ¶ 19.03 (rev. ed. 1996); PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 45 (1977).

63. *See Public Workshop on Consumer Information Privacy: Hearings Before the Federal Trade Commission* 101-05, 117, 126, 129 (June 10, 1997) [hereinafter *FTC Hearing I*].

64. The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (1994), provides consumers with

III. THE CONSUMER ELECTRONIC COMMERCE INDUSTRY

A. The Private Sector

1. Applicable Laws

Current law does little to protect the privacy of consumers who engage in electronic commerce. The Electronic Fund Transfers Act and Regulation E limit the consumer's maximum financial loss when there is an unauthorized electronic fund transfer involving the consumer's account through use of an access device such as a debit card or ATM card.[65] The Truth in Lending Act and Regulation Z limit the consumer's loss when a credit card is used in an unauthorized fashion.[66] If incorrect information is provided by a company to a consumer credit reporting agency, the 1996 amendments to the Fair Credit Reporting Act make it possible to impose liability on that company under certain circumstances.[67] Federal law provides no specific privacy protection for consumers who use credit cards. For consumers who use debit cards, the law provides only that the financial institution which issues the card must disclose "under what circumstances the financial institution will in the ordinary course of business disclose information concerning the consumer's account to third persons."[68]

2. Government Reports

Various federal government agencies and the Clinton administration recently have released reports, studies, and investigations of consumer privacy. These agencies and the administration acknowledge that serious threats to consumer privacy exist, but recommend that the government take no action. Instead, the federal government has decided to rely upon industry self-regulation. This is in stark contrast to the 1977 report of the Privacy Protection Study Commission. After exhaustively studying the state of affairs in the much less threatening pre-online world,[69] that Commission recommended many specific changes to statutory law to strengthen privacy protection.[70] Furthermore, the laissez-faire approach taken in the

---

certain protections and remedies in regard to inaccurate and incomplete information. The Act, however, applies only to transactions which involve consumer reporting agencies, a narrowly defined category of business. *Id.* § 1681(b); *see id.* § 1681(a)(f).

65. Electronic Fund Transfers Act, 15 U.S.C. §§ 1693-1693r (1994); Regulation E, 12 C.F.R. §§ 205.1-205.15 (1997).

66. Truth in Lending Act, 15 U.S.C. § 1643 (1994); Regulation Z, 12 C.F.R. § 226.12 (1997).

67. 15 U.S.C.A. § 1681s-2 (West Supp. 1998).

68. 15 U.S.C. § 1693c(a)(9) (1994).

69. The pre-online world posed less risk to consumer privacy because the online world enables privacy invaders to obtain far more information and to aggregate and model that information much more easily and inexpensively. *See supra* Part IIB.

70. Privacy Protection Study Commission, *supra* note 62.

recent reports is inconsistent with the approach taken by the European Union, which has issued a directive mandating that countries in the Union ensure privacy by adopting specific legal standards and prohibiting the transfer of personal data to nonmember countries which have not adopted comparable laws.[71]

In 1995, the National Telecommunications and Information Administration (NTIA)[72] issued a report on privacy concerns as they relate to the individual's use of telecommunications and information services such as the Internet. The NTIA identified the fundamental policy issues which must be taken into account when recommending any framework for privacy protection.

> Although privacy is a fundamental personal right that must be adequately protected, it is also true that the level of privacy protection desired varies widely among consumers. Furthermore, the free flow of information—even personal information—promotes a dynamic economic marketplace, which produces substantial benefits for individual consumers and society as a whole.[73]

The report recognized that the individual's control of information is crucial to maintaining privacy.[74] Control over the acquisition, disclosure and use of information is necessary in order to prevent others from being aware of confidential data about an individual such as health information, and to prevent others from using that information "improperly, unfairly, or for purposes other than those intended by an individual."[75] For example, an individual may tell a company his or her Social Security number for identification purposes, only to have it used by that company to obtain access to banking records.[76] The report also points out that as the National Information Infrastructure (NII) is further developed, it will become increasingly easy to store and process information about individuals,[77] and the costs of storing, processing and selling the information will continue to decrease.[78] "These developments presage an information environment in which more personal information will flow more quickly, more widely, more invisibly, and more cheaply with fewer legal and social constraints."[79]

The report dealt only with transactional data information, "information that is created in the course of an individual's subscription to a telecommunications or

---

71. *See infra* text accompanying notes 140-50.

72. "NTIA, a part of the U.S. Department of Commerce, is the Executive Branch agency principally responsible for developing and articulating domestic and international telecommunications and information policies." NATIONAL TELECOMM. & INFO. ADMIN., *supra* note7, at 4 n.18.

73. *Id.* at 24-25.

74. *Id.* at 2-3.

75. *Id.* at 3.

76. *Id.*

77. *Id.*

78. NATIONAL TELECOMM. & INFO. ADMIN., *supra* note 7, at 4.

79. *Id.*

information service or as a result of his or her use of that service."[80] A common example of how transactional data information is created is when a consumer signs up for an Internet service. The report identified three factors which will increase the risk of privacy invasions for consumers in the future.[81] First, increased competition will lead to a greater need for companies to use transactional data information to engage in direct marketing specifically tailored to attract certain segments of consumers. Second, companies will use this information for cross-selling as these companies branch into other lines of business. Third, as competition grows and profit margins shrink, companies will sell this information in order to increase revenue. Although there are several laws which offer limited privacy protection in narrowly defined circumstances, there is no comprehensive privacy law. Thus, consumers do not have adequate protection.[82]

In light of this situation, the report proposed a framework for the acquisition and use of transactional data information. NTIA recommended a "modified contractual model"[83] under which "each provider of telecommunications and information services would inform its customers about what [transactional data information] it intends to collect and how that data will be used."[84] In addition to this notice, the provider would be required to obtain the consent of the consumer before using the information it collected. Additionally, the provider could use the data only for the purposes about which it informed the consumer.[85] As the report notes, the Direct Marketing Association agrees that consumers should be able "to limit or prohibit ancillary or unrelated uses" of consumer information.[86]

Despite that agreement, the debate continues around the issue of whether consumers should be required to opt out. This approach requires the consumer to take affirmative steps, within a timeframe set by the company, in which the consumer notifies the company that information cannot be used for ancillary purposes.[87] In the alternative, companies would be prohibited from using information for ancillary purposes unless the consumer expressly opts in to such use.[88] The NTIA proposed that a distinction be made between sensitive and

---

80. *Id.* at 5. The report did not deal with the privacy of content information, data which constitutes the content of a communication between two parties. *Id.* at 5 n.22.

81. *Id.* at 6-7.

82. *Id.* at 8.

83. *Id.* at 20.

84. NATIONAL TELECOMM. & INFO. ADMIN., *supra* note 7, at 8. The notice would inform the consumer "about how personal information is collected, processed, exchanged, disclosed, and used.... Such notice should be conspicuous and in plain language...." *Id.* at 21. In addition to providing the notice, companies would be required to comply with the terms in the notice. *Id.* at 21 n.85. Furthermore, companies must "take steps to ensure that notice is not merely given but understood," for example, "when a prospective customer's primary language is not English." *Id.* at 22 n.86.

85. *Id.* at 22. The consent could be sent by the consumer electronically, thus obviating the need to mail consent forms. *Id.* at 26.

86. *Id.* at 23.

87. *Id.* at 24.

88. *Id.*

nonsensitive information. Sensitive information could not be used for ancillary purposes unless the consumer opted in.[89] Nonsensitive information could be used unless the consumer opted out.[90] The report does not define "sensitive" or "nonsensitive," but opines that Social Security numbers and health care information should be considered sensitive.[91] Finally, NTIA proposes that a company could never condition its providing services upon the consumer's giving consent.[92]

NTIA recommends that industry adopt the report's proposed framework. It provides two reasons why voluntary self-regulation is in the industry's self-interest. First, consumers will use these services only if they trust the service providers.[93] They will have that trust only if they have the ability to control how information about them is acquired and used. Second, the proposal has the virtue of imposing uniform requirements on all companies. Uniformity would prevent "competitive imbalances among rival firms," so all companies would be able "to compete on privacy as vigorously as they compete on price, service, and quality."[94] If industry refuses to voluntarily adopt the proposed rules, however, NTIA recommends government intervention to impose these rules.[95]

In 1996, Congress instructed the Federal Reserve Board (FRB) to study the following three areas: the availability of sensitive identifying information about consumers, whether sensitive information about consumers could be used to commit financial fraud, and whether there is an undue potential risk of loss to depository institutions as a result.[96] Pursuant to Congress' directive, the Federal Reserve issued a report.[97] As described above, the NTIA report acknowledged that policy decisions could be based upon the distinction between sensitive and nonsensitive information, but avoided defining or providing guidance for what type of data should be in each category.[98] In contrast, the FRB report explores this issue in depth. The FRB noted the different views persons have concerning what is considered sensitive information. Some would include only "Social Security number, mother's maiden name, prior addresses, and date of birth,"[99] while others would include

> place of birth, names of family members, names of schools attended, telephone numbers (listed and unlisted), employment information (past and

89. *Id.* at 25.
90. NATIONAL TELECOMM. & INFO. ADMIN., *supra* note 7, at 25.
91. *Id.* at 25 n.98.
92. *Id.* at 25.
93. *Id.* at 28.
94. *Id.* at 9.
95. *Id.* at 21, 27.
96. Consumer Credit Reporting Reform Act of 1996, Pub. L. No. 104-208, § 2422, 110 Stat. 3009-454 (1996).
97. FRB REPORT, *supra* note 59.
98. NATIONAL TELECOMM. & INFO. ADMIN., *supra* note 7, at 25.
99. *Id.* at 14

present), medical records, voter registration information, passport number, driver's license number, car registration, loan and credit card numbers, other financial account numbers, personal identification numbers (PINs), and insurance policy numbers.[100]

Information which might be considered sensitive in the future includes "retinal scans, encryption keys, and digitized fingerprints."[101] The FRB identified those items of information which appeared to be most crucial to the commission on financial fraud. These included "[a]Social Security number, mother's maiden name, prior addresses, date of birth, employment information (including salary), and credit card, loan, and other financial account numbers."[102] Because Social Security numbers are often used to access information, there was concern over their widespread availability.[103] Once a thief collects additional information, he can trick a creditor into believing he is the consumer, even if the thief does not have all of the information which most credit applications request.

The FRB noted that much of this information can be obtained from government databases or from reference services. "While several federal laws regulate access to certain types of information, there is no comprehensive federal law governing privacy or access to sensitive information. And, there are few restrictions on who can access personal identifying information."[104] The FRB found, however, that "it is not possible to estimate losses solely due to the use of sensitive information."[105]

In contrast to the NTIA report,[106] the FRB declined to make any recommendations. Instead, it merely noted that identity theft appears to be an increasing risk.[107] The FRB then suggested that Congress would have to balance the consumer's interest in privacy against the legitimate information needs of law enforcement and the private sector.[108]

In 1997, the Federal Reserve Bank of New York issued a report on information security practices of financial services institutions in the Second Federal Reserve District.[109] Internet transactions received special attention. The report found that "[m]ost vulernable is the Internet and, potentially, networks connected to it."[110] The report noted that "[h]istorically, attackers internal to the institution have posed the

100. FRB REPORT, *supra* note 61, at 14-15.

101. *Id.* at 15 n.11.

102. *Id.* at 16.

103. *Id.*

104. *Id.* at 16-17.

105. *Id.* at 20.

106. *See supra* text accompanying notes 75-98. The NTIA recommended government intervention if industry did not adopt its recommendations. *See supra* text accompanying note 98.

107. FRB REPORT, *supra* note 59, at 21.

108. *Id.*

109. FEDERAL RESERVE BANK OF N.Y., SOUND PRACTICES GUIDANCE ON INFORMATION SECURITY (1997).

110. *Id.* at 4.

greatest risks."[111] Whether the attack is internal or external, the Internet poses a tremendous risk to the safety and soundness of financial institutions. "The Internet exposes an institution's site to worldwide attack. As more products and services are offered via the Internet, the motivation for attack increases. The greatest risk is . . . to attack the internal network and gain access to an institution's information assets."[112] The report lists the myriad ways in which networks can be attacked, including attacks which compromise the confidentiality of data transmitted over networks.[113] The report points out the necessity of maintaining "a high degree of trust in the banking system," trust which has been undermined by publicity about Internet security concerns.[114] The FRB predicts that if consumer confidence can be established, "the Internet almost certainly will become a major channel for delivering financial services."[115] Consequently, the report recommends sound practices that financial institutions should follow in order to ensure the security and confidentiality of information transmitted via the Internet and other electronic systems. One of the sound practices the Federal Reserve Bank of New York suggests is the segregation of duties among employees.[116] In addition, employees and consultants should be subject to "rigorous screening procedures."[117] The report strongly recommends that financial institutions encrypt sensitive data transmitted across both private and public networks.[118] Finally, the report proposes that sound practices include "strong authentication of the customer" including digital signatures.[119]

Like the FRB's report, the Federal Reserve Bank of New York encourages self-regulation. Despite the vulnerability of the networks, which the report describes in detail, and the disastrous damage which could result from an attack, its recommendations are intended only as guidance, not regulation.[120]

In December 1997, the Board of Governors of the Federal Reserve System issued a notice to officers in charge of supervision and examination personnel at every Federal Reserve Bank and to all domestic and foreign banks supervised by the Federal Reserve. The letter summarized the major recommendations of the New York Federal Reserve Bank. While assuring banks that its findings were intended only as guidance, the letter noted that the Bank report discussed "the types of

---

111. *Id.* at 2. While as much as eighty percent of network attacks come from inside the institution, "the number of external attacks is increasing at a faster rate" than internal attacks. *Id.* at 6.

112. *Id.* at 8.

113. *Id.* at 6-7.

114. *Id.* at 1.

115. FEDERAL RESERVE BANK OF N.Y., *supra* note 109, at 3. "The sound management of risks associated with the delivery of full banking services over the Internet employing effective information security will be critical for maintaining public confidence." *Id.*

116. *Id.* at 13.

117. *Id.* app. A at 16.

118. *Id.* at 2.

119. *Id.* app. B at 15.

120. *Id.* at 3.

prudent and effective measures" that banks have and in the future would adopt "to protect information and ensure its integrity, availability, and confidentiality."[121] Thus, while insisting that member banks are not legally required to follow the Bank's recommendations, the Federal Reserve suggests that member banks comply with the recommendations to avoid possible unfavorable Fed action in the event a bank's systems are compromised.

In October 1996, three United States Senators requested that the Federal Trade Commission (FTC) "investigate the compilation, sale, and usage of electronically transmitted data bases that include identifiable personal information of private citizens without their knowledge."[122] In response, the FTC held several days of hearings in June 1997, known as the Public Workshop on Consumer Privacy.[123] After the hearings, the FTC sent a letter, excerpts of which were published on the Internet, to Senator John McCain and Congressman Thomas Bliley, summarizing the FTC's preliminary findings.[124] The Commission reported that "[c]onsumers are concerned about the security and confidentiality of their personal information in the online environment, and . . . 'they are looking for greater protections, preferably from voluntary efforts by industry, but if necessary from government.'"[125] The FTC found that public education was essential to gain consumers' confidence and that the FTC staff was committed to assisting industry and consumer groups in that educational effort.[126] The Commission voiced the "hope" that by March 1998, "'a substantial majority of commercial Web sites are clearly posting their information practices and privacy policies.'"[127] The FTC acknowledged that self-regulation would be effective only if such regulation was widely adopted, and new technology to protect online privacy would be effective only if "'readily available to consumers and easy to use.'"[128] Nevertheless, the FTC carefully refrained from proposing any mandatory government regulation in the event self-regulation is not widely adopted and the new technology is not available and user-friendly.

---

121. Richard Spillenkothen, *To the Officer in Charge of Supervision and Appropriate Supervision and Examination Personnel at Each Federal Reserve Bank and to Domestic and Foreign Banking Organizations Supervised by the Federal Reserve* (visited Feb. 10, 1998) <http://www.bog.frb.fed.us/boarddocs/SRLETTERS/1997/SR9732.htm>.

122. Senator Bryan et al., *Letter of Oct. 8, 1996, to Chairman Pitofsky* (visited Feb. 10, 1998) <http://www.epic.org/privacy/internet/FTC/ftc-databases.html>.

123. Federal Trade Comm'n, *FTC Outlines Steps for Commission Action on Consumer Privacy Issues in Letter to Congress* (visited Feb. 10, 1998) <http://www.ftc.gov/opa/9707/congpri2.htm>. Transcripts of the hearings were published. *FTC Hearing 1*, *supra* note 63; *Public Workshop on Consumer Information Privacy: Hearings Before the Federal Trade Commission* (July 11, 1997) [hereinafter *FTC Hearing 2*].

124. Federal Trade Comm'n, *supra* note 123. The FTC investigation looked specifically at privacy issues related to children using the Internet in addition to the matters referred to in the text. Those issues are beyond the scope of this article.

125. *Id.* (quoting the Commission's letter to Senator McCain and Representative Bliley).

126. *Id.*

127. *Id.* (quoting the Commission's letter to Senator McCain and Representative Bliley).

128. *Id.*

Several consumer and privacy groups expressed consternation at the FTC's summary of its preliminary findings. In a letter to Senator McCain, they charged that the summary "does not accurately reflect the substance of the hearings or the views of the consumer organizations that participated."[129] The groups disputed the contention that consumers prefer relying on voluntary industry efforts for privacy protection. In fact, several speakers at the Workshop advocated government regulation.[130] The groups also criticized the FTC for not describing the survey results presented at the Workshop in which 58% of computer users said they wanted privacy laws, noted the many threats to personal privacy which have occurred, industry's failure to develop adequate privacy safeguards, and industry's failure to follow those standards which have been adopted.[131]

On July 1, 1997, the Clinton administration released a report which proposed a framework for electronic commerce.[132] Although the report claims that Americans "treasure privacy" and link it to their "concept of personal freedom and well-being," and acknowledges that the global information infrastructure can lessen that privacy, the Clinton administration proposed relying on self-regulation.[133] The administration supported "private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes."[134] These efforts include "mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution."[135] The report cautions, however, that if industry and consumer groups cannot develop "effective privacy protection," the administration would reconsider

---

129. Jeff Chester et al., *Letter of Aug. 1, 1997, to Chairman McCain* (visited Feb. 7, 1998) <http://www.epic.org/privacy/databases/ftc_letter_0797.html>.

130. "'I think there is a need for self-regulation, I even think there is a need for government regulation because there is no customer relationship with many of these companies.'" *FTC Hearing 1*, *supra* note 63, at 91 (quoting Jerry Berman of the Center for Democracy and Technology).

> "[W]e have not yet seen voluntary self-regulation work in the privacy arena. It hasn't happened . . . .
>
> If these safeguards are good, if they're right, if they're going to work, let's back them up with law. Let's get people some remedies. Let's create an enforcement mechanism. Let's create a level playing field; everyone who's in the industry plays by the same rules."

Id. at 286 (quoting Marc Rotenberg of the Electronic Privacy Information Center). "'[I]f you give value to the concept of privacy, then there needs to be a factoring in of that harm as well. And I'm not sure that self-regulation is the best place for that equation to be massaged.'" *Id.* at 311-12 (quoting Shirley Sarna, Assistant Attorney General, New York Department of Law, National Association of Attorneys General). "'I think [basic privacy principles] have to be codified in the law because otherwise we will have who knows how many companies, . . . who are not playing by the same rules as the people here who are trying to construct good rules.'" *Id.* at 333 (quoting Susan Grant, National Consumers League).

131. Chester, *supra* note 129.

132. William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* (visited Apr. 25, 1998) <http://www.whitehouse.gov/WH/New/Commerce/read-plain.html>.

133. *Id.* II.5 (regarding privacy).

134. *Id.*

135. *Id.*

its preference for self-regulation.[136]

The federal government's reliance on self-regulation directly conflicts with a European Union Directive which becomes effective in October 1998.[137] Each member country must make its laws consistent with the Directive by that date. "In Europe, protection of information privacy is viewed as a fundamental, human right."[138] Consistent with that tradition, "the Directive takes a highly regulatory, overarching, and inclusive approach to privacy issues."[139] Strict rules are imposed on the "processing" of information.[140] Generally, consumers' consent must be obtained before information can be processed; they must be told that information is being collected, and informed of how it will be used. It must be used only for the stated and similar purposes. In addition, only the amount of information needed for that purpose may be collected. Sensitive data, including a person's race, ethnicity, health, sex life, and religious or political beliefs, generally may not be processed.[141] Security measures are also required. Every company that processes data must appoint a data controller who is responsible for processing and who must provide the government with specified information.[142] Furthermore, each country must establish an independent government authority to oversee the activities of companies which process personal information.[143]

Finally, the Directive poses a direct challenge to countries such as the United States which have chosen to rely upon self-regulation. Countries belonging to the European Union must enact laws prohibiting the transfer of information to countries which do not ensure an "adequate level of protection."[144] Adequacy is measured in terms of both substantive rules and enforcement mechanisms.[145] It remains to be seen if the United States' reliance on self-regulation will be deemed adequate. A European Community working paper indicates that self-regulation will not be regarded as adequate because it rules out contract-based privacy protection and business codes of conduct.[146] If the United States' self-regulation is not adequate, and if the European Union were therefore to halt transfers, such blockage of data flow "could significantly affect global commerce generally and electronic commerce specifically."[147]

---

136. *Id.*

137. *See* Barbara S. Wellbery, *An Overview of Information Privacy in The United States and European Union*, *in* PRIVACY IN ELECTRONIC COMMERCE 69, 71 (L. Richard Fischer ed., 1997).

138. *Id.*

139. *Id.*

140. Processing "includes any operations involving personal information, except perhaps its mere transmission." *Id.* at 72.

141. *Id.*

142. *Id.* at 73.

143. Wellbery, *supra* note 137, at 73.

144. *Id.*

145. *Id.* at 74.

146. William L. Fishman, *Should the United States Meet European Demands for Greater Protection of Personal Data?*, LEGAL TIMES, Sept. 15, 1997, at 29.

147. Wellbery, *supra* note 137, at 74.

3. *Industry's Self-Regulation Initiatives*

In 1997, major bank trade associations jointly issued uniform privacy principles.[148] Other organizations soon followed by publicly supporting self-regulation.[149] The banks' principles are examined here in detail because the other organizations' pronouncements either mirror the banks' principles or were less specific. The press release announcing the banks' principles stated that they are "designed to assure the American public that its personal privacy rights will be protected when conducting business with commercial banks."[150] Neither the press release nor the attached principles define those rights, or comment on whether they arise from statutes, case law, or contractual relationships.

The associations recognized surveys revealing how highly consumers value their privacy, and how vulnerable they feel about their ability to control industry use of personal information.[151] These surveys showed that consumers' main concern focused on financial records held by banks and brokerage firms; consumers were substantially more concerned about financial records than the unauthorized release of their medical records.[152] One survey found that consumers are far more worried about privacy today than they were five years ago.[153]

The organizations focused on the importance of retaining the customer's trust,[154] and also recognized the connection between "privacy, security and trust in

---

148. *See* Conference Materials, *Banking Industry Unites on Customer Privacy* (Sept. 18, 1997), *in* FINANCIAL SERVICES IN AN ELECTRONIC WORLD (released to press on Nov. 18, 1997) [hereinafter Press Release]. The American Bankers Association, the Consumer Bankers Association, The Bankers Roundtable, and the Independent Bankers Association of America agreed on principles set forth in the Press Release. *Id.* at 1.

149. *See, e.g.*, John Simons, *Credit Companies Agree to Set Limits For On-Line Data* WALL ST. J., Dec. 18, 1997, at B10 (explaining that reference services have agreed to "limit the availability of sensitive consumer information on-line" and to conduct and publicize the results of annual compliance audits); John Markoff, *Guidelines Don't End Debate on Internet Privacy*, N. Y. TIMES, Dec. 18, 1997, at A24 (noting that consumers can opt out of reference services databases in certain cases, but that the guidelines have failed to provide consumers access to personal information about themselves); *Privacy: Technology Trade Group Offers Information Age Privacy Guidelines*, 69 BANKING REP. (BNA) 879 (Dec. 15, 1997) (describing voluntary privacy guidelines issued by the Information Technology Industry Council (ITIC)). For a discussion of the code of conduct adopted by ITIC, see Andrew J. Glass, *Computer Firms Adopt Privacy Safeguards*, ATLANTA J.-CONST., Dec. 9, 1997, at F1. Apple, Compaq, Dell, Eastman Kodak, Hewlett-Packard, IBM, Motorola, NCR, Panasonic, Samsung, Sony and Xerox are some of the computer firms endorsing the new privacy standards. *Id.; see Smart Card Group Issues Guidelines to Protect Consumer Privacy Online*, 68 BANKING REP. (BNA) 890 (May 12, 1997) (adopting voluntary principles similar to those of the bankers' group) [hereinafter *Smart Card Group*].

150. Press Release, *supra* note 148, at 1.

151. *Id.*

152. *Id.* at 2.

153. *Id.*

154. *Id.* at 2-3. "[B]ankers appreciate that their relationship with the customer is dependent in large part upon trust, which bankers understand entails the responsible treatment of personal information." *Id.* at 2.

the context of electronic banking."[155] The adopted principles "focus upon privacy concepts universally recognized both in the U.S. and abroad."[156] The organizations announced their commitment to "self-monitoring and self-regulation."[157]

The concepts incorporated into the principles include recognizing the customer's expectation of privacy, adopting practices which ensure the security and confidentiality of personal information, and informing customers of the bank's principles.[158] The eight principles provide as follows:

(1) Financial institutions should recognize and respect the privacy expectations of their customers and explain financial privacy principles to their customers in an appropriate fashion.[159] The principles do not specifically spell out those expectations. However, the Banking Industry Technology Secretariat (BITS) has promised to conduct research into consumer attitudes concerning privacy, security and trust.[160]

(2) Financial institutions should limit their collection, retention and use of information about individual customers to situations where the information "would be useful (and allowed by law) to administering that organization's business and to provide products, services and other opportunities to its customers."[161] In other words, institutions could use information about its consumer customers to cross-sell other products offered by the firm.

(3) Information should be "accurate, current and complete in accordance with reasonable commercial standards."[162] Financial institutions should establish procedures to ensure that information meets those standards. Presumably, the provisions of the Fair Credit Reporting Act, while not ordinarily applicable,[163] would provide appropriate guidance.[164] In addition, the principles declare that when a customer requests that the institution correct inaccurate information, the bank should respond "in

155. *Id.* at 3.
156. Press Release, *supra* note 148, at 2.
157. *Id.* at 3.
158. *Id.* BITS is a division of the Bankers Roundtable. *Id.* at 1.
159. *Id.* at 2.
160. *Id.* attachment.
161. *Id.*
162. Press Release, *supra* note 148, attachment. The principles do not define reasonable commercial standards. *See* U.C.C. § 3-103(a)(4), (7) (1991) (defining "good faith" and "ordinary care").
163. A financial institution is not subject to the Fair Credit Reporting Act's provisions on procedures to ensure accurate information unless the institution comes within the definition of a "consumer reporting agency," which applies only to companies which regularly engage in the business of assembling or evaluating consumer information in order to sell the information to others. 15 U.S.C. § 1681a(f) (1994).
164. *See, e.g.*, 15 U.S.C. § 1681c (1994) (prohibiting the reporting of obsolete information).

a timely manner."[165]

(4) Institutions should implement internal controls to ensure the confidentiality of customer information.[166] The principles instruct firms to limit access to customer information to those employees who have a business reason for such access,[167] to conduct educational programs for their employees about the importance of preserving customer privacy and confidentiality, and to discipline those who violate the firm's privacy policies.[168]

(5) Institutions are advised to establish security standards and procedures to prevent unauthorized access to customer information.[169]

(6) Institutions should restrict their disclosure of customer information to "unaffiliated third parties for their independent use."[170] Disclosure would be permitted for several purposes such as reporting data to information reporting agencies and assisting in completing a consumer initiated transaction. The most controversial provision would allow disclosure when "the customer has been informed about the possibility of disclosure for marketing or similar purposes through a prior communication and is given the opportunity to decline (i.e., 'opt out')."[171] Privacy and consumer advocates favor instead an opt-in policy, contending that for a variety of reasons opting out unfairly puts the burden on consumers to protect themselves.[172]

(7) Institutions "should insist" that third parties to whom the institution provides personally identifiable customer information adhere to similar privacy principles.[173]

(8) Institutions should inform customers of their privacy policies.[174]

In conjunction with these privacy principles, BITS developed an implementation plan which was approved by The Bankers Roundtable.[175] The plan does little to clarify the ambiguities in the principles, or to provide specific guidance on how banks should convert the principles into operating procedures. The implementation plan provides that the Board of Directors or the Office of the Chair

---

165. Press Release, *supra* note 148, attachment. Compare the requirements of the Fair Credit Reporting Act, which provides far more specificity to ensure the integrity of the correction procedure employed. 15 U.S.C. § 1681i (1994).

166. Press Release, *supra* note 148, attachment.

167. *Id.*

168. *Id.*

169. *Id.*

170. *Id.*

171. *Id.*

172. *See supra* text accompanying notes 87-92.

173. Press Release, *supra* note 148, attachment.

174. *Id.*

175. *Id.* at 3.

of the Board adopt a plan for implementing the privacy principles.[176] The bank's privacy policies should be comunicated to the bank's customers, but "[h]ow that is done should be left to each bank to decide and may include use of existing channels."[177] Presumably, a bank could merely prepare a short description and include it in its monthly statement along with the usual flyers selling radios and socks. The plan recommends that each bank inform and educate its employees about its implementation plan.[178] How this is done is left for each bank to decide. Further, the plan proposes that each bank establish and maintain procedures so that customers can correct inaccurate information.[179] Again, no standards or guidelines are provided.

The plan states the bank should provide customers the opportunity to opt out when it informs them that it may provide information to third parties.[180] This does nothing more than repeat a portion of the sixth privacy principle, discussed previously. The plan includes no recognition of the arguments against opting out raised by privacy and consumer advocates. Consequently, there is no attempt to allay those advocates' concerns by adopting standards or specific guidance for how consumers might be informed or how consumers could exercise their right to opt out. For example, could the bank's notice and the consumer's opt out be oral, or would both have to be in writing? How specific should the bank's notice be to enable consumers to realize the significance of selling information about them to others? Should the notice describe the third parties to whom the information will be sold? Should the notice describe the types of uses to which these third parties could put the information? How much time should consumers be given, at a minimum, to exercise their opt out right?

One significant aspect of the implementation plan is its suggestion of the necessity and value in establishing a "banking industry privacy mark that assures the public that certain safeguards have been met."[181] Of course, even if the industry establishes a program to implement this proposal, it will do little to protect consumer privacy unless the safeguards are meaningful and enforceable.

B. Electronic Commerce in the Public Sector

In addition to consumers' need for privacy protection when dealing with private sector parties, consumers also need privacy protection when they deal with government agencies that increasingly are involved in electronic commerce

176. Conference Materials, *Privacy Principles Implementation Plan,* (Sept. 12, 1997) *in* FINANCIAL SERVICES IN AN ELECTRONIC WORLD (released to press on Nov. 18, 1997) [hereinafter *Implementation Plan*].

177. *Id.*

178. *Id.*

179. *Id.*

180. *Id.*

181. *Id.*

transactions. Government employees, for example, often are required to use credit cards and smart cards when they conduct government business. These smart cards serve as electronic payment devices and also perform other functions. Public employees deserve privacy protection as ever more information about them is loaded onto their smart cards.

Millions of recipients of government benefits receive those benefits via electronic fund transfers, and by 1999, virtually all payments, except refunds made by the Internal Revenue Service, will be made electronically.[182] The Personal Responsibility and Work Opportunity Reconciliation Act of 1996[183] requires states to deliver certain federally funded benefits such as Food Stamps and Temporary Aid to Needy Families (formerly called Aid to Families with Dependent Children) through a system called "electronic benefit transfer."[184] The Omnibus Consolidated Rescissions and Appropriations Act of 1996[185] requires other federal benefits to be made electronically by 1999.[186] States are also taking the initiative in using electronic technology to save money and prevent welfare fraud. Some state statutes require that welfare recipients be identified through biometric systems based on finger imaging technology.[187] This identifying information is stored in centralized data bases.

Several state universities also require students, faculty, and staff to use smart cards.[188] For example, the cards issued by Florida State University contain stored value which can be used in buses, the bookstore, the cafeteria, vending machines, and copying machines.[189] Inserting the card and a password gains one access to student financial information and other confidential records or shared faculty documents.[190]

Employees of several federal government agencies including the General Services Administration (GSA), the Departments of Defense, Treasury, Housing and Urban Development, Interior, State, and Agriculture, use smart cards.[191] For

---

182. *See* 31 U.S.C.A. § 3332(f)(2) (West Supp. 1998).

183. Pub. L. No. 104-193, §§ 825, 891, 110 Stat. 2105, 2324, 2346 (codified as amended at 15 U.S.C.A. § 1693b (West 1998)).

184. 15 U.S.C.A. § 1693b(d)(2)(A) (West 1998).

185. Pub. L. No. 104-134, § 31001, 110 Stat. 1321 (codified as amended at 31 U.S.C.A. § 3332 (West Supp. 1998)).

186. 31 U.S.C.A. § 3332(f)(2) (West Supp. 1998).

187. *See* Conference Materials, David Mintie, *Integrating the Operational Biometric System with Legacy Systems, in The Art of Implementation*, CardTech/SecurTech Government Sept. 15-16, 1997 (explaining Connecticut's current implementation of an electronic client identification system); Conference Materials, Richard M. Nawrot, *Automated Finger Imaging System, in The Art of Implementation*, CardTech/SecurTech Government, Sept. 15-16, 1997 (discussing the New York Department of Social Services' current automated finger imaging system).

188. *See, e.g.*, Scott Berinato, *Smart Cards Move to Head of Class*, PC WEEK, Mar. 24, 1997, at 22 (discussing Florida State University's multiple application smart cards).

189. *Id.*

190. *Id.*

191. *See* Conference Materials, G. Martin Wagner, *Riding Commercial Solutions to a Common*

example, GSA employees use their smart cards to gain access to buildings, and as travel, purchase and fleet cards.[192] Also, soldiers are issued credit cards to use for travel.[193]

When the government disburses public benefits through electronic payment systems, it assumes a role comparable to that of a business actor in a retail consumer transaction. Recipients of those benefits should have basic privacy protection. For example, information about their purchasing and banking activities should not be transferred by the government to others. Barriers should restrict information about these transactions so only government employees with a need to know have access to personal information about recipients. When government employees are required to use credit cards and smart cards, they also should have the protection of internal and external restrictions on the transfer of information about their use of the cards.

IV. THE INADEQUACY OF INDUSTRY SELF-REGULATION

Previous parts of this Article have shown that for retail electronic commerce to succeed, substantial consumer volume is necessary. In order to obtain the necessary volume, consumers must trust that their privacy is protected when engaging in electronic commerce transactions. Consumers currently believe electronic commerce systems are vulnerable to privacy invasions, a perception which is supported by the invasions that often have occurred and the security measures of many electronic systems that have been compromised. Government studies acknowledge some degree of vulnerability, but posit that government intervention in the form of mandatory regulation is currently unnecessary. The preferable course of action, according to the federal government, is to wait and see whether voluntary industry guidelines are effective in protecting consumer privacy.

There are several reasons to doubt the suitability of self-regulation as a substitute for government regulation. First, meaningful regulation requires participation by the entire electronic commerce industry. Unfortunately, the presence of great diversity in this industry makes universal participation unlikely. In fact, in this context, it is probably inaccurate to talk about the electronic commerce industry in the singular, for several industries are involved. The three major trade associations representing the strictly regulated banking industry have adopted voluntary guidelines.[194] Other organizations also have voiced a willingness to adopt privacy guidelines. But electronic commerce also involves others who apparently are not represented by any of the associations issuing guidelines on

---

Card Infrastructure for the Federal Government . . . in an Open Government Framework, in The Art of Implementation, CardTech/SecurTech Government, Sept. 15-16, 1997 (advertising current and future government users and applications).

192. *Id.*

193. Lisa Hoffman, *Traveling Soldiers Face Holiday Credit Card Crackdown*, ATLANTA J.-CONST., Dec. 25, 1997, at A13.

194. *See supra* note 148.

consumer privacy.[195] As FTC Commissioner Varney has pointed out, "[S]elf-regulation tends to capture the good guys that are doing the right thing to begin with."[196] She went on to suggest that perhaps government regulation was necessary because those committing fraudulent acts would not be parties to self-regulation.[197]

Many issuers of payment devices such as prepaid phone cards are one example of companies unrepresented by the groups agreeing to the guidelines. These type of companies are unregulated, and several already have gone out of business after issuing thousands of worthless cards.[198] Credit and debit card companies are also important participants in electronic commerce. Although these companies, including banks, have been in business for many years, they have never before issued voluntary guidelines ensuring consumer privacy.[199] Several companies are developing new types of payment devices, known variously as digital money, electronic money, or cyber cash.[200] Even if such companies agree to self-regulation, nothing assures that new companies entering the field and developing new types of payment devices and services will agree to self-regulation. Many companies engaged in electronic commerce contract with others to operate various components of the system.[201] Companies involved in outsourcing may decide not to be a party to self-regulation.

Given the great diversity of companies, a significant number of companies are unlikely to agree on a uniform set of guidelines. Even among those who agree to the guidelines, some may not in fact comply with them.[202] Over time, some who at first complied may cease to do so while not publicly acknowledging that they are no longer in compliance. Without an independent party to monitor and enforce

---

195. At the time of the FTC privacy hearings, when other associations were announcing privacy guidelines, the Promotional Marketing Association (PMA) representative admitted his group had no current plans to issue guidelines. *FTC Hearing 2*, *supra* note 123, at 134. The PMA includes in its membership "many of the most prominent marketers in the U.S." *Id.* at 135.

196. *Id.* at 158.

197. *Id.* "[T]here are a number of companies and organizations who have no public presence, who don't have a good name to lose, and so those are the folks who in essence are not looking at this as either an ethical or business issue." (statement of Janlori Goldman. *Id.* at 156). Goldman is a Visiting Scholar at Georgetown University Law Center. *Id.* at 148.

198. *See* Mark E. Budnitz, *Stored Value Cards and the Consumer: The Need for Regulation*, 46 AM. U. L. REV. 1027, 1035 & n.54 (1997).

199. *See generally* BAKER & BRANDEL, *supra* note 62, ¶¶ 19.01 - 19.06 (discussing privacy laws and the need to balance the consumer's need for privacy against the industry's need for information free of restrictions).

200. *See generally* PETER WAYNER, DIGITAL CASH: COMMERCE ON THE NET (2d ed. 1997) (describing digital cash types and systems); DANIEL C. LYNCH & LESLIE LUNDQUIST, DIGITAL MONEY: THE NEW ERA OF INTERNET COMMERCE (1996) (describing digital cash types and sytems).

201. *Tech Bytes: Upstate N.Y. Bank Hires M & I for Tech Services*, AM. BANKER, Apr. 29, 1998, at 15.

202. Less than one-third of the members of the Direct Marketing Association have implemented that trade association's guidelines. *FTC Hearing 2*, *supra* note 123, at 99 (statement by Ms. Landesburg). It is primarily the newer, smaller companies that refuse to agree to the trade group's guidelines. *Id.* at 100, 103, 125, 161.

compliance, consumers have no way to judge whether or not a company is actually in compliance with such guidelines. If a statute were to make the guidelines mandatory and provide meaningful remedies, consumers at least would be assured that companies have an incentive to comply.

Voluntary guidelines indicate that the industry may not be willing to agree on privacy safeguards which will adequately protect consumers and provide them with sufficient remedies to cure privacy invasions. Unless voluntary guidelines are embodied in contracts between industry and consumers, they provide no realistic protection. The guidelines, however, do not request that banks incorporate the guidelines in their consumers contracts. Moreover, merely including the guidelines' provisions in contracts is not sufficient because such contractual provisions would inevitably lead to litigation.

Consumers need a statute. Otherwise, parties will endlessly litigate over the contract provision. For Internet transactions, vendors will want to display the contract on their web site, raising a host of questions regarding the adequacy of the display and how the parties would sign these contracts. Furthermore, consumers need a statute that grants government agencies the power to enforce privacy rights violations. FTC Commissioner Mary Azcuenaga has stated that the FTC at present has no authority to enforce trade association guidelines.[203] Moreover, even assuming a contract provision is an adequate method for granting consumer privacy rights, in order for consumers to be able to enforce the contracts, it must be economically feasible for them to obtain adequate relief for breach of the contracts by suing in court; otherwise, the contracts will provide a right, but no meaningful remedy. Enforcing contract rights requires the consumer to hire a lawyer. Because of the high costs of legal representation, the only way to ensure that consumers can enforce a contractual right to privacy is through legislative provisions comparable to those in present consumer protection laws. These statutes include provisions that allow class actions in appropriate cases, attorney's fees if the consumer prevails, actual damages, and encourage enforcement by allowing statutory damages.[204]

Regulatory measures to ensure that consumers can enforce a right to privacy are anathema to the industry which has consistently opposed them. Businesses claim such regulation leads to abusive and frivolous litigation.[205] Case law under the Truth in Lending Act[206] is frequently cited to prove the point.[207] However, it would be far more relevant to look at experience under the Electronic Fund Transfers Act, a statute more closely related to electronic commerce. Very few cases brought under

---

203. *Id.* at 104.

204. *See, e.g.*, Electronic Fund Transfers Act, §§ 915, 2001, 15 U.S.C. § 1693m(a) (1994) (providing a framework for participants in electronic fund transfer systems).

205. *E.g.*, Jeffrey L. Hiday, *Lawsuit Alleges Fleet Defrauded Michigan Clients, Fleet Calls the Suit Frivolous and Points to Its Timing on the Eve of Hearings over Shawmut*, PROVIDENCE J.-Bull., Aug. 26, 1995, at B11 (describing the lawsuit which alleges violations of the Federal Truth in Lending Act, the Housing and Community Development Act of 1987, and RICO).

206. 15 U.S.C.A. §§ 1601-1667e (West 1998).

207. Hiday, *supra* note 205.

the Act by consumers have been reported,[208] which may indicate that the law has worked well.

Doubts about the efficacy of self-regulation also come from the aggressive moves financial institutions are making to ensure that consumers cannot get to court at all. Increasingly, these institutions require consumers to resolve disputes exclusively in arbitration operated by entities of the industry's choosing.[209] Mandatory arbitration is inadequate for several reasons. The arbitration rules of the organizations chosen by the industry often restrict discovery, the types of damages awarded, and class actions.[210] Additionally, the arbitrator is not required to follow the law.

Whereas the private sector at least has recognized the importance of consumer privacy concerns and many businesses, through trade associations, have taken steps to regulate themselves, the public sector has taken no voluntary steps to protect the privacy of government employees who participate in electronic commerce or the public when they engage in electronic commerce with the government.[211] Therefore, legislation is needed to protect consumers engaging in electronic commerce with the government as well.

In summary, consumers cannot rely upon self-regulation to ensure their privacy. They need legislation to guarantee at least a minimal, enforceable privacy right. The voluntary industry guidelines, however, provide much of the basic body of safeguards consumers need to bolster their confidence in electronic commerce. Apparently, the procedures in the guidelines are operationally and financially feasible for industry, or industry would not have proposed them. Embodying them in a statute would require companies to do that which the guidelines assert they should be doing anyway.

V. A MODEL STATUTE

As discussed in Part IV, because of inherent, systemic inadequacies, industry self-regulation cannot adequately protect consumer privacy. Therefore, consumers who purchase goods and services in electronic commerce need statutory protection. Legislation should apply to persons who purchase goods and services from both the private and public sector. Government employees engaged in electronic commerce

---

208. A review of the cases listed in the United States Code Annotated under all sections of the Electronic Fund Transfers Act includes a total of six cases during all of the 1980s, and five cases in the 1990s. 15 U.S.C.A. §§ 1691-1693r. (West Supp. 1998).

209. Industry favors arbitration panels in which the consumer has no right to punitive damages, discovery is limited, class actions are not permitted, and the arbitrator is not required to follow consumer protection and privacy laws designed for the benefit of consumers. *See* Mark E. Budnitz, *Arbitration of Disputes Between Consumers and Financial Institutions: A Serious Threat to Consumer Protection*, 10 OHIO ST. J. ON DISPUTE RESOLUTION 267, 281-98 (1995) (explaining applicable federal and state arbitration law).

210. *Id.* at 281, 336, 339.

211. *See supra* text accompanying notes 182-93.

need legislative protection as well. Electronic commerce occurs in cyberspace, and federal legislation, rather than state legislation, is essential to ensure consumers and businesses uniform and consistent rules.[212] Because of the complexities involved in defining what type of data should be covered and the rapid pace of technological innovations and new product development, the statute should authorize a government agency, such as the Board of Governors of the Federal Reserve System, to promulgate regulations.[213] The statute should contain a description of the law's purpose that makes clear its purpose is to protect consumer privacy, and regulations promulgated pursuant to the statute must promote and effectuate that purpose.

Consumer electronic commerce privacy legislation should contain the following elements: (1) broad coverage; (2) notice to consumers of the kinds of consumer information collected, how it is collected, and from whom it is collected; (3) notice and explanation of a company's policy and practice regarding dissemination of consumer information to others; (4) the right to access information[214] collected by a company,[215] and notice of that right and how the consumer can exercise it; (5) the right to correct inaccurate or incomplete information in the consumer's files, notice of that right, and how the consumer can exercise it; (6) consumer control and choice, including the ability to opt in to permit companies to use, store, and disseminate information, rather than opt out which requires consumers to act affirmatively to prevent use, storage, and dissemination; (7) procedures and structures to prevent unauthorized use of information by employees and service providers; (8) procedures to ensure that information is disseminated only to proper third parties; and (9) a specific grant of authority for government agencies to enforce the statute and effective consumer remedies for violation of their statutory rights. In addition, statutes applicable to electronic signatures and encryption should include provisions to ensure reasonable levels of security regarding authentication and the transmission of information.

For the most part, the privacy requirements of the legislation proposed here are identical to or closely parallel the guidelines and principles proposed by major

---

212. If legislation varied from state to state, endless questions would arise concerning which state's law applied. For example, what law would apply if a consumer who resides in Tennessee used her laptop to conduct a transaction with the Montana office of a Utah-based company, while the consumer was vacationing in California?

213. *See* Quittner, *supra* note 1, at 35 (addressing advocates of a new government consumer privacy agency); *Dangerous Times*, MACLEAN'S, Aug. 22, 1994, at 13 (warning by federal privacy commissioner that with increasing consumer use of electronic commerce, "Canadians could find their behavior monitored and the data used and sold for purposes they never intended").

214. This includes information related to an electronic commerce transaction. For example, it would not include confidential personnel information if the consumer is also an employee of the company or government agency. The statute proposed here is not intended to interfere with the government acting in its law enforcement role. *See, e.g.*, *FTC Hearing 1*, *supra* note 63, at 142-43 (discussing law enforcement exemption from mandatory access).

215. "Company" and "business" as used in Part V include government agencies engaged in electronic commerce.

participants in electronic commerce.[216] Therefore, industry cannot credibly object on the basis that the requirements are onerous, unrealistic, infeasible, prohibitively expensive, or an unwarranted government intrusion. The legislation would not require companies already following industries own guidelines to change the way they conduct business.

As noted below, many firms already adhere to several of the proposed procedures.[217] In light of the industry's very public embrace of the principles and guidelines, many more firms will likely adhere to them in the near future. Actually, the main effect of the enactment of such a statute would be to bring marginal and fringe businesses within the fold who may be the most tempted to engage in serious privacy violations because of a need to gain a competitive advantage. Consequently, although firms may argue that legislation will be burdensome because they do not intend to comply with the industry's voluntary guidelines, recognizing this view in public policy would be unwise. Absent a privacy statute regulating those who refuse to abide by voluntary guidelines, companies that comply with the guidelines would be at a competitive disadvantage.[218]

A. Scope

A model consumer privacy statute should include all types of electronic commerce. Consumers need privacy protection regardless of the specific system. Moreover, excluding certain systems would make it very confusing for consumers. If only certain systems are included, consumers may wrongly assume all systems protect privacy.

The statute should broadly define privacy, as well as the types of information covered. Consumers regard privacy as part of their unique identity, not just a commodity that businesses can use and sell at will.[219] The disturbing escalation of identity theft[220] demonstrates that consumers are correct in their belief that information collected by industry, especially when aggregated and disseminated electronically, constitutes a crucial aspect of each consumer's identity in today's electronic world. Even if one accepts the premise that privacy and information should be broadly defined, drafting definitions is a difficult task. Firms generally agree that certain information, including Social Security numbers, mothers' maiden names, prior addresses, and birth dates should be included in the definition of

---

216. *See supra* text accompanying notes 151-184 (analyzing the Bank trade association privacy principles and plan). The main addition of this model statute consists of the provisions ensuring that consumers can enforce the rights granted in the legislation and granting government agencies the authority to enforce the statute.

217. *See supra* text accompanying notes 148-49.

218. *FTC Hearing 2*, *supra* note 123, at 176-77.

219. Clinton & Gore, *supra* note 132, II.5.

220. *See Report of the President's Commission on Critical Infrastructure Protection*, *supra* note 58.

protected information.[221] However, there is a lack of consensus over whether other information also should be included.[222] One way to approach the definitional issue is for the statute to contain a definition that includes those items about which parties generally agree. The statute would direct a government agency to promulgate regulations including additional items to the list of protected data that are deemed appropriate for inclusion to effectuate the broad remedial objective of the statute after considering comments from industry and the public.

However a model statute defines the information covered, companies' collection, retention, use, and dissemination should be limited to that information needed to administer accounts, provide service, and develop and offer new products. The bank associations' joint principles[223] and the Smart Card Forum include this limitation.[224]

B. Consumer Information

All interests are best served by companies offering electronic commerce products in a competitive environment. Regulation should interfere with the free market only to the extent necessary. But the model statute proposed here, rather than more comprehensive and restrictive legislation, can be justified only if consumers make informed choices. Therefore, legislation must require certain disclosures to ensure that consumers are provided essential information. Consumers need notice explaining what information is being collected about them, from whom it is collected, and how it is collected. For example, consumers using the Internet should have the right to be informed whether cookies[225] are being used when first visiting a site and before divulging any personal information.[226] The consumer should be informed of whether and, if so, how personal information is disseminated to others.

Information should be accessible to consumers. The model statute should require companies that collect, store and disseminate information about consumers to provide notice informing consumers of their right to know what information a company has about them and the procedures available to obtain that information.[227] Consumers also need the right to correct erroneous and incomplete information.[228]

---

221. These issues are explored in FRB REPORT, *supra* note 59.

222. *Id.*

223. Press Release, *supra* note 148, attachment.

224. *See Smart Card Group*, *supra* note 149, at 890.

225. *See supra* text accompanying note 30 (describing "cookie").

226. For example, Netscape's Version 4.0 informs consumers of its cookies and offers consumers the ability to choose among a variety of options including the ability to disable all cookies. *FTC Hearing 2*, *supra* note 123, at 138.

227. Attendees at the FTC Workshop recommended that consumers be permitted to inspect the personal information that sellers collect and maintain. *FTC Hearing 1*, *supra* note 63, at 321.

228. Thomas Kiely, *The Internet: Fear and Shopping in Cyberspace*, HARV. BUS. REV., July-Aug. 1997, at 13.

Consumer access and the opportunity to improve the quality of information helps the industry as well as the consumer, because the industry thrives only if it has accurate and complete information. The bank associations and the Smart Card Forum both support facilitating consumers' ability to correct inaccurate information.[229] Several companies currently disclose their privacy policies,[230] and the bank association's joint principles state that all banks should make this disclosure.[231]

The notices proposed here need not impose significant burdens upon the industry. As with other regulatory schemes, the agency to whom rulemaking powers are delegated can draft model notices that make it simple and inexpensive to comply with the notice requirements.[232] The notices for transactions such as those on the Internet could be provided online. Consequently, companies would not have the expense of mailing written notices.

C. Consumer Control and Choice

Consumers should have the ability to opt in because a choice to opt in gives consumers, in the first instance, greater control over their personal information. Some in the industry favor an opt-out mechanism whereby the industry can collect and disseminate information however it wants unless the consumer takes an affirmative step to inform the company not to engage in those practices.[233] The opt-out approach can be justified if one views consumer privacy as a minor issue and not a right to be zealously protected. Consumers may fail to opt out for a variety of reasons that have little to do with whether they truly want a company to collect and disseminate information about them. For example, they may not understand the nature of the information that will be collected, aggregated, and disseminated; how the company will use the information for its internal purposes; the nature of third parties to whom the data may be distributed; or what those third parties may do with the data. Companies now have "the combination of computing and database power, multiple database sources, and a very low cost distribution and the ability to

---

229. Press Release, *supra* note 148, at 2; *Smart Card Group, supra* note 152, at 890.

230. *See, e.g.*, Time, Inc. maintains the Pathfinder web sites which disclose to consumers their privacy policy. *Pathfinder Privacy Policy* (visited Feb. 11, 1998) <http://www.pathfinder.com/pathfinder/guide/privacy.html> (disclosing presence of cookie and use policies); *About Amazon.com* (visited Feb. 11, 1998) <http://www.amazon.com/exec/obidos/subst/help/first-time-visitors.html> (disclosing its privacy policy with respect to credit card purchases on its welcoming page).

231. Press Release, *supra* note 148, attachment.

232. The Federal Reserve Board has done this pursuant to several consumer protection statutes. *See* Equal Credit Opportunity Act, 15 U.S.C. § 1691 (1994), 12 C.F.R. pt. 202, app. C at 41-48 (1997) (providing sample notification forms). H. Robert Wientzen, President and Chief Executive Officer of the Direct Marketing Association stated at the FTC hearings that his organization believed every Web site selling products should be required to post their privacy policy. *FTC Hearing 2, supra* note 123, at 95. "It costs nothing to use this tool." *Id.*

233. *FTC Hearing 1, supra* note 63, at 253 (explaining DMA's opt-out policy).

distribute information and use it in ways which weren't fully intended."[234] Moreover, the opt-out method is easy for companies to abuse.[235] The opt-in approach is far more consistent with consumer control[236] because it assumes consumers do not want their privacy invaded. Therefore, consumers automatically are protected from invasions. If consumers are willing to give away their privacy or to trade it in return for a benefit they desire, they have the ability to do so.

Also, the model statute should require companies to disclose the use of technology such as cookies and to inform consumers how they can block their use. Software that blocks cookies is available free of charge.[237] As discussed below in Part VI, the electronic commerce industry should voluntarily develop programs which would allow consumers to choose from several alternative levels of privacy protection. The role of the statute would be to ensure that consumers have essential information about a company's data collecting activities and the ability to prevent information from being collected. Industry would be free to encourage consumers to surrender some of their privacy in return for benefits. This surrendering of privacy is not objectionable as long as it is conducted in a manner which is not unfair, deceptive, in bad faith, or unconscionable—standards which are already embedded in law.[238]

D. Restricted Internal and External Access

Regulations should require companies to maintain and follow procedures which restrict the internal access of consumer information to those employees and service providers with a need to know. The bank associations' joint principles include this restriction,[239] and the Smart Card Forum endorses this practice as well.[240] In the smart card environment, a card may have financial information, medical information, or even a student's academic record. Regulations should require that access to each type of data be restricted to appropriate parties. For example, the financial institution that issues the stored value component should not have access

---

234. *Id.* at 78.

235. America Online announced it will sell subscribers' names and addresses with an option for consumers to opt out. Unfortunately, the box which subscribers must check off in order to opt out reportedly is difficult to find. Art Kramer, *AOL Changes Course on Telemarketing Plan*, ATLANTA J.-CONST., July 25, 1997, at D6.

236. "It is Consumer Federation of America's position that consumers should have sovereignty over their personal transaction information, that consumers should be able to control the disclosure of that information used by other parties. You can call that opt-in . . . ." *FTC Hearing 2*, *supra* note 123, at 175 (testimony of Jean Ann Fox, Director of Consumer Protection, Consumer Federation of America).

237. Quittner, *supra* note 1, at 33.

238. *See, e.g.*, The Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (1994) (prohibiting unfair and deceptive acts or practices); U.C.C. §§ 1-102(3), 1-203 (1995) (requiring that parties act in good faith); U.C.C. § 2-302 (1991) (governing unconscionable sales contracts or clauses in contracts).

239. *See supra* text accompanying notes 169-71 (describing those principles).

240. *See Smart Card Group*, *supra* note 149, at 890 (adopting similar principles).

to medical information stored on the card.[241]

Regulations also should require companies to adopt policies and procedures designed to ensure that the third parties to whom information is disseminated use that information for permissible purposes and take measures to safeguard the consumer's privacy. The bank associations' joint principles and the Smart Card Forum recommend this practice.

E. Effective Government and Consumer Remedies

Guaranteeing consumer privacy is ineffectual without enforcement. The statute should provide that violation of the statute shall be deemed a violation of the Federal Trade Commission Act.[242] However, government resources alone cannot provide sufficient enforcement. Therefore, like other consumer protection statutes,[243] the privacy statute should contain a private-attorney-general provision granting consumers the right to sue. If the suit is successful, the statute would entitle claimants to actual damages, minimum statutory damages, attorneys' fees, injunctive relief, and other remedies, enabling consumers to obtain legal representation and relief for any violation of privacy.

F. Security

Regulations should require a minimum level of security in regard to the authentication and transmission of information. Industry and government are presently considering various approaches for authenticating identity in online transactions. Available technology permits the use of electronic signatures, but there are many possible alternatives approaches. For example, a bill introduced by Congressman Baker would establish a national certification authority to license entities who would be the only firms permitted to provide electronic authentication services.[244] In addition, a Standards Review Committee would develop specific standards for authentication and would have the authority to promulgate and enforce its rules.[245] Several states have already adopted digital or electronic signature statutes, and many more are currently considering such legislation.[246]

---

241. *See, e.g.*, Drew Clark, *Insurance Card Firm to Use Gemplus, DEC, MCI*, AM. BANKER, Dec. 17, 1997, at 16 (smart card used by doctor to obtain electronic reimbursement from consumer's insurance company; future applications would enable consumer to use same card to access a line of credit, savings, and checking accounts).

242. *See* Electronic Fund Transfers Act, 15 U.S.C. § 1693o(c) (1994) (providing for FTC enforcement authority).

243. *See id.* § 1693m (providing private civil liability).

244. *Reps. Baker, Dreier Introduce Legislation to Ease Acceptance of Electronic Signatures*, Banking Rep. (BNA) 742 (Nov. 17, 1997).

245. *Id.*

246. *See Summary of Electronic Commerce and Digital Signature Legislation*, Baker & Coles (last modified Jan. 29, 1998) <http://www.mbc.com/ds_sum.html> (listing all legislation and legislative

Security in the transmission of information can be achieved through encryption. The implementation of encryption has been hampered by the government's insistence on key recovery, in which the government would have the ability to engage in electronic surveillance.[247] Meanwhile, industry has been developing encryption standards. The primary movers are Visa and MasterCard, who have won widespread adoption of their Secure Electronic Transaction (SET) protocol.[248] Because electronic signatures and encryption involve a host of issues which go well beyond consumer privacy,[249] this Article does not propose that consumer electronic commerce privacy legislation include provisions on these matters. Statutes that regulate authentication and the security of transmission, however, should include measures to ensure consumer privacy.

VI. SELF-REGULATION OPPORTUNITIES

Even with enactment of the proposed model statute, there will be many opportunities for important self-regulation initiatives to boost consumer confidence. For example, the World Wide Web Consortium[250] has developed a "Platform for Privacy Preferences," which they refer to as "P3."[251] This program is based on the principles of notice, control, and choice. Consumers decide what level of privacy they prefer and set their computer to operate at this preference setting when visiting web sites.[252] For instance, consumers could choose to preserve as much privacy as possible, to allow sites to use information internally, or to permit the site to share personal information with others. Each web site would describe its privacy practices. When the consumer visits a site which requests more information than the consumer's privacy preference would allow, the site can refuse entrance to the consumer, request that the consumer make an exception and accept a lower privacy preference level for access, or waive its information requirements and allow the consumer to visit on the consumer's terms.[253]

Microsoft and Netscape advocate an alternative approach called the "Open

---

proposals). For a detailed account and analysis of various state initiatives, see R.J. Robertson, Jr., *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787 (1998).

247. *Encryption: Government Pursues Encryption Policy with Showcase of Key Recovery Projects*, 69 Banking Rep. (BNA) 748 (Nov. 17, 1997).

248. Jerry Ashworth, *Visa, MasterCard Extend Certificates; Banks Can Continue SET 0.0 Pilots*, REPORT ON SMART CARDS, Nov. 24, 1997, at 7.

249. *See* Jane Kaufman Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 S.C. L. REV. 739 (1998).

250. The World Wide Web Consortium is an international industry organization whose mission is to produce specifications and reference software which is available at no cost. *About the World Wide Web Consortium* (Oct. 3, 1997) (visited Jan. 29, 1998) <http://www.w3c.org/Consortium/>.

251. Joseph Reagle, *P3 Prototype Script* (visited Feb. 11, 1998) <http://www.w3c.org/TALKS/970612-ftc/ftc-mast.html>.

252. *Id.*

253. *Id.*

Profiling Standard."[254] This standard would enable consumers who want to shop on the Internet to establish electronic passports on which they indicate what types of sites they want to visit, but does not include their names.[255] This approach would allow consumers to preserve their privacy and restrict unwanted marketing. Businesses on the Web would have information about consumers' product interests and could use the information to try to make a sale without invading consumers' privacy. The business would not know the identity of the consumers except when they actually purchased a good or service which forces consumers to reveal their identity.

At least a few major enterprises believe electronic commerce can thrive and at the same time protect consumer privacy. For example, when people sign up for America Online and CompuServe, they are asked whether they want to be consumers and let the service supply their names to companies selling products and services on the Internet.[256]

VII. CONCLUSION

Consumer electronic commerce privacy legislation would offer trade associations and individual companies many opportunities to develop creative and innovative approaches to market their products while protecting consumer privacy. This legislation would also allow companies to develop imaginative approaches to providing privacy protection. The objective of the model statute is to permit self-regulation as long as consumers maintain control of their personal information and are informed so they can make reasoned choices. Consumers or government agencies must also be able to enforce these statutory rights.

Electronic commerce will be successful only to the extent of consumer confidence, which is gained only if the systems protect consumers' privacy. Although self-regulation contains inherent limitations which prevent such confidence, legislation such as the model statute here proposed could establish that confidence. Government regulation, therefore, is an important step in promoting electronic commerce. The model statute, moreover, represents sound public policy independent of the financial needs of electronic commerce. As businesses and government agencies increase the amount of personal information contained in vast databases and as technology permits these institutions to develop more sophisticated ways to aggregate and use data, the potential for serious social harm increases enormously. The model statute proposed in this Article attempts to ensure that consumers are accorded meaningful enforceable privacy rights. While industry self-regulation is an inadequate substitute for legislation, it nevertheless can play an important role in developing techniques which promote industry objectives while

254. Quittner, *supra* note 1, at 34; *see also FTC Hearing 2*, *supra* note 123, at 106-16 (discussing the TRUSTe program).

255. Quittner, *supra* note 1, at 35.

256. Kiely, *supra* note 228, at 13.

preserving the privacy guarantees embodied in the model statute.