CONSUMER PRIVACY AND DATA PROTECTION

PROTECTING PERSONAL INFORMATION THROUGH COMMERCIAL BEST PRACTICES

Paula Selis[*]
Anita Ramasastry[**]
Susan Kim[***]
Cameron Smith[****]

Summary: This report presents to businesses, consumers, and government officials a compilation of "best practices" for protecting personal information collected by businesses. The report analyzes the current state of federal and state[1] law, self-regulatory industry practices, and consumer concerns surrounding the use[2] of consumers' personal information. This report offers principles to guide businesses as they develop privacy policies, allowing businesses to prosper along with increasing consumer confidence.

This report presents some of the most successful and practical responses to managing privacy concerns both online and offline. It is designed to be accessible to government officials, businesses, and consumers. This report contains the following parts:

- Part I discusses the emergence of privacy as a consumer issue.
- Part II provides general background information regarding consumer concerns regarding personal privacy, and further discusses how consumer information is gathered and used for business purposes.
- Part III presents current regulatory measures that govern privacy issues and discusses why current disclosure laws are inadequate.
- Part IV presents the "best practices" guidelines offered by the Attorney General of Washington and the Shidler Center for Law and Technology at the University of Washington School of Law.

[*] Senior Counsel, State of Washington Attorney General's Office
[**] Assistant Professor of Law; Associate Director, Shidler Center for Law, Commerce & Technology, University of Washington School of Law
[***] J.D. Candidate, University of Washington School of Law (expected June 2002)
[****] J.D. Candidate, University of Washington School of Law (expected June 2003)

[1] This report is limited to the current state of "Washington State" law.
[2] The term "use" includes, but is not limited to, the actions of, gathering, collecting, selling, sharing, and generally disseminating consumer information.

- Following the conclusion, this report includes, as appendices, a number of model one-page summaries of privacy policies.

The use of personal information by businesses is an issue of local and national concern. National polls indicate that most consumers are concerned about, and opposed to, the unexpected or unintended use of personal information. However, the majority of consumers fail to exercise their rights under federal law, to opt out of having some of their information bought and sold.

Consumers and businesses sometimes have conflicting agendas. On the one hand, businesses want to maximize opportunities to utilize personal information for commercial reasons, including offering goods and services to consumers. On the other hand, consumers generally want to limit the ways their personal information is utilized and want control over that information. By addressing this conflict and examining the growing concerns of businesses and consumers, this report seeks to:

- promote industry self-regulation and
- create appropriate best practices of protection for consumers' personal information.

In the United States there is no comprehensive privacy law that addresses the collection or use of personal information. For the most part, businesses have employed self-regulatory mechanisms to deal with privacy and data protection concerns. The main tools for privacy protection have been the use of disclosures or privacy policies. By disclosing data collection practices to consumers, businesses are providing valuable information. However, disclosures can only be effective if they do their job – by providing useful information and educating consumers through bold and conspicuous disclosure.

The importance of clear and conspicuous disclosure has been highlighted by the recent disclosure practices of the financial services and insurance industries. The Financial Modernization Act of 1999 (the Gramm-Leach-Bliley Act) requires financial institutions to tell consumers what personal information they have collected and what they do with the information. The law provides that consumers be given the ability to "opt out"[3] of having their information shared with third parties. Because of the complexity of the disclosure notices, the disclosure and opting-out effort has not been successful. Only five percent of consumers nationwide who were given a chance to opt out of financial information disclosure took advantage of the opportunity.[4]

---

[3] *See* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6802(b)(1). A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless--

(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 504 [15 USCS § 6804], that such information may be disclosed to such third party;

(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and

(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

[4] Seattle Times, "Legalese May Have Made Privacy Option Unclear," August 27, 2001.

This report concludes that while disclosures and privacy policies are necessary, their prominence and clarity are of equal importance.

Produced by the Washington State Attorney General's Office and the Shidler Center for Law, Commerce and Technology at the University of Washington School of Law, this report provides a set of "best practices" guidelines for protecting personal information. The report also highlights the current state of federal and state law, government recommendations, and self-regulatory practices governing the protection of personal information, and discusses why current regulations are not sufficient, by themselves, to protect and educate consumers. The report aims to increase consumers' understanding of the tools available for their self-protection. The report encourages businesses to voluntarily adopt practices that maximize their success while creating consumer confidence.

I. INTRODUCTION

Many consumers enjoy the benefits of the free flow of personal data. Most of them do not realize the underlying mechanisms that allow it to take place. Time-conscious consumers have come to rely on customized products and services that require high-tech data collection, including obtaining quick access to credit, purchasing or selling stocks quickly, and checking bank and credit account balances easily. The convenience they rely on is largely due to the ease with which businesses can obtain, share, and transfer information. Information movement is easier because of computerized interactions among businesses.

Computerized interactions give businesses the means to build large, sophisticated databases. Such databases can help them to effectively target and expand the market for the products and services they provide.[5] As this information is sold to and shared with others, more Americans are finding that their personal and financial data--like social security and credit card numbers, bank and credit card balances, and buying habits--as well as records of their online browsing activity, are being used in ways they may not have expected. Such information is routinely disclosed to entities consumers do not know and with whom they have no relationship, and sometimes exposed to parties with unauthorized access.

The growth of the Internet has added new dimensions to the distribution of personal information. The Internet has become the fastest growing electronic technology in world history. In the United States, for example, after electricity became publicly available, 46 years passed before 30 percent of American homes were wired; 38 years passed before the telephone reached 30 percent of U.S. households, and 17 years for television. The Internet reached 30 percent of American households in only seven years.[6] Even after five years of explosive growth, new

[5] The $1.7 billion merger between online advertising giant DoubleClick and offline market researcher Abacus Direct illustrates the tremendous value businesses place on consumer information. *See* http://news.cnet.com/news/0-1005-200-1463444.html

Internet enrollment remains high. In the first quarter of 2000, more than five million Americans joined the online world – roughly 55,000 new users each day.[7]

The rapid evolution of the Internet has created both positive and negative consequences. The technological advancements that have made it feasible to obtain easy access to information and commercial goods, have also made it all too realistic for Internet companies to collect, store, transfer, and sell vast amounts of personal data from and about the individuals who visit their web sites. The collection of personal information by companies from web site visitors is a growing concern for the American public.[8]

The collection of data, and in particular the use of this collected information, has raised great public concern and increased anxiety about online privacy. A November 2000 study prepared at UCLA found that two-thirds of American Internet users and three-quarters of non-Internet users fear that going online endangers their privacy.[9] A recent Harris Poll revealed that 94% of Americans are concerned about the possible misuse of personal information by businesses.[10] Twenty-nine percent believe that they have personally been the victims of privacy invasions.[11] The confidence ratings are worse for Internet users. Only 21% stated that they had confidence in information practices of Internet sellers and 61% of Internet users reported they decided not to make a particular purchase because they were not sure how their personal information would be used.[12] Businesses clearly have a vested interest in assuring that privacy issues are addressed through new legislation or self-regulated privacy policies.

As public concern surrounding consumer privacy grows, industry leaders and the federal government have attempted to provide solutions to the problem. Industry leaders have relied mainly on self-regulation. The Internet industry has utilized self-adopted privacy principles and online privacy seal programs as the primary means of self-regulation on the Internet.[13] Seal

---

[6] The UCLA Internet Report "Surveying The Digital Future", UCLA Center for Communication Policy, November 2000. *See* http://www.ccp.ucla.edu/ucla-internet.pdf, at 11.

[7] Id. at 10.

[8] Id. at 32.

[9] Id. at 11. Privacy has emerged as the subject in the UCLA Internet Report that raises the greatest concern about the Internet among both users and non-users. In several questions, respondents express considerable concern that using the Internet creates risks to individual privacy. When asked if "people who go online put their privacy at risk," almost two-thirds (63.6 percent) of Internet users and more than three-quarters (76.1 percent) of non-users either agree or strongly agree.

[10] Harris Poll, January 2000, "The Use and Abuse of Personal Consumer Information." *See* http://www.harrisinteractive.com/harris_poll/index.asp?PID=8

[11] Id.

[12] Id.

[13] *See*, e.g.: http://www.truste.org; http://www.bbbonline; http://www.thedma.org; http://www.networkadvertising.org

programs require their members to implement certain fair information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their websites. As discussed in this report, the federal government has created a number of laws addressing the rights of individuals with respect to the government's use of personal information.[14] However, there are fewer laws governing the use of personal information by private entities.[15]

II. CONSUMER CONCERNS ABOUT PRIVACY

A. Identity Theft

Consumers are often unaware of the reuse and disclosure of personal information they provide to others during daily transactions. In some instances, consumers may be victims of identity theft as a byproduct of the proliferation and free flow of information. Their "identities" may be stolen and used to establish credit and make purchases, leaving the victims accountable for defaults in payments and ruined credit histories.

Identity theft is a real and growing problem. Between 500,000 and 700,000 people in the United States will have their identities stolen this year. The problem costs consumers nearly $1 billion per year.[16] The Federal Trade Commission in an April 1999 report to Congress claimed there were 1,153 investigations of social security number misuse in 1997 compared with only 305 in 1996.[17] The FTC also reported the Trans Union Credit Bureau had 522,922 consumer fraud inquiries in 1997, up from 36,235 in 1992.[18] The American Bankers Association reported that large banks had dollar losses averaging about $20 million per bank in 1996.[19] Individual victims of identity theft spend an average of two or more years attempting to fix their credit report and restore their credit status.[20]

---

[14] *See*, *e.g.*, Census Confidentiality Statute, 13 U.S.C. §9 (census data used for statistical purposes only); Privacy Act of 1994, 5 U.S.C. §552a (limiting collection, use, and dissemination of personal information by federal agencies), Computer Matching and Privacy Act of 1988, 5 U.S.C. §552(o)-(q) (regulating how federal agencies can match personal information against data stored in other agencies' databases).

[15] *See*, *e.g.*, Telecommunications Act of 1996, 47 U.S.C. §§ 151 et seq.; Video Privacy Protection Act of 1988, 18 U.S.C. §§2710-2711; Electronics Communications Privacy Act of 1986, 18 U.S.C. §2511; Cable Communications Privacy Act of 1984, 47 U.S.C. §551; Right to Financial Privacy Act of 1978, 12 U.S.C. §§3401 et seq.; Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801, Fair Credit Reporting Act, 15 U.S.C. §601; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§6501 et seq.

[16] U.S. Gen Accounting Office, Identity Fraud: Information on Prevalence, Cost and Internet is Limited (May 1998). The Secret Service estimates that actual losses to victimized individuals and institutions are $745 million.

[17] *See* www.wa.gov/ago/privacy/Privacy_report.html (Section II, Part D); www.ftc.gov/os/1999/identitythefttestimony.htm.

[18] Id. Note that calls to TransUnion included "precautionary" phone calls as well as reports from fraud victims.

[19] supra, note 17.

[20] Michelle Singletary, Laws are Failing to Keep Pace with Rate of Identity Theft, Sun-Sentinel, May 15, 2000, at 19 (citing California Public Internet Research Group and Privacy Rights Clearinghouse study regarding the victims of identity theft).

Identity theft can be correlated to the loss of privacy. As personal information passes more freely through online and offline sharing, it is more available to those seeking to misuse it. While recent laws, such as Washington's new identity theft provision, Chapter 217, Laws of 2001, seek to protect victims and create increased penalties for violators,[21] the availability of personal information, which can be stolen or misappropriated, has not been limited through legislation. As long as the information is freely available, it may be freely misused.

B. Information Sharing and Telemarketing Fraud

A second example of the possible misuse of information is telemarketing fraud. This costs consumers between $15 billion and $40 billion a year.[22] The free availability of personal information enhances the ability of fraudulent telemarketers to victimize consumers. Using account information obtained from financial institutions to contact customers, unethical telemarketers have made unauthorized charges on the customer's credit card accounts.

The States of Connecticut and Washington recently filed a lawsuit against BrandDirect Marketing which highlighted this practice.[23] BrandDirect obtained account information from some of the nation's biggest banks. It then contacted their customers, offering thirty-day "free trial" memberships in discount buying clubs. It did not disclose that at the end of the thirty days, the customer's credit card would be automatically charged. Nor did it disclose that the customer's financial institution had provided the customer's credit card information to BrandDirect. Were it not for the sharing of the customer's account information, BrandDirect would not have been able to make the unauthorized charges it did.

The states' lawsuit against BrandDirect resulted in a settlement valued at $13 million. Had there been protections against the sharing of the account information itself, the lawsuit would not have been necessary and thousands of victims would not have lost money.

C. Online Data Collection

Consumers are clearly concerned about how their private personally identifiable[24] and financial information are being handled through the Internet medium. They are still shocked to

[21] Chapter 217, Laws of 2001 Washington State Legislature, provides for increased penalties, self-help for victims, credit reporting agency responsibilities, and collection agency limitations, among other provisions.

[22] Patrick Michele, "You May Have Already Won…" Telemarketing Fraud and the Need for a Federal Legislative Solution, 21, PeppL.Rev 553, at 573-74

[23] State of Washington and State of Connecticut v. BrandDirect Marketing, Inc., Docket # 300CV1456, US District Court, the District of Connecticut, filed August 9, 2000.

[24] "Personally Identifiable Information" is defined as any piece of information that relates to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifiable name, number, or to other factors more specific to one's physical, physiological, mental, economic, cultural, or social identity. *See* www.export.gov/safeharbor/sh_workbook.html

learn that information about their activities, ranging from online browsing to grocery shopping, is used for a variety of purposes and made available to other companies without their permission.

According to a recent Gallup Poll, 53% of Internet users are "very concerned" about the privacy of personal information that they give out on the Internet.[25] Moreover, a Federal Trade Commission (FTC) study revealed that 97-99% of web sites sampled collect at least one type of personal information from site visitors.[26] Ninety-two percent of web sites collected personal information such as social security numbers, gender, and age.[27]

In July 1999, Washington State Attorney General Christine Gregoire brought together a diverse group of business, consumer, and legislative leaders to examine the issues regarding consumer privacy. The Workgroup examined consumer privacy issues that arise in commercial business settings. Like elsewhere in the country, it was clear that Washington State consumers were very interested in the issues the Workgroup was asked to study. Since April 1999, when the Attorney General's Office began keeping statistics on privacy-related complaints, the office has received approximately 1000 complaints about privacy violations and identity theft.[28]

D. Levels of Privacy[29]

1. Online Levels of Privacy

There are virtually no online activities or services that guarantee an absolute right of privacy. For sake of analysis, activities engaged in over the Internet can be categorized in three general groups – public activities, private electronic mail services, and limited-access activities. The level of privacy one can expect from an online activity is often governed by the nature of the activity.

a. Public Activities

---

[25] *See* http://www.gallup.com/poll/indicators/indPuter_Net.asp (visited July 30, 2001).

[26] *See* Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace (visited 4-18-01) http://www.ftc.gov/reports/privacy2000pdf [hereinafter Privacy Online 2000].

[27] *See* Federal Trade Commission, Privacy Online 1998: A Report to Congress (visited 4-18-01) http://www.ftc.gov/reports/privacy3/toc.htm [hereinafter Privacy Online 1998].

[28] As of September 30, 2001, the Washington Attorney General's consumer complaint database registered 1,021 complaints. The complaints consisted of: 34.4% for unauthorized charge on credit card, 3% for unauthorized electronic funds transfer from bank account, 3% for problem caused by person with same or similar name, 3% for personal information available from public sources, 24.4% for unauthorized use of name and credit information by a third party, 14.7% for personal information sold/provided to unauthorized third party, 1% personal medical/prescription information provided to third party and 16.9% for other complaints.

[29] This section of the document has been adopted from a Privacy Rights Clearinghouse fact sheet. *See* http://www.privacyrights.org/fs/fs18-cyb.htm (visited 4-18-01).

Engaging and participating in public activities[30] over the Internet does not create an expectation of privacy. In fact, according to federal law, it is not illegal for anyone to view or disclose an electronic communication if the communication is "readily accessible" to the public.[31] For example, if a user posts a message to a public newsgroup or forum or to an online newsletter, that information is readily accessible for public access. Typically, the user's online name, electronic mail address, and information about her service provider are usually available for inspection as part of the message itself.

Given the practices of most Internet Service Providers (ISP's), it is unlikely that one's ISP information will be kept private. Some ISP's have membership directories that may list much more personal information than an individual might wish to share. This depends on how much information is provided by an individual, and the policy of the particular ISP. Most ISP's, however, will allow users to have their information removed from membership directories upon request. In addition to their online directories, service providers may also sell their membership list to direct marketers. Consumers should read their membership agreements to determine their ISP's policies.

b. Private E-mail Services

Virtually all online service providers offer "private" electronic mail services for their subscribers. The Federal Electronic Communications Privacy Act (ECPA) makes it unlawful for anyone to read or disclose the contents of an electronic communication.[32] However, there are important exceptions to the ECPA:

(1) The ISP may view private email if it suspects the sender is attempting to damage the system or harm another user. However, random monitoring of email is prohibited.
(2) The ISP may legally view and disclose private email if either the sender or the recipient of the message consents to the inspection or disclosure. Many commercial ISPs require a consent agreement from new members when signing up for service.
(3) If the employer owns the email system, the employer may inspect the contents of employee email.
(4) Law enforcement officials may access or disclose electronic communication only after receiving a court-ordered search warrant. Only certain officials may apply for this order and a detailed procedure is outlined in the ECPA for granting the order.[33]

[30] Public activities include, but are not limited to, actions such as engaging in chat room discussions and posting messages on ISP bulletin boards.

[31] Electronic Communications Privacy Act, 18 USC § 2511(2)(g)(I).

[32] 18 USC § 2511.

[33] 18 USC §§ 2516-2518. These provisions are relaxed for messages stored in a system for more than 180 days (18 USC § 2703).

(5) If an ISP reasonably believes that an emergency involving immediate danger of death or serious injury to any person requires disclosure of the information without delay, under the U.S. Patriot Act of 2001 (Pub. L. 107-56 (2001) Sec. 2702 (b)(6)(C)), it may disclose the electronic communication containing the information to a law enforcement agency.

c. Members-Only User Groups, Chat Rooms, and Other Limited Access-Activities [34]

Often the presence of security or limited access safeguards on Internet forums can lead users to believe that communications made within these services are private. For example, some bulletin board services maintain forums or chat rooms that are restricted to users who have a password.

While those members who have access may mutually send communication within these borders, there is nothing that prevents those members from retrieving information and data about users. Often, the Internet service provider describes the activities and communications within the "walls" of these forums as private. However, chatline users may capture, store, and transmit these communications to outsiders. Additionally, these activities are subject to the same monitoring provisions governing private e-mail which may not, under all circumstances, be so "private."

2. Levels of Privacy Offline

Privacy in the offline world is regulated only by a number of sector-specific laws described in section **IV B** below. Unlike the online context, the laws are not medium specific.

III. INFORMATION GATHERING PRACTICES

The information revolution, the affiliation of previously unrelated types of businesses, as well as the growth of data mining[35] and target marketing have contributed to a change in data collection. A consumer's personal information has the potential of being bought and sold like any other valuable commodity. It is available from list brokers, look-up or reference businesses, public databases, and credit reporting agencies. It is kept and exchanged by financial institutions, direct marketers, advertisers, and many others.

---

[34] Supra, note 30.

[35] A standard definition for data mining is the non-trivial extraction of implicit, previously unknown, and potentially useful knowledge from data. Another definition is that data mining is a variety of techniques used to identify nuggets of information or decision-making knowledge in bodies of data, and extracting these in such a way that they can be put to use in areas such as decision support, prediction, forecasting, and estimation. *See* http://www.dacs.dtic.mil/databases/url/key.hts?keycode=222

American consumers probably have more choices of products and services offered to them by businesses than consumers anywhere else in the world. They respond actively to those offers, especially when they connect directly with the individual's personal life situation and interests.[36]

Market efficiencies come with a cost: an increased loss of individual privacy. In order to get their marketing messages across, businesses have developed more sophisticated ways to collect and analyze detailed personal and financial information about consumers. Much of the compilation is done without the individual's knowledge. As businesses become more competitive, and seek innovative ways to reach new customers and market to existing ones, an individual's zone of privacy may become increasingly eroded.

A. Offline Information Gathering

There are currently more than one thousand companies compiling comprehensive databases about individual consumers, a ten-fold increase in just five years.[37] Rather than engaging in mass marketing, they focus on gathering as much information as possible about specific people to engage in targeted or "profile" marketing. By compiling layer upon layer of information about specific individuals, they are able to produce a profile based on income, lifestyle, and an enormous variety of other factors.[38]

Using these databases, it is possible to identify people by what many would consider private aspects of their lives, including their medical conditions, their SAT scores, and their ethnicities.[39] Those selected by their personal characteristics can be targeted not only by direct marketers, but also by lawyers, insurance companies, financial institutions, and anyone else who has the funds to pay for the information. It is all available for a fee. For example: an unlisted phone number can be purchased for $49, a Social Security number costs $49, and a bank balance costs $45.[40]

B. Online Information Gathering

1. The Internet

[36] A 1998 Harris poll indicated 63 percent of Americans (representing a base of 124 million adults) say that they purchased in that year products or services from targeted mail offers sent to them at their home or office.

[37] Mike Hatch, Electronic Commerce in the 21st Century: the Privatization of Big Brother: Protecting Sensitive Information from Commercial Interests in the 21st Century, 27 Wm.Mitchell L. Rev. 1457, 1471 (2001) citing Robert O'Harrow Jr., Data Firms Getting Too Personal?, (Wash. Post) March 8, 1998 at A-1.

[38] *Id*. at 1471.

[39] *Id*. at 1471.

[40] *Id*. at 1471, citing Adam Penenberg, The End of Privacy, Forbes, Nov. 29, 1999, at 183. Note that the purchased information is generally not directly available from the source, i.e., the Social Security numbers are not sold directly by the Social Security Administration.

Information technology raises new privacy concerns and may exacerbate existing ones. Information sent over the vast network comprising the Internet may pass through dozens of different computer systems on the way to its final destination. Each of these different computer systems may be managed by a different systems operator, and each system may capture and store online data. Furthermore, the online activities of Internet users can be monitored, both by their own Internet service provider and by the various operators of any sites on the Internet which they visit.[41]

2. Cookies, Clickstream Data, and the Perils of Online Profiling

Many types of online activities do not involve sending email messages between parties or other active communication events. Often, individuals "passively" surf the Internet to retrieve information or documents from web sites. Records of subscribers' browsing patterns, also known as "transaction-generated information," are a potential source of valuable revenue for businesses. This information is useful for its marketing value. In a response to this increased data collection activity, the Federal Trade Commission urges commercial web site operators to spell out their information collection practices in privacy policies posted on web sites.[42]

Most often, information is gathered through the Internet by advertising mechanisms. Internet advertising allows a Web-based business to reach those consumers most likely to be interested in its goods and services. Online profiling allows merchants to target their advertising to those who have shown an interest in their products or services. Consumer interest may be evidenced by prior visits to other web sites of a similar nature. For example, consumers who have recently visited travel web sites, might find themselves viewing customized banner ads on future web sites they visit, even non-travel ones. Online profiling is a unique practice, but is nevertheless a recognizable analog of long-established and accepted offline marketing techniques.

Online profiling is a complex topic involving many definitions. It can refer to the collection of anonymous transactional data that is used to create customized web sites or targeted advertisements. It can also refer to the merger of "clickstream data" with personally identifiable

---

[41] *See,* http://www.techweb.com/encyclopedia/defineterm?term=internet&x=19&y=15, (visited February 1, 2002) Description of "The Original Internet:" In 1995, the Internet was turned over to large commercial Internet provider (ISPs), such as MCI, Sprit, and UUNET, who took responsibility for the backbones to provide lines for their subscribers, and the smaller ISPs hook either directly into the national backbones or into the regional ISPs. Internet computers use the TCP/IP communications protocol. There are more than 20 million hosts on the Internet, a host being a mainframe of medium to high-end server that is always online via TCP/IP. The Internet is also connected to non-TCP/IP networks worldwide through gateways that convert TCP/IP into other protocols. Although most new users interact with the Internet via their Web browsers, for years, command-line UNIX utilities were used. For example, an FTP (File Transfer Protocol) program allows files to be downloaded, and the Archie utility provides listing of these files. Telnet is a terminal emulation program that lets you log onto a computer in the Internet and run a program. Gopher provides hierarchical menus describing Internet files (not just file names), and Veronica lets you make more sophisticated searches on Gopher sites.

[42] Supra, note 26.

information. It has contributed to the expansion of Internet advertising, which has been the key to funding the explosive growth in Web content available to consumers without charge.[43]

The online marketing methods of network advertisers have given rise to concerns about user privacy. The intervention of a third party, in the form of a network advertising company that delivers a targeted banner advertisement to the consumer, introduces an uninvited guest to the consumer's Internet experience. In general, these companies do not merely supply banner ads; they also gather data about the consumers who view their ads. The information gathered by network advertisers is often anonymous (i.e., preference profiles are linked only to the identification number of the advertising network's cookie[44] on the consumer's computer browser rather than the name or e-mail address of a specific person).

Information about how a consumer uses the Web, including the sites visited, may be collected by web sites themselves, or may be collected by advertising networks or marketing companies. This data is often referred to as clickstream data. Data collected can include a user's computer's Internet protocol address ("IP"), the type of browser used, a user's activities during his or her last visit to a web site, and activities conducted on other web sites. Clickstream data, which may or may not be enough to identify a specific individual, can be collected at various points during a user's online activity. It is available for potential reuse and disclosure in multiple ways. For example, America Online records customers' travels through its proprietary content and uses the information in the aggregate (without personally identifiable information) to refine the system and court advertisers.[45] An individual's clickstream is stored in huge databases that allow websites (or DoubleClick, on behalf of the 1,500 sites on which it places ads) to sort web habits into categories, such as potential car buyer, DVD-player owner and so on.[46]

When a user goes online, the type of information that may be collected includes: site visits, search terms, online purchases, and "click through" responses to advertisements. The web site operator or a third party such as an advertising company may place a "tag" referred to as a

---

[43] *See* http://networkadvertising.org/aboutopm_advertising.asp. The U.S. Census Bureau estimates that retail e-commerce sales for the first quarter of 2001 were $6.99 billion dollars, an increase of 33.5% from the first quarter of 2000. *See* http://www.census.gov/mrts/www/current.html (visited July 30, 2001). It is estimated that world wide net commerce will reach $6.8 trillion dollars by the year 2004. *See* http://www.forrester.com/ER/Press/ForrFind/0,1768,0,00.html (visited July 30, 2001). A February 2000 Gallup Poll reveals that Americans use the Internet for various reasons; 95% to obtain information, 89% to send or receive email, 45% for shopping, and 21% to visit chat rooms. According to the same poll, among all Internet users, 48% say they have purchased products or information on the Internet, which represents about a fourth of all adults in the country. *See* http://www.gallup.com/poll.releases/pr000223.asp (visited July 30, 2001).

[44] According to Netscape, cookies are a "general mechanism which server side connections can use to both store and retrieve information on the client side of the connection." This means that cookies are small data files written to your hard drive by some Web sites when you view them in your browser. These data files contain information the site can use to track such things as passwords, lists of pages you've visited, and the date when you last looked at a certain page. Cookies can store database information, custom page settings, or just about anything that would make a site individual and customized.

[45] *See* http://www.kiplinger.com/magazine/archives/2000/August/managing/e-privacy2.htm

[46] Id.

cookie on a consumer's computer. This identifier can then be used to track a user's movements on the web.

Cookies are one means by which companies can collect consumer information. Cookies are unique, small text files that web sites "write" (i.e., place) on a user's hard drive. Cookies enable web sites to capture data about users' online activities. They contain information such as login information (including passwords) and online "shopping cart" information. Data stored in a cookie can range from an anonymous profile (created by assigning a random number to a user that can be matched to a profile during repeat visits) and codes, which link the cookie to a specific identifiable customer within a web site's database.

When a consumer visits a web site, a cookie may be placed on their computer. The cookie will allow the web site to determine whether a user is a repeat visitor and can customize the experience for the visitor. The cookie can also be used to then record and store clickstream data from the users session and then store the information in a manner that links it to an individual cookie. If a user repeatedly visits a site, the cookie is then used to call up preferences and data relating to the user.

In addition to merchant cookies, advertising companies which provide banner advertisements on multiple web sites may also place cookies on a user's computer. Therefore, if a user visits a travel site, the advertising company which provides the banner advertisements for the site may also place a cookie on the user's computer. This so called "third party" cookie will then record the user's interest in travel. The next time the user logs on and visits a new site - say a news site, he or she may see a banner ad for vacations or for an airline - this is because the advertising company's cookies will be recognized and a customized banner ad will pop up on a new and unrelated site. Thus, online profiling through third party cookies can occur across web sites.

The information gathered through cookies, by itself, poses minimal privacy risks. However, significant privacy concerns surround the practice of using profiles derived from cookies and merging them with personally identifiable information.[47] Clickstream data can also be combined with data on the consumer's offline purchases, or information collected directly from consumers through surveys and registration forms.[48]

The merging of anonymous clickstream data with personally identifiable information has created consumer concerns. In November 1999, DoubleClick, the largest network advertiser,

---

[47] *See*, http://networkadvertising.org/apoutpm_howopmworks.asp The result is a profile that attempts to predict the individual consumer's tastes, needs, and purchasing habits and enables the advertising companies' computers to make split-second decisions about how to deliver ads directly targeted to the consumer's specific interests.

[48] Id.

acquired database marketer Abacus Direct and with it gained capacity to link its own data with Abacus' list of names and purchase histories of 88 million households that bought from major retail stores and mail-order catalogs. The announcement unleashed protests by privacy advocates and triggered investigations by the Federal Trade Commission and by several state attorneys general.[49]

In response, the company announced it would launch a "privacy initiative," including outside audits of its practices and increased consumer outreach. Then, in March 2000, DoubleClick said it would suspend any plan to link anonymous data gathered online with individual consumers' names until government and industry agreed to a set of common privacy standards.

IV. REGULATORY MEASURES

A. Constitutional Right to Privacy?

The United States Constitution does not explicitly guarantee a comprehensive right to privacy. However, the U.S. Supreme Court has held that the Constitution protects individuals from unwarranted governmental intrusions when making certain intimate or personal decisions.[50] Many individuals assume that these protections extend to all aspects of their daily lives, but in fact, they are only applicable when government agents invade the individual's privacy.

Civil remedies for infringements on an individual's right to privacy are limited to the tort doctrines of false light, appropriation, private facts, and intrusion.[51] Consequently, although the general public may have a reasonable expectation of privacy regarding personal information, constitutional privacy protections and tort laws do not protect them from being subjected to the collection and use of their personal information by private businesses. Previously, consumer gave consent to information sharing by filling out forms, for example, credit card applications. Congress has responded in some instances, however, and has enacted privacy measures for particular industries and practices.[52]

B. Current Government Privacy Regulations

[49] "Big Browser is Watching You," Consumer Reports, May 2000.

[50] *See Paul v. Davis*, 424 U.S. 693, 713 (1976); *Einstadt v. Baird*, 405 U.S. 438 (1972); *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[51] Restatement (Second) of Torts §§ 652B-E (1977).

[52] Congress has enacted privacy regulatory measures for the following: government (Privacy Act of 1974, 5 USC § 552a(1994); the cable industry (Cable Communications Policy Act of 1984, 47 U.S.C. §551); video rental industry (Video Privacy Protection Act of 1988, 18 U.S.C. §§2710-2711 (1988)); banking and finance (Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1978)); Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801, Fair Credit Reporting Act, 15 U.S.C. §601; electronic Communications (Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §2511; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §6501.

The United States does not have a comprehensive privacy statute that governs the collection and use of personally identifiable information, either online or through traditional business practices. There are, however, a number of sector-specific laws that govern the collection and use of data.

1. COPPA

Currently, no federal statutes require the placement of privacy policies on Internet web sites other than the Children's Privacy Protection Act of 1998 (COPPA). COPPA is applicable only to web sites collecting information from children who are younger than 13 years old.[53] The law became effective on April 1, 2000.

The Act requires Internet operators, including ISPs and web site operators, to:

(1) Provide parents with conspicuous notice of what information is collected, how the information will be used, and the website's disclosure practices;
(2) Obtain prior, verifiable parental consent for the collection, use and disclosure of personal information from children (there are limited exceptions);
(3) Provide parents the opportunity to view and prevent the further use of personal information that has been collected on the website;
(4) Limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for that activity; and
(5) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information that is collected.

COPPA also provides a safe harbor if an operator of a web site complies with a self-regulatory set of guidelines that have been approved by the FTC.[54]

2. Gramm-Leach-Bliley Financial Modernization Act (GLBA)

The GLBA was signed into law on November 12, 1999 by President Clinton. Title V of the GLBA governs the collection, use, and dissemination of non-public consumer financial information by financial institutions.[55]

Gramm-Leach-Bliley requires financial institutions to:

---

[53] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506. Note, also that under certain limited circumstances, the GLBA requires privacy policies to be posted online. *See*, ft. 55

[54] *See* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm and http://www.coppa.org/ftc_how_to.htm.

[55] *See* 12 CFR § 40.18 and Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801.

(1) Provide clear and conspicuous notice to consumers of their privacy policy upon establishing the customer relationship and at least annually thereafter;
(2) Give consumers the opportunity to "opt out" of having their non-public personal information disclosed to nonaffiliated third parties; and
(3) Provide a reasonable method for consumers to "opt out" of such disclosures to nonaffiliated third parties.

The GLBA addresses privacy concerns with the financial institutions' use of consumers' personal information both offline and online.

a. Opting Out Under the GLBA

The GLBA nominally gives consumers the ability to opt-out of having their personal information disclosed by giving them notice of their right to do so. In practice, however, the GLBA opt-out provision has failed. Financial institutions that complied with the statute's disclosure requirements found that only five percent nationwide responded to the privacy "opt-out" notices.

This lack of response has largely been ascribed to the "legalese" and fine-print jargon in the notices which made them essentially unreadable. According to an August 2001 *Seattle Times* article, most of the notices "read like pages from a law book."[56] Confusing language used in the notices, including terms like "non-public personal information" and "non-affiliated third parties," made them too dense to sift through for most consumers. Even though the new law was designed to protect consumers' privacy rights, the manner in which those rights were disclosed effectively made them non-existent.

Responding to confusing opt-out notices, the consumer group Public Citizen petitioned the U.S. Federal Trade Commission (FTC) to force financial institutions to give consumers more explicit notice of their right to keep personal information from being shared with third parties.[57] The petition asked the FTC to require financial institutions to send new notices alerting consumers of their opt-out right in the first paragraph of the notice, using boldface type and plain English.[58] The petition also requested that the opt-out notice include a detachable, post card-size, self-addressed form that consumers could simply clip from the form and send in.[59]

---

[56] Supra, note 4.

[57] *See* http://www.newsbytes.com/news/01/167141.html

[58] Id.

[59] Id.

Additionally, the proposal would require companies to include a telephone number that consumers could call at any time to exercise their opt-out rights.[60]

Due to complaints from consumer groups such as Public Citizen, the FTC held a public workshop on GLBA privacy notices on December 4, 2001.[61] The eight federal agencies that issued regulations implementing the Act's privacy provisions heard testimony from financial institutions, consumer and privacy groups, experts on readability and consumer communication, government officials, industry associations, and others. The issues were discussed through moderated panel discussions,[62] and included such topics as identifying successful GLBA privacy notices, discussing strategies for communicating complex information, and encouraging industry self-regulatory efforts and consumer and business education.[63] Additionally, the workshop provided financial institutions with guidance about the form and content of their notices from federal agencies charged with implementing and enforcing the GLBA.[64]

3. Other Statutes, Regulations, and Directives Containing Provisions Protecting Privacy of Consumer Information Include:

a. Cable Communications Policy Act of 1984 (47 USC §521 et seq., §611)

This Act addresses concerns about the ability of interactive cable systems to track cable consumer viewing or buying habits. It prohibits the collection of personally identifiable information without the consumer's prior consent except as needed to render service provided by the operator or to prevent interception.

b. Communications Assistance for Law Enforcement Act of 1994 (47 USC §§1001-1-10; §1021; 18 USC §2522)

This Act establishes protection for cordless telephone conversations and establishes a warrant requirement for government access to e-mail addresses.

c. Driver Privacy Protection Act of 1994, and as amended in 1999 (18 USC §§2721-2725)

---

[60] Id.

[61] *See* http://www.ftc.gov/opa/2001/09/glbwkshop.htm

[62] Id.

[63] Id.

[64] *See* http://www.ftc.gov/bcp/workshops/glb/

This law protects state motor vehicle records and restricts their dissemination to only authorized parties and in many instances only for specified purposes. The 1999 amendments tie state compliance to the appropriation of federal transportation funds for states.

d. Electronic Communications Privacy Act of 1986 (18 USC §1367, § 2232, §2510 et seq., §2701 et seq., §3117, §3121 et seq.)

This Act protects all forms of electronic transmissions, including video, text, audio and data from unauthorized interception.

e. Electronic Fund Transfer Act (15 USC § 1693)

The Act requires financial institutions to include in an initial account disclosure the circumstances under which it will disclose information to third parties.

f. Fair Credit Reporting Act (15 USC §1681 et seq.)

This Act regulates the disclosure of personal information by consumer credit reporting services. It requires such services to adopt reasonable procedures to ensure the accuracy of personal information contained in their credit reports. It also provides a process for consumers to review and correct inaccurate information on a credit report. Credit report information can be shared with affiliates when a consumer is told the information may be shared and is given the opportunity to opt out from information sharing with affiliates.

The FCRA does not restrict the amount or type of information to be released to third party inquirers when the reporting agency has reason to believe it will be used for credit, employment or insurance evaluations or other "legitimate business needs" affecting the individual consumer. It prohibits those who are no credit reporting agencies from disseminating or redistributing credit information. The law does not explicitly address the sharing of transactional, empirical information. This silence has been interpreted by the Office of the Comptroller to mean that the information can be shared freely with third parties.

g. Family Education Rights and Privacy Act of 1974 (20 USC §1232g)

This Act protects the accuracy and confidentiality of student records.

h. Federal Trade Commission Act (15 USC §41 et seq.)

This Act, which creates the Federal Trade Commission ("FTC") establishes among other things consumer fair business practices and gives the FTC jurisdiction and authority to address unfair, deceptive or misleading business practices.[65]

[65] *See* http://www.ftc.gov/ogc/brfovrvw.htm

i. Federal Privacy Act (5 USC §552a)

This Act establishes a code of fair information practices applying to government record keeping and allows individuals to discover, correct and control dissemination of sensitive personal information in the government's possession. This Act also limits circulation of identifiable personal information and prohibits government from selling or renting an individual's name and address unless specifically authorized to do so by law.

j. Identity Thefts and Assumption Deterrence Act of 1998 (Pub L. 105-318, Oct. 30, 1998, 112 Stat. 3007)

This law enacts no new sections of law but amends existing laws. It criminalizes fraud in connection with unlawful theft and misuse of personal identifying information itself, regardless of whether it appears or is used in documents. Previously, only the fraudulent creation, use, or transfer of identification documents was illegal, not theft and misuse of personal identifying information itself. The criminal provisions are enforced by the U.S. Department of Justice. In response to the Act, the Federal Trade Commission has established a toll free number for identity theft calls (1-877- ID THEFT), an online complaint form at ***www.consumer.gov/idtheft***, and a centralized clearinghouse of identity theft complaints that is accessible to law enforcement officers throughout the country. The Commission has also published and distributed more than 100,000 copies of a consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*.[66]

k. Privacy Protection Act of 1980 (42 USC §2000aa et seq.)

This Act guards against law enforcement searches and seizures, without a warrant, of materials intended for publication, extending as some commentators believe, to materials intended for publication on online systems or bulletin boards.

l. Right to Financial Privacy Act of 1978 (12 USC §3401 et seq.)

This Act protects against disclosure to government of personal financial records held by banks, except with a search warrant.

m. Telephone Consumer Protection Act of 1991 (47 USC §227, §331)

This Act provided the basis for the FCC rule requiring persons engaged in telemarketing to maintain a list of consumers who request not to be called. It also prohibits junk faxes[67] and automatic dialing and announcing devices.

---

[66] Available online at http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

[67] The transmission of unsolicited faxed advertisements. *See* http://www.junkfaxes.org/

n. Video Privacy Protection Act of 1988 (18 USC §2710, §2711)

This Act prohibits disclosure of video customer rental records. Customer names and addresses can be disclosed for direct marketing purposes unless the customer prohibits this use.

o. Privacy of Consumer Financial and Health Information, Chapter 284-04 WAC

This rule, promulgated by the Washington State Insurance Commissioner, governs the treatment of non-public personal health information and non-public personal financial information by all insurance companies licensed to sell insurance in Washington.

p. The European Union Directive

The European Union Directive, adopted by the European Union in October 1998, is a comprehensive privacy law that permits the transfer of data with non-E.U. nations that provide an "adequate" level of security protection.[68] The directive makes no distinction between online and offline collection and transfer of data. Due to the fact that the United States and the European Union take a different approach to privacy, the E.U. and the U.S. Department of Commerce developed a safe harbor framework to bridge the differing privacy approaches and to provide a streamlined means for U.S. businesses to comply with the Directive.

The safe harbor is an important way for U.S. businesses to avoid experiencing interruptions in their business dealings with the E.U. or facing prosecution by European authorities under European privacy laws. The decision by U.S. business to enter the safe harbor is entirely voluntary. Businesses that decide to participate in the safe harbor must comply with the safe harbor's requirements and publicly declare their intentions to do so.

To qualify for the safe harbor, an organization can (1) join a self-regulatory privacy program that adheres to the safe harbor's requirements[69]; or (2) develop its own self-regulatory privacy policy that conforms to the safe harbor. To enjoy safe harbor benefits, an organization needs to self-certify annually to the Department of Commerce that it satisfies safe harbor requirements such as notice[70], choice[71], access[72], and enforcement[73]. It must also publish a

---

[68] *See* http://www.export.gov/safeharbor/sh_overview.html (visited July 30, 2001).

[69] *See, e.g.*, BBB*Online* and TRUSTe.

[70] **Notice:** Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

[71] **Choice:** Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

privacy policy stating that it adheres to the safe harbor principles. The Department of Commerce maintains a list of all organizations that file self-certification letters and makes both the list and the self-certification letters publicly available at www.export.gov/safeharbor.

In general, enforcement of the safe harbor will take place in the United States in accordance with U.S. law and will be carried out primarily by the private sector.[74] Private sector self-regulation and enforcement is backed up by government enforcement of federal and state unfair and deceptive trade practices statutes. For example, under the Federal Trade Commission Act, a company's failure to abide by commitments to implement the safe harbor principles might be considered deceptive and actionable by the Federal Trade Commission. This is true even where an organization adhering to the safe harbor relies entirely on self-regulation to provide the enforcement required by the safe harbor enforcement principle. The FTC has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to $12,000 per day.[75]

C. The Federal Trade Commission

The Federal Trade Commission (FTC) has played an active and prominent role in offline and online privacy issues. Traditionally, the FTC had taken the position that self-regulation by industry would be the most effective way to manage the privacy of personal data on the Internet. To encourage self-regulation, in its June 4, 1998 Report,[76] the FTC established four "fair information practice principles" that should be followed by businesses.

These principles are not new, or limited to the online world. They were first articulated in 1973 when the U.S. Department of Health, Education, and Welfare released its seminal report on privacy protections in the age of data collection, "Records, Computers and the Rights of Citizens."

---

[72] **Access:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

[73] **Enforcement:** In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles.

[74] *See* http://www.export.gov/safeharbor/sh_overview.html

[75] Id.

[76] Supra, note 27.

In addition to the HEW report, these principles have been set forth in the U.S. Privacy Protection Study Commission's report, "Personal Privacy in an Information Society,"[77] and the Organization for Economic Cooperation and Development's "OECD Guidelines on the Protection of Privacy."[78] Further, these concepts are promulgated in the Safe Harbor Principles of the U.S. Department of Commerce, which were issued as a response to the European Union's Directive on Data Protection.[79] The FTC's "fair information practices principles" are as follows:

(1) Notice/Awareness: Consumers should be informed of a web site's privacy policy.

(2) Choice/Consent: Consumers should be given a choice as to how a web site can use the information it collects.

(3) Access/Participation: Consumers should be given an opportunity to view and correct the information a web site collects about them.

(4) Integrity/Security: Personal data should be kept reasonably secure and updated.

In 2000, the FTC changed its views and advocated government intervention. In May of 2000, the FTC issued its report entitled, "Privacy Online: Fair Information Practices in the Electronic Marketplace."[80] In this report the FTC abandoned its prior emphasis on self-regulation as the primary approach to protecting online privacy and concluded that legislation is necessary to ensure implementation of fair information practices online. The FTC encouraged new legislation that would require web sites to "take reasonable steps to protect the security of the information that they collect from consumers, and added a fifth fair information practice principle--the need for methods of enforcement and remedies."[81]

On October 4, 2001, Chairman Timothy J. Muris presented a detailed FTC enforcement plan, developed over the prior four months through meetings with agency, consumer, industry, and trade association officials.[82] The plan involves "every division of the Bureau of Consumer Protection and increases the resources devoted to privacy issues substantially."[83] As the nation's leading consumer protection agency, the Commission's new Privacy Agenda will contain the following major law enforcement and education initiatives:

---

[77] *See* http://www.cdt.org/privacy/guide/basic/ppc.html

[78] *See* http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_60.31.pdf (Appendix A).

[79] *See* http://www.export.gov/safeharbor/sh_overview.html

[80] Supra, note 26.

[81] Supra, note 26.

[82] *See* http://www.ftc.gov/opa/2001/10/privacy.htm

[83] *See* http://www.ftc.gov/speeches/muris/privisp1002.htm

- Creating a National Telemarketing Do-Not-Call List;
- Beefing Up Enforcement Against Deceptive Spam;
- Helping Victims of Identity Theft;
- Putting a Stop to Pretexting;[84]
- Encouraging Accuracy in Credit Reporting and Compliance with the Fair Credit Reporting Act (FCRA);
- Enforcing Privacy Promises;
- Increasing Enforcement and Outreach on Children's Online Privacy;
- Tracking Consumers' Privacy Complaints;
- Enforcing the Telemarketing Sales Rule;
- Restricting the Use of Pre-acquired Account Information;
- Enforcing the Gramm-Leach-Bliley Act (GLB); and
- Holding Privacy-related Commission Workshops.[85]

The new Privacy Agenda appears to retreat from the FTC's prior endorsement of government intervention. Regarding possible legislation concerning both Internet and off-line privacy, the Chairman said that while there are "clearly good arguments for such legislation," such as the establishment of a clear set of rules about how personal information is collected and used, "it is too soon to conclude that we can fashion workable legislation to accomplish these goals."[86] Citing the recent GLB privacy notices, he added, "we should at least digest this experience" before moving forward.[87]

D. Current Self-Regulatory Initiatives

1. Online Initiatives

---

[84] "Pretexting" is the practice of fraudulently obtaining personal financial information, like account numbers and balances, often by calling banks under the pretext of being a customer.

[85] *See* http://www.ftc.gov/opa/2001/10/privacyagenda.htm for further information about these topics.

[86] *See* http://www.ftc.gov/speeches/muris/privisp1002.htm

[87] Id.

Several online business organizations have responded to the FTC's core principles of Choice, Access, Security, and Enforcement and have implemented programs that encourage Internet businesses to comply with the core principles and hold themselves accountable for failure to do so.

a. Network Advertising Initiative (NAI)

The Network Advertising Initiative is a group of leading Internet Advertising entities[88] that have banded together to offer a framework for self-regulation of "online preference marketing" (OPM) or "profiling."[89] (See Section III.B.2 above).

Online profiling can involve the use of non-personally identifiable information or a combination of personally identifiable information and non-personally identifiable information. The NAI Principles were developed to provide consumers with a clear explanation of the types of data they collect, how they use it, as well as the ability of consumers to opt out if they choose not to participate.

The NAI has worked with the Federal Trade Commission and the U.S. Department of Commerce to develop a self-regulatory regime governing NAI companies and the practice of online profiling. These self-regulatory principles detail the specific protections to be afforded to consumers when online profiling involves personally identifiable information or anonymous non-personally identifiable information.[90] The NAI's foremost commitment is to provide consumers with clear explanations of Internet advertising practices and how they affect the consumer and the Internet.

*b. Better Business Bureau Online (***BBB***Online)*

BBB*OnLine* is a wholly-owned subsidiary of the Council of Better Business Bureaus. Its mission is to promote trust and confidence on the Internet through the BBB*OnLine* Reliability and BBB*OnLine* Privacy programs.[91] The BBB*Online* Privacy Seal program helps web users identify companies that stand behind their privacy policies and have met the program

---

[88] NAI members include: Avenue A, DoubleClick, Engage, Inc., L90, MatchLogic, Inc., and 24/7 Media.

[89] *See* http://www.networkadvertising.org/aboutnai_nai.asp (visited July 30, 2001).

[90] *See* http://www.networkadvertising.org/aboutopm_glossary.asp. Definitions: **Personally Identifiable Information (PII) –** PII is data used to identify, contact, or locate a person, including name, address, telephone number, or E-mail address. **Non-Personally Identifiable Information (Non-PII) –** Non-PII (anonymous) used for OPM by network advertisers is not linked to a particular person and is typically compiled from click stream information compiled as a browser moves across different Web sites (or a single Web site) serviced by a particular network advertiser or from information provided by third parties (so long as that information is not personally identifiable to the network advertiser) (visited July 30, 2001).

[91] *See* http://www.bbbonline.org/ (visited July 30, 2001).

requirements of notice, choice, access, and security in the use of personally identifiable information. It is another method for Internet businesses to demonstrate compliance with credible online privacy principles.

The BBB*OnLine* Privacy Program offers a Privacy Dispute Resolution program for consumers with online privacy complaints against BBB*OnLine* Privacy Program participants and non-program participants.[92] The BBB*Online* Privacy Program Dispute Resolution Process provides for a review of an eligible complaint by the Privacy Policy Review Service (PPRS) of BBB*Online*, Inc.[93] Additionally, where the complaint is against a company or individual that is a participant in the BBB*Online* Privacy Program there may be an opportunity for a PPRS decision to be appealed to the Privacy Review Appeals Board.[94]

c. TRUSTe

TRUSTe is a self-regulatory seal program participant, similar to the BBB*Online* organization. It is an independent, non-profit privacy initiative dedicated to building users' trust and confidence on the Internet and accelerating growth of the Internet industry.[95]

According to its web site, the TRUSTe program embodies principles that comply with fair information practices approved by the government and prominent industry-represented organizations.[96] The TRUSTe principles include the following provisions: (1) adopting and implementing a privacy policy; (2) posting notice and disclosure of collection and use practices regarding personally identifiable information; (3) offering users choice and consent over how their personal information is used and shared; and (4) implementing data security and access measures. Moreover, TRUSTe will monitor a licensee's web site to ensure compliance with its privacy principles.

2. Offline Initiatives

a. The Direct Marketing Association

The Direct Marketing Association (The DMA) is the oldest and largest trade association for users and suppliers in the direct, database and interactive marketing field. The DMA has

---

[92] *See* http://www.bbbonline.org/privacy/dr.asp

[93] *See* http://www.bbbonline.org/privacy/dr.pdf

[94] Id.

[95] *See* http://www.truste.org/about/truste/index/html (visited July 30, 2001).

[96] Id.

more than 4,700 member organizations, commercial as well as not-for-profit, from the United States and over 53 nations on six continents.[97]

The DMA's members can fall into three broad segments: consumer marketers, business-to-business marketers, and suppliers. Both consumer and business-to-business marketers are the *users* of direct marketing techniques. These marketers employ a number of media, including telephone marketing, catalogs and other direct mail pieces, television, radio, newspaper, magazines, and increasingly the Internet. [98] The suppliers are those companies that provide users with supplies and services.[99]

In October 1997, The Direct Marketing Association (DMA) Board of Directors made a "Privacy Promise" to American consumers. The "Privacy Promise" is a public assurance that, by July 1, 1999, all members of The DMA will follow certain specific practices to protect consumer privacy.[100]

In order to comply with the "Privacy Promise," DMA members are required to do the following:

1. Provide customers with notice of their ability to opt out of information exchanges;
2. Honor customer opt-out requests not to have their contact information transferred to others;
3. Accept and maintain consumer requests to be on an in-house suppress file to stop receiving solicitations from the DMA member; and
4. Use the DMA Preference Service suppression files which exist for mail, e-mail and telephone lists, in order to give consumers the right to choose not to be contacted.

III. "BEST PRACTICES" IN DISCLOSURE

The assortment of self-regulation, statutorily mandated disclosures, and governmental recommendations has left many businesses in a quandary. Many want to alleviate consumer concerns, but are at a loss as to how to achieve this goal. Some err on the side of over-disclosure, operating on the theory that if they tell consumers everything they do with personal

---

[97] *See* http://www.the-dma.org/aboutdma/whatisthedma.shtml

[98] The U.S. direct marketing industry will generate a projected $1.7 trillion in 2000 sales, according to a DMA commissioned study by The WEFA Group. According to Economic Impact: U.S. Direct & Interactive Marketing Today, consumer sales represent 54 percent of the total, with business-to-business sales catching up. In 2005, total direct marketing sales in the United States are projected to surpass $2.7 trillion. *See* http://www.the-dma.org/aboutdma/whatisthedma.shtml#impact

[99] *See* http://www.the-dma.org/aboutdma/whatisthedma.shtml#who

[100] *See* http://www.the-dma.org/library/privacy/privacypromise.shtml

information, they won't leave anything to question, and won't be targeted by regulators. Some decide to disclose nothing, operating on the theory that if they make no assurances about protecting the privacy of consumers' private information, they won't be accused later of making misrepresentations, should information inadvertently slip out, or should their privacy policy change.

Neither over-disclosure nor non-disclosure serves businesses or consumers well. If a business chooses overwhelming disclosure, as was seen in the recent disclosure and opt-out program mandated by the Graham-Leach-Bliley Act, consumers simply do not read the information. Thus, the right to opt out becomes meaningless. Likewise, if the consumer is given no disclosure, and no right to exercise a choice about the use or sharing of personal information, he or she has no knowledge, and no control over personal information.

However, a middle ground exists. While businesses, regulators, and consumers may disagree over the exact details of what should be included in a privacy policy, there is an area where agreement can be reached at least in terms of how businesses can provide meaningful disclosure. When a business chooses to afford privacy protections to consumers, it should describe those protections in a way that consumers can understand.

The balance of this report discusses a menu of "best practices." It emphasizes the need for meaningful disclosure. The report suggests a two-step approach for privacy policies--a one-page summary for consumers highlighting the privacy policy and a more comprehensive explanation of the policy attached or hyperlinked to the one-page summary. It discusses the importance of creating a policy that most Americans are able to read and understand. It does not mandate that the most protective policy be adopted, but gives businesses a number of options based on their own decisions about the necessary level of protection.

The "best practices" suggested in the balance of this report are applicable to both the online and the "brick and mortar" world.

A. PRIVACY POLICY GUIDELINES – GENERAL OVERVIEW[101]

Introduction:

These guidelines are provided as an example for businesses to utilize when developing their own privacy policies. Each business should take into consideration the needs of their own business practices vis-à-vis their customers' preferences when developing a privacy policy. Business models vary, as do data use and retention practices. The differences in business

[101] The skeleton of this guideline was adopted from the Better Business Bureau Online Privacy Seal Program Requirements. *See* www.bbbonline.org

structure and size make a one-size-fits all policy impossible. Accordingly, the following recommendations are made with the knowledge that they may need to be adapted to fit a particular business' constraints:

a. The privacy notice should be easy to read, follow, and understand.

b. The privacy notice should be easily located and be clearly and conspicuously presented on all the home pages of the firms' web sites, services, affiliated links[102] or other Internet mediums at which the firm collects personally identifiable information, including electronic mail addresses.

c. Notices which are given offline should be likewise clear and conspicuous, and provided to the customer at a meaningful time in an appropriate medium.

d. The privacy notice should be written in language and terms that are easily understood by the average individual. The readability factor should comport to the reading level of the average adult based on the Flesch reading scale.[103]

e. The privacy notice should be displayed in a simple text format with minimal graphics.

f. The privacy notice should contain all required disclosures in a single document in a one-page summary linked to the policy itself either through a direct reference or a hyperlink.

g. If the business is engaged European Union-United States data transfers, then the privacy notice should comply with the safe harbor privacy principles set forth by the United States

---

[102] "Affiliated links" refers to links owned and/or operated by "affiliates." "Affiliates" are generally businesses that have common ownership relationships with other business entities. The most common example is a parent and subsidiary relationship. The Gramm-Leach-Bliley Act defines "affiliates" as any company that controls, is controlled by, or is under common control with another company.

[103] The Flesch Reading Ease Scale measures readability as follows:

100	Very easy to read.	Average sentence length is 12 words or less. No words of more than two syllables.
65	Plain English.	Average sentence length is 15 to 20 words. Average word has two syllables.
0	Extremely difficult to read.	Average sentence length is 37 words. Average word has more than two syllables.

The higher the score, the easier the text is to understand. By the very nature of technical subject matter, the Flesch score is usually relatively low for technical documentation. The approach to calculating the Flesch score is as follows: (1) Calculate the average sentence length, L.; (2) Calculate the average number of syllables per word, N.; (3) Calculate score (between 0-100%). *See generally* http: //www. mang. canterbury.ac.nz/ courseinfo/Academic Writing/Flesch.htm.

Department of Commerce. These principles were developed in compliance with the European Union's Directive on Data Protection.[104] [105]

h. The privacy notice should build upon the core principles espoused by the Federal Trade Commission, e.g., notice, choice, access, and enforcement.[106]

i. The privacy policy should refer to existing law applicable to the particular business.[107]

2. Privacy Notice Content

a. Notice

1. The privacy notice should be clearly and conspicuously written and presented.

2. The privacy notice should be easy to find, not buried on the page in an obscure spot, and not hidden in fine print.

3. The privacy notice should specify the various types and categories of personally identifiable information[108] actually collected, or any information that will be collected in the future. In addition, the organization should notify individuals regarding purposes for which they collect and use such information.[109]

---

[104] *See* www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm

[105] The U.S. Department of Commerce in consultation with the European Commission developed a safe harbor framework. The safe harbor--approved by the EU this year--is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. *See* www.export.gov/safeharbor/sh_overview.html

[106] *See* Federal Trade Commission May 2000, A Report to Congress, Privacy Online: Fair Information practices In The Electronic Marketplace. (The core privacy principles espoused by the FTC are Notice, Consent, Access and Correction, Security, Enforcement, and no State preemption).

[107] These guideline provisions are to cover sites not already covered by the following regulatory measures. Congress has enacted privacy regulatory measures for the following areas: Government (Privacy Act of 1974, 5 USC § 552a(1994); The cable industry (Cable Communications Policy Act of 1984, Pub.L.No. 98-549, 98 Stat. 2779 (codified as amended in scattered sections of 47 U.S.C.)); Video rental industry (Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (1988)); Banking and Finance (Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1978)); Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801, Fair Credit Reporting Act, 15 U.S.C. §601; Electronic Communications (Electronic Communications Privacy Act of 1986 (ECPA)), 18 U.S.C. §2511; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §6501.

[108] "Personally Identifiable Information" is defined as any piece of information that relates to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifiable name, number or to other factors more specific to one's physical, physiological, mental, economic, cultural or social identity. *See* www.export.gov/safeharbor/sh_workbook.html

[109] In order to comply with the Department of Commerce safe harbor (NOTICE) principle, organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure. *See* www.export.gov/safeharbor/sh_overview.html

4. If no personally identifiable information is actually collected, or will be collected in the future, then the privacy notice should state this fact in a clear and conspicuous manner.

5. The privacy notice should disclose with whom the information is shared. In the case of online organizations, if there exist links between web sites or online services covered by the policy and non-covered web sites or online services, maintained by the online organization, the privacy notice should identify by URL (or some other identifier) the non-covered web sites or online service.

6. If information is shared with, used by, or sold to affiliates or unaffiliated third parties the notice should disclose the identity of those affiliates or unaffiliated third parties. The affiliates or unaffiliated third parties should be bound by the covered firm's privacy policy.[110]

7. For each type and category of personally identifiable information actually collected or that will be collected in the future, the privacy notice should clearly and specifically disclose how that information will be subsequently used, processed, shared, or sold to any other third party business entity or entity within their own organization.

8. If the organization limits the privacy promises stated in the privacy notice to residents of one particular geographical, or other category of jurisdiction, the notice should so state in a clear and conspicuous manner. The limitations should be presented in an obvious manner and not buried in fine print, or at the bottom of the page.

9. The privacy notice should clearly explain how a consumer may access and review all their personally identifiable information that has been collected or will be collected in the future. The firm should maintain all personally identifiable information in retrievable form. If personally identifiable information is collected, and not maintained in retrievable form, the privacy notice should so disclose. In addition, the organization should provide alternative means to obtain access to the information collected and provide a mechanism to make factual corrections through another medium (i.e. hard copy corrections via the U.S. Postal Service).[111]

---

[110] In order to comply with the Department of Commerce safe harbor (ONWARD TRANSFER) principle, organizations that disclose information to a third party must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principle. *See* www.export.gov/safeharbor/sh_overview.html

[111] The term "corrections" includes, but is not limited to, amending, deleting, updating, and modifying the collected data to ensure accuracy.

10. The privacy notice should clearly explain how a consumer may make factual corrections and update all their personally identifiable information that has been collected or will be collected in the future.

11. If an organization utilizes 'cookies'[112] to gather any personally identifiable information and/or transaction-generated information, it should disclose this fact in a clear and conspicuous manner.[113] In addition, the organization should clearly and specifically disclose how the information, retrieved by the cookie(s), will be utilized. If this information is subsequently shared and/or sold to affiliates or other third parties, it should be disclosed to the user. Moreover, the organization should clearly and explicitly explain how individuals may prevent this transfer of information, at any time, by opting-in or opting-out.

12. If the organization uses personally identifiable information for its own direct marketing, the privacy notice should explain how an individual can, at any time, opt-in or opt-out of this direct marketing.[114]

13. The privacy notice should state the organization's commitment to data security. The organization should specifically describe what measures they take to protect and safeguard the information.

14. The privacy notice should provide contact information for the organization in the instance there are questions or concerns about the organization's privacy and security policies.

15. If information submitted by individuals acting solely in a business capacity (such as a purchasing agent) is excluded from the protections of the privacy notice, the privacy notice should clearly and conspicuously disclose this fact.

---

[112] "Cookies" allow web sites to store information about one's visit to that site on their hard drive. If a user returns to the web site, cookies will read the user's hard drive to find out if they have been there before. The web site will typically use the information that they learn about the user, to market certain products and/or services to them.

[113] "Transaction-Generated Information" is a term that describes information that is collected from cookies that monitor a user's browsing pattern. The information collected is highly valuable for marketers.

[114] In order to comply with the Department of Commerce safe harbor (CHOICE) principle, organizations must give individuals the opportunity to choose (opt-out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt-in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose authorized subsequently by the individual. ["Sensitive" Data is information that pertains to racial or ethnic origins, political or religious beliefs, or health or sex life.] *See* www.export.gov/safeharbor/sh_overview.html

16. If access to any part of the site or service is conditioned on the disclosure of personally identifiable information, the privacy notice should disclose this fact at the point of collection.

17. If information collected online is combined with data obtained from outside parties for purposes of an organization's marketing or any other affiliated or unaffiliated firm's marketing or for any other business endeavor, the privacy notice should disclose this fact in a clear and conspicuous manner.

18. If there are other organizations that reside on a firm's web site or online service and collect personally identifiable information from individuals while they remain on the web site or online service, then the privacy notice should disclose this fact in a clear and conspicuous manner. No information should be collected unless the user has an opportunity to evaluate the other organizations' privacy policies and has the opportunity to opt in or opt out of the data collection. This disclosure and opportunity should be available prior to any collection of data. The privacy notice should identify these other organizations and provide a URL (or some other form of contact information) that would allow an individual the opportunity to evaluate the privacy and security policies of these other organizations.

19. For online businesses, the privacy notice should provide a special note regarding children. Organizations should follow the legal guidelines set forth by the Children's Online Privacy Protection Act (COPPA).[115]

20. If a business has frequently changing business relationships, an effort should be made to update the privacy policy on a regular basis (e.g., quarterly) and to alert consumers to the fact that the privacy policy will be updated periodically. Large businesses may have frequently changing business relationships, which impact their ability to provide up-to-the-minute notice concerning various aspects of their privacy practices. Given this factor, such businesses should state how often they and their affiliates update their privacy policy to take into account new use of personal data as well as changes to the list of parties with whom the business shares information.

b. Shared Information

1. All firm employees, agents, contractors, or other affiliated personnel who have access to personally identifiable information should honor the organization's privacy and security

[115] COPPA, 15 U.S.C. §§ 6501-6506. Section 6502(a) of COPPA prohibits the collection of "personal information" from children under the age of 13 by operators of web sites and on-line services that are directed to children, as well as by operators who knowingly collect personal information from children under the age of 13, in a manner that violates specific regulations promulgated by the FTC. 15 U.S.C. § 6502(a).

policies, hold such information in confidence, and not use such information for any purpose other than to carry out the services they are performing for the organization.

2. An organization should not share any personally identifiable information with any outside party or corporate affiliates when such parties may use such information for their own or subsequent parties' marketing or any other endeavor, without notifying the individual to whom the information relates. The organization should provide the individual an opportunity to opt in or opt out.

3. When the organization transfers any personally identifiable information to outside parties or corporate affiliates, the organization should have in place mechanisms to ensure that such parties are aware of the organization's privacy and security policies applicable to such data. Furthermore, such parties should take reasonable precautions to similarly protect such information.

c. Consent

1. Where an organization uses personally identifiable information for its own direct marketing, it should provide individuals with a choice concerning the direct marketing.

2. An organization should provide individuals a choice about the use of information about them that was not permitted in the privacy notice in effect at the time the information was collected or that is unrelated to the purpose for which the information was collected.

3. The organization should provide individuals with a choice regarding the transfer of information to outside parties; if corporate affiliates operate under a different privacy policy, the organization should note that some of the affiliates with whom it shares data might have different privacy policies.

4. Where the web site conditions the granting of access to some or all of its web site(s) or online service(s) based on the disclosure of personally identifiable information, the organization should inform individuals, in its privacy notice or at the point of collection, of the consequences of refusing to provide such information.

d. Access and Correction

1. An organization should have in place a reasonable process, unlimited by frequency or fee, by which factual inaccuracies in information collected and maintained in retrievable form may be corrected upon request. In addition, the process should be easily utilized by the average individual. Any corrections should be amended in a timely manner.

2. An organization should have in place a process for providing access by making all personally identifiable information maintained in retrievable form, available to the subject of that data upon request. If information is not readily retrievable, an organization should provide alternative means for accessing the information collected. In all instances, an individual should have the opportunity to review, correct, amend, delete and verify any and all information extracted by an organization for factual content and accuracy.[116]

3. An organization should have in place a process to authenticate the identity of a consumer who requests access or correction.

4. For all personally identifiable information to which an organization cannot provide access, either because it is not maintained in retrievable form, or it cannot meet any reasonable frequency or fee limits, the organization should provide:

   a. an explanation why access cannot be provided,
   b. a contact for further information, and
   c. provide alternative means for accessing the information collected (i.e. hard copy review via U.S. Postal Service) in order to make any corrections.

e. Security

An organization should take reasonable steps to ensure that all personally identifiable information is safe from unauthorized access, either physical or electronic. These steps should include at least the following:

1. The organization maintains logs to properly track information and assure that data is only accessed by authorized individuals.

2. The organization maintains a written data security policy.

3. The organization performs at least an annual review of its written data security policy.

4. The organization provides adequate training for employees, agents, and contractors.

5. The organization stores information in a secure environment (using features such as doors, locks, firewalls and/or electronic security).

[116] In order to comply with the Department of Commerce safe harbor (ACCESS) principle, organizations must have personal information about them that an organization holds and be able to correct, amend, or delete, that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. *See* www.export.gov/safeharbor/sh_overview.html

6. An organization should take reasonable steps to assure that personally identifiable information is accurate, complete, and timely for the purposes for which it is used.

7. An organization should take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.[117]

8. Personal information should be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.[118]

f. Enforcement

1. Principles for privacy protection should contain consequences for those who fail to comply with the guidelines.

2. Organizations should participate in privacy seal programs and adhere to the requirements and consequences set forth by such programs.

3. For businesses engaged in European Union-United States data transfers, there should be readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the European Union safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions should be sufficiently rigorous to ensure compliance by the organizations.[119]

Appendix--Model Policies

The following pages consist of four one-page summaries of hypothetical privacy policies. Appendix A incorporates an online "opt-in" policy. The model summary document includes hyperlinks to a copy of the company's complete privacy policy. This provides consumers with easily accessible information and helps them understand the policy's function and scope.

Appendix B incorporates an offline "opt-in" policy. The model summary document includes citations to an attached copy of the company's complete privacy policy. Analogous

[117] *See* www.export.gov/safeharbor/sh_overview.html - Department of Commerce safe harbor principles (SECURITY).

[118] *See* www.export.gov/safeharbor/sh_overview.html - Department of Commerce safe harbor principles (DATA INTEGRITY).

[119] *See* www.export.gov/safeharbor/sh_overview.html - Department of Commerce safe harbor principles (ENFORCEMENT).

to hyperlinks in an online policy, the attached policy provides easily accessible information and aids consumers in understanding its function and scope.

Appendix C incorporates an online "opt-out" policy. The model summary document includes hyperlinks to a copy of the company's complete privacy policy. It allows the consumer to opt out of marketing deals by email, telephone, or direct mail, while reminding the consumer what information can be legally shared. Should consumers not want to opt out online, a hotline is available to answer questions about the policy, to opt out, and to give feedback.[120]

Appendix D incorporates an offline "opt-out" policy. The model summary document includes citations to an attached copy of the company's complete privacy policy. The model document allows consumers to opt out of marketing deals by email, telephone, or direct mail.

Addendum

A draft of this report was circulated for comment prior to its publication. Attached as an Addendum is a compilation of comments received by the authors.

[120] *See, e.g.,* http://personalfinance.firstunion.com/pf/cda/cs/privacy/

ABC WIDGETS, INC.
Privacy Policy- SUMMARY DOCUMENT

WELCOME:

Thank you for visiting our web site and reviewing our privacy policy. This page is a summary document supplementing our more complete and detailed privacy policy. It highlights the most important details for you. We have chosen an "opt-in" model of information collection. No information will be collected from your visit to our site unless you make the decision to share information with our web site. Please review our entire privacy policy for more detailed information < hyperlink to complete privacy policy >

ABC Widgets, Inc. knows that privacy is very important to you and we take privacy concerns seriously! Please read below to learn more about YOUR privacy rights. The following topics are covered in our complete and detailed privacy policy:

1. NOTICE – What information do we collect? What do we do with it?

- We offer a detailed privacy policy < hyperlink >
- We offer you a choice to "opt-in" to any information gathering practices < hyperlink >
- The following provisions apply if you choose to "opt-in":

  - We do not knowingly collect information from or about children and we comply with COPPA < hyperlink >
  - We use "cookies" to gather information about your browsing activities and your IP address < hyperlink >
  - We allow other businesses to place "cookies" on our web site and to gather only non-personally identifiable information < hyperlink >
  - Businesses that have our permission to place cookies are bound by the terms of our privacy policy < hyperlink >
  - We collect personally identifiable information only when you provide it to us < hyperlink >
  - We collect information for the following purposes: (1) to customize advertisements to your specific interests, (2) to fulfill your orders for our products, (3) to contact you when we have any specials or promotions, and (4) to gather statistical information for future marketing plans.
  - We do not sell, rent, transfer, or otherwise share personally identifiable information to other businesses < hyperlink >

2. CONSENT

- You may choose to offer any personal information (opt-in). If you want us to collect your personally identifiable information, click here < hyperlink >
- We place "cookies" only with your permission. To accept cookies, click here < hyperlink >

3. ACCESS

- You have full access rights to any personally identifiable information that we have collected. You have the right to review the information for accuracy and to make any necessary changes or corrections < hyperlink >

4. SECURITY

- ABC Widgets, Inc. uses industry-standard SSL encryption to protect data transmission so that it is virtually impossible for hackers to access your information < hyperlink >
- Our employees are committed to protecting your privacy and will be bound by the terms of this privacy policy < hyperlink >

5. QUESTIONS, SUGGESTIONS, OR COMMENTS

- Please contact us for any reason. We are committed to our customers and want to encourage open communications to meet all of your needs < hyperlink >

ABC WIDGETS, INC.
Privacy Policy- SUMMARY DOCUMENT

WELCOME:

Thank you for reviewing our privacy policy. This page is a summary document supplementing our more complete and detailed privacy policy. It highlights the most important details for you. We have chosen an "opt-in" model of information collection. No information will be collected unless you make the decision to share information with our company. Please review our entire privacy policy for more detailed information < attach copy of complete privacy policy >

ABC Widgets, Inc. knows that privacy is very important to you and we take privacy concerns seriously! Please read below to learn more about YOUR privacy rights. The following topics are covered in our complete and detailed privacy policy:

1. NOTICE – What information do we collect? What do we do with it?

- We offer a detailed privacy policy < see attached policy >
- We offer you a choice to "opt-in" to any information gathering practices < citation to policy section >
- The following provisions apply if you choose to "opt-in":
  - We collect personally identifiable information only when you provide it to us < citation to policy section >
  - We collect information for the following purposes: (1) to customize advertisements to your specific interests, (2) to fulfill your orders for our products, (3) to contact you when we have any specials or promotions, and (4) to gather statistical information for future marketing plans.
  - We do not sell, rent, transfer, or otherwise share personally identifiable information to other businesses < citation to policy section >

2. CONSENT

- You may choose to offer any personal information (opt-in). If you want us to collect your personally identifiable information, please complete and mail the attached pre-paid card, contact us via email < insert address > or call our toll free hotline < insert phone number >

3. ACCESS

- You have full access rights to any personally identifiable information that we have collected. You have the right to review the information for accuracy and to make any necessary changes or corrections. To view your personally identifiable information, please visit our website < insert hyperlink > or call our toll free hotline to request a copy < insert phone number >

4. SECURITY

- Our employees are committed to protecting your privacy and will be bound by the terms of this privacy policy < citation to policy section >

5. QUESTIONS, SUGGESTIONS, OR COMMENTS

- Please contact us for any reason. We are committed to our customers and want to encourage open communications to meet all of your needs < insert phone number > and < email address >

ABC WIDGETS, INC.
Privacy Policy- SUMMARY DOCUMENT

WELCOME:

Thank you for visiting our web site and reviewing our privacy policy. This page is a summary document supplementing our more complete and detailed privacy policy. It highlights the most important details for you. We have chosen an "opt-out" model of information collection. Information will be collected from your visit to our site unless you exercise your right not to share information. Please review our entire privacy policy for more detailed information < hyperlink to complete privacy policy >

ABC Widgets, Inc. knows that privacy is very important to you and we take privacy concerns seriously! Please read below to learn more about YOUR privacy rights. The following topics are covered in our complete and detailed privacy policy:

1. NOTICE – What information do we collect? What do we do with it?

- We offer a detailed privacy policy < hyperlink >
- We offer you a choice to "opt-out" of any information gathering practices < hyperlink >
- The following provisions apply unless you choose to "opt-out":

  - We do not knowingly collect information from or about children and we comply with COPPA < hyperlink >
  - We use "cookies" to gather information about your browsing activities and your IP address < hyperlink >
  - We allow other businesses to place "cookies" on our web site and to gather only non-personally identifiable information < hyperlink >
  - Businesses that have our permission to place cookies are bound by the terms of our privacy policy < hyperlink >
  - We collect personally identifiable information < hyperlink >
  - We collect information for the following purposes: (1) to customize advertisements to your specific interests, (2) to fulfill your orders for our products, (3) to contact you when we have any specials or promotions, and (4) to gather statistical information for future marketing plans.
  - We do not sell, rent, transfer, or otherwise share personally identifiable information to other businesses < hyperlink >

2. CONSENT

- If you do not want us to collect your personally identifiable information, click here < hyperlink >
- To prohibit the use of cookies, click here < hyperlink >

3. ACCESS

- You have full access rights to any personally identifiable information that we have collected. You have the right to review the information for accuracy and to make any necessary changes or corrections < hyperlink >

4. SECURITY

- ABC Widgets, Inc. uses industry-standard SSL encryption to protect data transmission so that it is virtually impossible for hackers to access your information < hyperlink >
- Our employees are committed to protecting your privacy and will be bound by the terms of this privacy policy < hyperlink >

5. QUESTIONS, SUGGESTIONS, OR COMMENTS

- Please contact us for any reason. We are committed to our customers and want to encourage open communications to meet all of your needs < hyperlink >

ABC WIDGETS, INC.
Privacy Policy- SUMMARY DOCUMENT

WELCOME:

Thank you for reviewing our privacy policy. This page is a summary document supplementing our more complete and detailed privacy policy. It highlights the most important details for you. We have chosen an "opt-out" model of information collection. No information will be collected unless you make the decision to share information with our company. Please review our entire privacy policy for more detailed information < attach copy of complete privacy policy >

ABC Widgets, Inc. knows that privacy is very important to you and we take privacy concerns seriously! Please read below to learn more about YOUR privacy rights. The following topics are covered in our complete and detailed privacy policy:

1. NOTICE – What information do we collect? What do we do with it?

- We offer a detailed privacy policy < see attached policy >
- We offer you a choice to "opt-out" of any information gathering practices < citation to policy section >
- The following provisions apply if you choose not to "opt-out":
  - We collect personally identifiable information < citation to policy section >
  - We collect information for the following purposes: (1) to customize advertisements to your specific interests, (2) to fulfill your orders for our products, (3) to contact you when we have any specials or promotions, and (4) to gather statistical information for future marketing plans.
  - We do not sell, rent, transfer, or otherwise share personally identifiable information to other businesses < citation to policy section >

2. CONSENT

- If you do not want us to collect your personally identifiable information, please complete and mail the attached pre-paid card, contact us via email < insert address > or call our toll free hotline < insert phone number >

3. ACCESS

- You have full access rights to any personally identifiable information that we have collected. You have the right to review the information for accuracy and to make any necessary changes or corrections. To view your personally identifiable information, please visit our website < insert hyperlink > or call our toll free hotline to request a copy < insert phone number >

4. SECURITY

- Our employees are committed to protecting your privacy and will be bound by the terms of this privacy policy < citation to policy section >

5. QUESTIONS, SUGGESTIONS, OR COMMENTS

- Please contact us for any reason. We are committed to our customers and want to encourage open communications to meet all of your needs < insert phone number > and < email address >

Addendum

Of

Comments

January 30, 2002

Paula Selis, Senior Counsel
Office of the Washington State Attorney General
900 Fourth Ave., Suite 2000, TB-14
Seattle, WA 98164-1012

Dear Paula,

Thank you for giving me the opportunity to comment on the best practices guidelines you've put together. In reading through your materials, I can see that you and Professor Ramasastry have spent a great deal of time putting them together. Your dual goals of promoting industry self-regulation and creating appropriate standards for consumer protection are admirable.

I certainly speak on behalf of Washington credit unions (and probably on behalf of credit unions generally), when I say that conspicuousness and clarity are of great importance to credit unions as well. After all, the clearer a credit union can make its privacy policies, the less phone calls it can expect to receive from confused members!

Since your e-mail requested any thoughts I might have on whether the information was accurate or whether additional points should be made, I've included a series of comments, thoughts and suggestions attached to this letter. I hope that you find them useful and that I've been able to accurately convey them. Of course, if you have any questions about them, please give me a call and I'll attempt to explain them with greater clarity in person.

In your materials, you state that "[i]n practice…the GLBA opt out provision has failed." While I don't think the GLBA opt out requirements are a failure, I would agree that their success is dubious. Unfortunately, I also believe your worthwhile goal of providing clearly understandable privacy disclosures to the average consumer has been severely (some might say "irreparably") compromised by the regulatory agencies charged with promulgating interpreting regulations.

As you know, the federal financial regulatory agencies were charged with the promulgation of regulations for each of their regulated industries. The final regulations contain safeharbor language that protects financial institutions from liability. While a financial institution certainly isn't *required* to use the suggested language, the arcane nature of the regulation makes the use of the language "blessed" by the federal regulators very wise indeed.

This presents a significant hurdle to the adoption of the model privacy policy you've created—at least for financial institutions required to comply with the GLBA.

It's my belief that few financial institutions will choose language that's more easily understood by consumers at the risk of potential regulatory intercession. (There may not be penalties written into the GLBA, but in the financial community, regulators wield a big stick.)

If I might suggest a course of action, you might want to consider broaching the subject with the federal financial regulators. I would be happy to connect you to the NCUA staff member assigned to work with the bank and thrift regulators on the implementation of the rule.

Finally, in order to encourage businesses to adopt the policies you've drafted, I would suggest that at least one of the model policies should address a more complex hypothetical business, thereby providing an example of the model disclosures suggested in subsection III(A)(2) #(5), #(6), and #(7). The hypothetical businesses used for the models you've provided appear to have a very simple business model and don't appear to share information with any third parties. Since many businesses do share information with third parties, I think it would be very instructive to see examples that cover these more complex situations.

Paula, thanks again for allowing me to share these thoughts with you. I hope that you find them helpful.

Very truly yours,

Stacy S. Augustine
Senior Vice President, Policy & Public Advocacy

Notes & Comments

Page 16, Section IV(B)(1). The first line of the section summarizing the Children's Privacy Protection Act states that no federal statues require the placement of privacy policies on the Internet. While that appears to be true, financial institutions (as they are broadly defined by the Gramm Leach Bliley Act) are required to provide an initial privacy disclosure to the consumer not later than when they establish their account relationship. Therefore, if a financial institution was establishing account relationships through the Internet, the regulations interpreting the Act would require the privacy notice to be posted on the financial institution's Web site. (Each regulated institution has it's own set of regulations, but for credit unions, the initial notice requirement is spelled out in 12 C.F.R. 716.4(a)(1). Guidance on what constitutes an adequate privacy notice on the Internet is provided at 12 C.F.R. 716.3(b)(2)(iii).)

Page 16, Section IV(B)(2). The second subpoint summarizing the Gramm Leach Bliley Act (GLBA) states that financial institutions are required to "obtain consent from consumers prior to disclosing a consumer's nonpublic personal information to nonaffiliated third parties…" This should probably be rephrased since GLBA doesn't require consent; rather, it allows the consumer to excuse themselves from participation in some (not all) information sharing. For example, the subsection could be rephrased to saying something like: "allow consumers to exempt themselves from information sharing with most nonaffiliated third parties."

Page 19, Section IV(B)(8). The section summarizing the Fair Credit Reporting Act accurately describes the Act's compliance requirements for consumer reporting agencies ("credit bureau"). However, I think it's worth pointing out that the Act has a compliance affect on other parties as well. In order to avoid *becoming* a consumer reporting agency, persons who obtain a credit report for the reasons authorized under the FCRA aren't allowed to disseminate or redistribute credit information (except to the consumer herself). This creates significant deterrent effect, since consumer reporting agencies are fairly heavily regulated.

Page 31, III(A)(2)(a)(5). This subsection suggests that businesses should disclose the parties with whom they share information. In order to keep the disclosure simple and understandable, I would suggest that the business disclose the *categories* of parties with whom they share information. First, because listing all of the parties with whom some businesses share information could result in a very long list (I'm basing this on what other businesses have told me, it's not really based my experience with credit unions). Second, the names of parties with whom a business might share information may not educate the average consumer. For example, if a credit union told its members that it shared information with "Ascend United" most consumers wouldn't fully understand the disclosure. On the other hand, if the credit union disclosed the category of business with whom it disclosed information, things might be clearer. For example "we share information with third party collection agencies…" These same comments apply to page 32, III(A)(2)(a)(6).

Page 31, III(A)(2)(a)(5). This same subsection refers to "covered" and "non-covered" Web sites, and I'm not sure what that means.

Page 31, III(A)(2)(a)(7). This subsection requires businesses to describe how information released to third parties will be subsequently used. I think it would be helpful if the best practices model clarified that this subsequent use should be illustrated with examples, but shouldn't have to be exhaustive (again, in the interests of simplicity).

Page 32, III(A)(2)(a)(9)&(10). I'm still not entirely comfortable with the concept of a consumer being able to come in and "correct" their information. I suspect this is because in my past incarnation as a credit union employee I occasionally had to respond to members who demanded to have factual information removed from their files. I think you're onto a winner when you talk

about “factual” information in your model though. There may simply be some things the business and consumer disagree about, but the business should always correct inaccurate fact-based information. This same comment is applicable to page 35, III(A)(2)(d)(1)&(2).

Page 34, III(A)(2)(b)(2). While I can see that having a black and white policy that requires a business to offer consumers an opt out before sharing any information with an outside party would be easy to enforce, I think it overlooks the complexity of many business relationships out there. For example, credit unions routinely share information with mailing services in order to market their own products. I think it’s fair for a business to share information with an outside party if the information is being shared for the businesses’ own marketing purposes or use, as long as the business has a contract with the third party requiring it to keep the information confidential. It’s quite another story for a business to share information with a third party for the *third party’s* marketing purposes, and I think that’s what you’re trying to avoid.

Page 35, III(2)(c)(2). This subsection suggests that information shouldn’t be used for reasons “unrelated to the purpose for which the information was collected” without providing an opt out. While I think it’s fair to require a business to redisclose if they’re using consumer information in a new way, given my druthers I’d avoid any standard that relies on the consumer’s expectation, since it’s pretty hard to tell what most consumers expect out of a transaction.

February 11, 2002

Paula Selis
Senior Counsel
Office of the Attorney General
900 Fourth Avenue-Suite 2000
Seattle, WA 98164-1012

Dear Ms Selis:

Consumer Privacy Protection

The Alliance of American Insurers is a national trade association of 326 property/casualty insurers. Insurer privacy practices in Washington are regulated by the Office of Insurance Commissioner. Additionally, we recognize the inter-relationship between OIC regulations and federal rules applicable to other elements of the financial services industry under the Gramm-Leach-Bliley (GLB) Act. Alliance member companies are in compliance with both the letter and spirit of GLB and OIC regulations.

I am puzzled as to why the Attorney General's Office, which has no statutory role in regulating the financial services industry, has produced the draft report entitled "Protecting Personal Information Through Commercial Best Practices." Nevertheless, we appreciate the opportunity to comment upon the draft report.

One over-arching observation is that the draft report is clearly promoting a Washington-specific approach. This would have the effect of erecting new barriers to commerce that were intentionally torn-down by GLB. This would also impose costly mandates upon insurers, which would ultimately translate into higher premiums and fewer choices for Washington insurance consumers.

With regard to the content of privacy notices, the Alliance has already suggested some proposed parameters or guiding principles for the federal regulators of banking and securities and the Federal Trade Commission (FTC), as well as the National Association of Insurance Commissioners (NAIC). The concepts reflect a more cost-effective alternative to some of the "best practices" suggested in the draft report. The concepts are inter-related, and the order of listing here is not necessarily in order of importance.

I. CLARITY

Privacy notice language should be clear and conspicuous, so that it is reasonably understandable and designed to call the consumer's attention to the nature and significance of the information. Title V of the Gramm-Leach-Bliley (GLB) Act, federal rules, and the 2000 National Association of Insurance Commissioners (NAIC) model privacy regulation already provide guidance. Examples already include: short sentences, bullet points, avoiding highly technical business terminology, use of plain language headings, easy to read type face and type size, etc.

II. FAIRNESS & BALANCE

Any privacy notice language developed should recognize and acknowledge *both* legitimate consumer concerns and rights, as well as legitimate business needs and uses for nonpublic personal information.

III. NEUTRALITY

No attempt should be made to steer consumers toward or away from any sort of preordained opting choice. Within the consumer protections already afforded by Title V of GLB, federal rules, and the 2000 NAIC model regulation, no attempt should be made to dictate or prohibit the use of any particular type face, type size, color, format, medium or technology.

Flexibility

Given the wide array of insurer corporate structures, lines of business, customer profiles, and marketing strategies, etc., an effective "one size fits all" approach may not be workable or desirable. Within existing consumer privacy protections, nothing should be done that would stifle financial service company innovation. Any model privacy notice language(s) developed should be a "safe harbor", not a mandate or "best practice."

In addition to the flexibility to be different, it is also important for affiliated financial services companies to also be able to use the same privacy notice for all of their products and services.

IV. COST EFFECTIVENESS

The administration and content of privacy notices and the opting process should be addressed in a cost-effective fashion for both consumers and financial services companies, since higher costs often translate into higher fees or premiums, or lower returns for financial services

consumers. Often the seemingly "easiest" or "most convenient" approach for the consumer can ultimately translate into the most expensive.

V. TIMING

Any roll-out or start date for federal model language should be coordinated with the NAIC and other state regulators. Sufficient lead-time is crucial. Any changes should be applied prospectively to new business and/or upon renewals.

Consistency & Uniformity

Any model language should be consistent with Title V of GLB and existing federal rules. This process should be used to improve and "fine tune" the implementation and enforcement of GLB. The process should also encourage the NAIC and state insurance departments to promote operational consistency with federal requirements, as well as between and among the states.

Uniformity between and among the state insurance privacy approaches is desirable, but literal uniformity may not be possible, given that many states have laws or regulations that deviate from GLB, the 2000 NAIC model regulation or are based upon the 1982 NAIC model law. Further, this process should *not* be used to develop new substantive or procedural mandates beyond the scope of GLB.

Level Playing Field

Banks, securities firms, and insurers should be allowed, under both federal and state approaches, to use similar language to avoid competitive disadvantage(s). Affiliated financial services companies should also be able to use the same privacy notice for all of their products and services, if they so desire. The same should be true between and among states.

If you need any further information, please contact me (630.724.2109) or Larry Kibbee (360.466.4709).

Sincerely,

Reynold E. Becker
Vice President-Property/Casualty

Copies to: Larry Kibbee
Jean Leonard

G:\PERSLINE\REB\REB2002\LTRWAAG.DOC

January 25, 2002

Paula Selis
Office of the Attorney General
900 Fourth Avenue, Suite 2000,
Seattle, Washington 98164-1012

RE: Comments: National Association of Mutual Insurance Companies (NAMIC)
Consumer Privacy Protection Paper,
State of Washington

Dear:

The purpose of this letter is to provide NAMIC's comments on the above referenced paper. We want to begin by thanking you for your efforts to clarify this process, and the opportunity to offer comment. It is in this spirit that we offer the following comments.

NAMIC is a full-service international trade association with more than 1,200 member companies that underwrite 40 percent ($123.3 billion) of the property/casualty insurance premium in the United States. NAMIC members conduct business in all 50 states, the District of Columbia and Canada. NAMIC's membership includes five of the 10 largest property casualty carriers, every size regional and national property casualty insurer and hundreds of farm mutual insurance companies.

Our first, and most serious concern surrounds the use of the phrase "best practices". We have two primary objections to this phrase.

First, it implies that the practices endorsed in the paper are superior to any others. We are concerned that such a title would carry far too much weight with a jury. Consider, the potential ramifications of issuing such a paper. Assume that a company has issued a privacy notice that does not conform to your proposed best practices, but is nonetheless clear and legally compliant. Assume further that the company is sued over its privacy practices and that the suit barely survives summary judgment. Your paper, and its "best practices" label could be used by plaintiff's counsel with devastating effect. This document may be employed in the way that so many other similar documents have been over the years. Plaintiff's counsel uses it in deposition to establish that defendant's notices do not comply with these "best practices". Counsel may then make this same point in cross-examination in trial and closing argument. The use of the phrase "best practices" implies that authorities have done an exhaustive study and that there are no better ways to write privacy notices. The title that you have attached to your document will carry far too much weight in front of a jury.

Further, we would note that this damage might not be contained to the state of Washington. Depending on the court, it may be used persuasively almost anywhere.

Our second objection is that we are not convinced that these notices have been subjected to sufficient scrutiny to warrant this title. While we certainly don't intend to demean your efforts, or the individuals involved, we have noted the absence of industry privacy experts in your

review. Since Gramm Leach Bliley (GLB) became law, insurance companies have worked diligently to comply with this law. They have found it to be a complex, labor intensive and expensive process. In fact, many major companies have hired Privacy Officers to oversee this process and ensure its compliance with the law. Thousands of hours of staff and legal time have gone into industry effort. It is fair to argue that Corporate Privacy Officers know more about the problems and challenges of implementing GLB than anyone else. Any "best practices" model that fails to include their input will be inadequate, at best.

Finally, we would note that the National Association of Insurance Commissioners (NAIC) has taken up the task of working with industry to find a way to improve privacy notices. I would note that their process has included industry privacy experts. Further, we have raised the same concerns with the appropriate NAIC committee leadership at the their National Meeting in Chicago last December. They are now reconsidering whether it is appropriate to produce a best practices model.

We remain unconvinced that the low response to privacy notices is a result of consumer confusion.

The low response rate to privacy notices should come as no surprise. It was clear from the public debate over GLB that an opt-out requirement would produce a much lower number of people with restricted information than an opt-in requirement. It is general knowledge in political circles that a targeted mailing is successful if it receives a 1 to 2% response. Considering that targeted mailings are sent to people who are identified as motivated to respond to the mailer, the 5% response you cited is outstanding.

We must also take exception to the assertion that "…because of the complexity of the disclosure notices, the disclosure and opting-out effort has not been successful.", yet you offer no evidence to support the existence of a nexus between the two. Further, while we don't contest that people are concerned about the privacy and integrity of their personal information, I would point you to page 4 and footnote 9 of your paper, which provides evidence that refutes the very nexus that you have asserted. This part of the paper provides statistics showing that over 2/3 of internet users believe that their privacy is compromised by use of the internet. One page 7, you cite a recent Gallop Poll indicating that 53% of those who use the internet are "very concerned" about the security surrounding their personal information. Yet, they continue to use the internet and as your paper notes, it continues to grow at an extraordinary rate. This suggests that while people are concerned about their privacy, they are also willing to expose themselves to certain risks in return for the benefits. Absent specific evidence to the contrary, it is hard to imagine that people exhibit different behavior when they receive privacy notices.

The use of "legalese".

Your paper is critical of the use of legal terms in notices, and quite correctly notes that phrases like "non-public personal information" are confusing. While this criticism may be valid, it is not validly directed against industry. Rather, government and the tort system should be the focus of this complaint. In this day and age we do not have to work too hard to imagine a scenario where a "plain language" notice would be found noncompliant by a regulator for vagueness because the wording in the notice varied from the precise meaning of the law. Of even greater concern is corporate susceptibility to class action lawsuits for alleged noncompliance and/or misleading plain language notices.

We appreciate your recognition, on page 28, of the problems faced by industry, but we believe that the remedy for this problem is a safe harbor plain language in provision in GLB and to pursue tort reform. With regard to GLB in particular, a plain language safe harbor provision would go a long way to resolving this problem. Corporate conservatism in this regard is a reflection of the current legal climate; the solution is reform of that climate.

In conclusion, we make the following suggestions:

1. Abandon the pursuit of a "best practices" approach in that, despite your good intentions, it can do much more harm than good.
2. If you continue to be convinced that the wording of privacy notices is the cause of the 5% response rate, focus on reform efforts that will allow industry to write plain language notices, such as: safe harbor amendments to GLB and tort reform.
3. Consider working with the NAIC in that they already have a process underway.
4. Perhaps most important, involve corporate privacy officers.

Thank you for the opportunity to comment.

Sincerely,

Peter A. Bisbecos
Legislative and Regulatory Counsel

The benefits of information use

Because of the relative free-flow of information, the United States has the most robust economy in the world, and its consumers have greater choice and receive greater value than consumers anywhere else in the world.

1. Consumer benefits of information use

Direct marketing: Direct marketing services increase choice and opportunity and reduce costs. Direct marketing offers present consumers with products and services from companies about which they may otherwise never have known. By identifying the characteristics of consumers likely to be interested in certain kinds of products and services, direct marketers reduce unwanted mail and send only offers that consumers are likely to want or need.

Similarly, market analysis services help businesses identify the common characteristics of their customers. A richer understanding of their customer base helps businesses better plan media campaigns, determine retail site location, develop new product offerings, better position their brands, have a clearer understanding of their customers' service needs, and reach new customers. For consumers, the result is lower product cost, better customer service, more convenient shopping, faster delivery, reduced unwanted mail and exposure to useful new products and services.

An April 2001 study by the Information Services Executive Council (ISEC) of the Direct Marketing Association found restrictions on marketing information use would cost catalog and Internet apparel shoppers $1 billion annually. According to the study, that cost would be shared disproportionately by inner city and rural catalog shoppers. Inner city neighborhoods generally are under-served by traditional retail stores, and rural consumers often live long distances from the nearest mall or retail center. As a result, these two groups are more reliant on catalog or Internet shopping alternatives.

Similarly, a December 2000 study by Ernst & Young found members of the Financial Services Roundtable (FSR) – a group of 90 of the nation's top banking, insurance and securities firms – save approximately $1 billion a year by using targeted marketing. Much of those savings are passed directly on to consumers.

Credit reporting: The United States' unique credit reporting system dramatically increases American consumers' choices and opportunities for financial services. The open U.S. credit reporting system provides a foundation for lender confidence, increasing the availability of loans, reducing the cost of credit and increasing competition for customers, all of which benefit the U.S. consumer. Because of the U.S. automated credit reporting system, American consumers can obtain credit and secure other financial services at lower costs from a larger number of providers than anywhere else in the world. It has been said that credit reporting is a secret ingredient of the U.S. economy's resilience. Some estimate that because of the U.S. credit

reporting system, consumers in this country save as much as $80 billion a year on mortgage loans alone.

Individual reference services: Often the benefits of individual reference services, and the services themselves are taken for granted. Yet they are used everyday. People, businesses, law enforcement and other organizations utilize individual reference services routinely to locate, identify and contact people for a variety of very positive reasons. The most familiar example of an individual reference service is the telephone book. Basic reference services, such as a telephone book, are available to almost anyone. Experian separately provides more sophisticated services only to law enforcement or other qualified users. A few of the users of individual reference services and how such services are utilized are listed below.

- **You:** through the telephone book or directory assistance to find a telephone number or an address to send a thank you note or holiday greeting.
- **Lenders, retailers, e-tailers:** to verify the identities of potential customers and protect you from fraud.
- **Law enforcement agencies:** to locate crime witnesses and apprehend criminal suspects.
- **Child support agencies:** to locate parents who are behind in their child support payments.
- **Government agencies:** to find missing pension fund beneficiaries and heirs.
- **Alumni Associations:** to contact recent graduates and send event notices to current members.
- **Businesses:** for product recalls and product notices.

2. Overall economic benefits of information use

Information promotes competition in the marketplace. Information sharing for target marketing and credit reporting opens the door for small, emerging businesses to compete with larger, established companies. It levels the playing field by making the cost of entry affordable to everyone.

Information sharing "allows new market entrants, which cannot afford mass market advertising and lack the customer lists of their well-established competitors, the ability to reach those people most likely to be interested," said Fred H. Cate and Michael E. Staten in their paper*, Putting People First: Consumer Benefits of Information-Sharing*.

The implication is that large companies could bear the cost of mass marketing – ostensibly unfettered distribution to every U.S. consumer. For small businesses, it means being forced out of the marketplace. With reduced competition, consumers would be faced with higher prices and less choice.

The ISEC study mentioned above reached the same conclusion when looking at an opt-in approach to marketing information as opposed to the current opt-out standard. Implementation of data use restrictions would drive total costs up from 3.5 to 11 percent. The result would be devastating to small firms and new market entrants.

According to the study, “Since marketing costs will likely increase if external opt-in restrictions are put in place, some retailers will be forced to exit the market and other, new companies will be deterred form entry. With a smaller marketplace, competition suffers, giving consumers less choice and higher costs when distance shopping.”[13]

It is easy to overlook the impact of information use on our local, small businesses. We too often take for granted the local food store, pharmacy or men’s clothing store. In today’s economy, they are competing not only with giant supermarkets, drug outlet stores and shopping malls, but also with online services that may deliver to your door. In such an environment, information sharing is critical for small businesses just to maintain a storefront in the community.

CONSUMER ACCESS TO BUSINESS DATABASES

Providing consumers access to data that is collected about them and the right to correct inaccuracies in that data is often considered an essential fair information practice. The Fair Credit Reporting Act (FCRA), for instance, mandates easy and inexpensive access to consumer credit reports as well as a minimum level of service that consumer reporting agencies must provide consumers to correct inaccurate information. Some privacy advocates would like to extend those rights and benefits to consumers who want to access and correct information contained in databases used for marketing purposes.

Experian believes that a legislative mandate for access to marketing databases, whether online or offline, raises more issues relating to personal privacy and security than it solves. Data used for consumer reporting is vastly different that that used for marketing. The analogy that both sets of data should be available to consumers for access and correction is specious.

There are two major differences between the data in credit reports and the data that are typically collected for marketing purposes. First, credit data is arrayed in name-driven consumer profiles and contains the necessary information (such as Social Security numbers and account numbers) that can serve to authenticate the identity of the person requesting access to the data. Marketing data is usually arrayed by summarized household attributes, not name driven profiles. This household information rarely contains the necessary identifying information necessary to authenticate a person's request for access. To give access to requestors based only on name and address, which is widely available in public sources such as telephone directories, raises greater privacy risks than it solves.

The second and most important distinction is that credit data is used as the basis for major underwriting decisions affecting consumers, such as whether to grant a loan, provide insurance coverage, offer a job or extend utility services. With such high stakes for consumers, the need to know the scope and accuracy of the data in consumer reports is of utmost important. Marketing data, on the other hand, is simply used to make the best estimate of an individual's propensity to be interested in, and respond to, a specific offer or solicitation.

Access requirements, therefore, should be constructed by balancing the benefits to and privacy of consumers against the risks and costs to companies that hold the data. Allowing access to marketing databases would be enormously expensive. Existing database architecture would need to be redesigned and disparate databases linked together to form name-driven profiles; large customer service staffs would need to be hired; stringent security safeguards would need to be put into place; files would have to contain sensitive identifying information for authentication purposes. While that expense is justified and necessary for information covered by the Fair Credit Reporting Act, it is of questionable value for data collected for marketing purposes only. Further, there appears to be little consumer demand for access. The overwhelming majority of individuals, upon learning that access is not an option, appear satisfied to learn that they may simply "opt-out" of having their name shared for marketing purposes.

JANUARY 31, 2002

Paula Selis
Office of the Attorney General
900 Fourth Avenue, Suite 2000

Seattle, Washington 98164-1012

Dear Ms. Selis,

Thank you for providing the Washington Retail Association ("WRA") with an opportunity to review and comment on the University of Washington's "Protecting Personal Information through Commercial Best Practices" draft. Those comments outlined in this letter and the attached paper reflects the general response from our membership. The comments provided in no way however, endorse the "Protecting Personal Information through Commercial Best Practices" draft and this letter should not be seen as supporting any concepts or themes in the publication.

With that said, developing a document that may be used to educate both businesses and consumers is valuable, particularly because it will serve as a basis for further discussion of the varied and complex issues surrounding privacy. To that end, the WRA submits the following comments to ensure that the concepts laid out in such a document accurately reflect the current status of privacy laws and business practices and also that any recommended best practices are both workable and necessary.

WRA was asked to submit comments to the Washington State Attorney Generals office in August of 2000 with the understanding that those comments would then be taken into consideration for a recommendation by the Washington Attorney Generals office to the National Association of Attorneys General (NAAG). The comments the WRA submitted then still accurately reflect the position and views the WRA holds.

In August of 2000 WRA submitted comments regarding five privacy principles that the Attorney Generals office identified as being "necessary" to address in privacy legislation. Those principles are:

1. Notice—data collectors must disclose their information practices before collecting personal information from consumers;
2. Choice—consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;
3. Access—consumers should be able to view and contest the accuracy and completeness of data collected about them;
4. Security—data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use; and
5. Enforcement—the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices.

When WRA submitted our comments regarding the five principles we asked that four more principles be added when reviewing privacy legislation. The four other key principles are:

1. Consumer Benefit—Laws and regulations intended to protect consumer privacy should maximize consumer benefits;
2. Reasonableness—Laws and regulations intended to protect consumer privacy should be reasonable in their scope and consequences;
3. Proportionality—Privacy protection should be commensurate with the harm threatened if personal data are misused; and
4. Convenience—Privacy protections should be convenient, easy to use, and predictable, and to the extent possible, should reflect reasonable consumer expectations.

WRA also would like to make the following specific comments on your draft. These comments focus on issues of accuracy, as well as certain points that may not have been fully addressed in WRA's comments, submitted in August of 2000.

- In discussing the effects of identity theft and noting that the victims may be "accountable for defaults in payment and ruined credit histories", the report omits any discussion on the laws that limit a consumer's liability in the event of credit card fraud that is reported to the card issuer. We would recommend including a discussion of that point. (Page 6, last sentence of paragraph 1 of Section II.A)

- The report asserts that increases in identity theft may be correlated to a loss of privacy; however, the report cites no support for that conclusion. Misuse of information is not necessarily increased simply because that information may be transferred between companies. Any such statement should be supported by specific studies. (Page 6, last paragraph of Section II.A)

- Sub-item (2) under the discussion of the Gramm-Leach-Bliley Act (the "GLB") does not accurately reflect the requirements of the GLB. It indicates that companies must obtain consent from customers prior to disclosing information to nonaffiliated third parties. In fact, the GLB requires companies to provide notice and an opportunity to opt-out before sharing such information. The report should be corrected to accurately describe the GLB. (Page 16, Section IV.B.2)

- In discussing the Direct Marketing Association ("DMA") suppression services, the report indicates that DMA email suppression is not yet available. In fact, the DMA is currently offering email suppression services to consumers on the DMA website (www.the-dma.org). (Page 26, Section IV.D.2.a)

- While the WRA agrees that having a one-page summary followed by a more detailed privacy policy is a good recommendation, we don't think that companies should be limited to following that approach. There may be more effective ways to communicate, and, for some companies, it may not be possible to fit all of the required disclosures on a single page, while addressing them in a clear and meaningful way. (Page 30, Section V.A.e)

- In discussing the types of disclosures that should be made in privacy policies, in many instances, the report recommends that companies disclose not only current uses, but also future uses. In addition, it often mandates very specific disclosures (e.g., disclosures of the specific uses that will be made of information and of the specific entities with which it will be shared). These are very difficult standards to satisfy and potentially could mean that companies have to make weekly changes in their policies. As businesses change and evolve, their use of information may change, and the companies with which it is shared may change. For example, while a company may enter into a partnership with one website to provide a service, it ultimately may decide to switch to a different partner that offers a wider range of services. It serves the interests of neither the business nor the consumer to require disclosures that are that specific or that try to forecast all possible future actions. Instead, businesses should disclose the categories of information that may be shared, the types of uses to which it may be put and the types of businesses with which it may be shared. We think GLB sets the appropriate standard—as well as the appropriate balance between the general v. the specific—in that regard. If further specifics are required, it will simply serve to lengthen the notices that the report criticizes for already being too long and complex. (Pages 31-34, Section V.A.2.a)

- The report specifies that businesses should be required to join privacy seal programs. We do not believe that laws should mandate such a requirement, as a company may choose an alternative means to ensure compliance. (Page 37, Section V.A.2.f.2)

The Washington Retail Association appreciates the opportunity to have their over-view included in the addendum to the "Protecting Personal Information through Commercial Best Practices" published by the University of Washington. We would however wish to express again our concerns that our submittal not be viewed as an all inclusive response, nor an endorsement of any views expressed in the publication.

The Washington Retail Association represents over 2700 retail businesses in Washington state whose livelihood depends upon good public policy. It is WRA's hope that any future discussions or published papers on this issue will take into consideration WRA's comments.

Sincerely,

Jan Teague, President
Washington Retail Association

Cc: Jan Gee, Contract Lobbyist, Washington Retail Association
Dedi Hitchens, Government Affairs Director, Washington Retail Association

III. Best Practices in Disclosure

A. PRIVACY POLICY GUIDELINES – GENERAL OVERVIEW

b. The privacy notice should be easily located and be clearly and conspicuously presented on all the home pages of the firms' web sites, services, affiliated links, or other Internet mediums at which the firm collects personally identifiable information including electronic mail addresses. Notices which are given offline should be likewise clear and conspicuous, and provided to the customer at a meaningful time in an appropriate medium.

Microsoft understands the necessity of clear and conspicuous notice to customers. However, this recommendation seems to suggest that there should be one privacy statement for an entire company. That would be impossible for companies such as Microsoft, which has many different businesses and many different products and services. Even if it were possible, such a requirement would make the statement incredibly long and complex.

d. The privacy notice should be displayed in a simple text format with minimal graphics.

This statement creates the impression that graphic hinder, rather than assist users in accessing a company's privacy policy. On the contrary, graphics can oftentimes aid in the readability and navigation of a document. Furthermore, graphics can also help a user find the privacy policy on a web site. Microsoft has considered using "Privacy Icons" to enhance the readability of our statements and believes that design requirements are not necessarily useful in government-developed guidelines.

e. The privacy notice should contain all required disclosures in a single document in a one-page summary linked to the policy itself either through a direct reference or a hyperlink.

As noted above, a one page privacy summary might work in certain cases, (i.e. small company with limited products and lines of business), but does not fit well within the business model of multi-service companies such as Microsoft.

f. If the business is engaged in international business then the privacy notice should comply with the safe harbor privacy principles set forth by the United States Department of Commerce. These principles were developed in compliance with the European Union's Directive on Data Protection

As you know, Microsoft has agreed to abide by the safe harbor principles of the EU Data Protection Directive. However, many companies choose not to be designated as "Safe Harbor compliant," but to simply comply with the individual jurisdiction's privacy laws. Further, the Safe Harbor principles are relevant only for EU-US data transfers. Some companies may choose to use those principles internationally, but some may not. Therefore, it would seem that guidance on compliance with international privacy is an issue best left to federal and international regulatory bodies.

2. Privacy Notice Content

a. Notice

2. The privacy notice should be easy to find, not buried at the bottom of the page, and not hidden in fine print.

This statement ignores current industry practice within the online industry, as it has become standard for companies to put the privacy notice at the bottom of the page. Indeed, the Washington AG web page follows what is common for the rest of the private sector. Indeed, this is not considered a bad practice by TRUSTe and other self-regulatory and safe harbor seal programs.

3. The privacy notice should specify the various types and categories of personally identifiable information actually collected, or any information that will be collected in the future. In addition, the organization should notify individuals regarding purposes for which they collect and use such information.

TRUSTe and other self-regulatory seal programs direct companies that their privacy notices should inform consumers of the company's current operations—and with good reason. Given the continuous evolution of marketing and other business relationships, it is nearly impossible to predict what information may be collected in the future. Quite simply, companies whose business relationships change on a daily basis could not possibly comply with such a requirement.

5. The privacy notice should disclose with whom the information is shared. In the case of online organizations, if there exist links between covered web sites or online services and non-covered web sites or online services, maintained by an organization, the privacy notice should identify by URL (or some other identifier) the non-covered web sites or online service.

As previously noted, business relationships change daily with any large company. The kind of data sharing that occurs as a result of a simple online purchase involves multiple parties, including the vendor's bank, the user's bank, the credit card processing entity, one or more shipping companies, a fulfillment partner, etc. However, this requirement would require a company's privacy statements to list thousands of companies – if it were to cover every potential data sharing scenario. And the statement would likely need to be updated on a daily basis.

6. If information is shared with, used by, or sold to affiliates or unaffiliated third parties the notice should disclose the identity of those affiliates or unaffiliated third parties. The affiliates or unaffiliated third parties should be bound by the covered firm's privacy policy.

With regard to the first statement, we would restate the point previously noted, namely, that given our changing business relationships, it is extremely difficult to identify all affiliated and unaffiliated third parties. The most reasonable expectation would be for a company to describe the types of third parties with which data may be shared, and under what circumstances.

Further, it is unclear what would be required under the principle contained in the second clause. As a threshold matter, it is important to note that such a policy is not in practice today on

the Internet as a whole with respect to unaffiliated web sites. We agree that if the data is shared with a third party that is acting as an agent of the data collector, the agent should treat the data in a way that is consistent with the data collector's privacy policy. Such a requirement is usually dealt with through vendor contacts. However, outside of the agent relationship, people often provide links to another site's privacy links, and do not guarantee, or are held accountable for compliance with the original site's privacy policies.

If the data sharing is in a non-agent scenario, then providing a link to the other company's privacy statement should be sufficient. And this should not necessarily have to be done in the privacy statement itself. For example, on a co-branded web site, notice of another company's involvement can be provided on the data collection screen itself, with links to both our privacy statement and the statement of the other company.

7. *For each type and category of personally identifiable information actually collected or information that will be collected in the future. The privacy notice should clearly and specifically disclose how that information will be subsequently used, processed, shared, or sold to any other third party business entity or entity within their own organization.*

Again, companies cannot predict the future. Rather, companies provide consumers with notice of the general uses for which their information is currently, or could be used in the future.

9. *The privacy notice should clearly explain how a consumer may access and review all their personally identifiable information that has been collected or will be collected in the future. The firm should maintain all personally identifiable information in retrievable form. If personally identifiable information is collected, and not maintained in retrievable form, the privacy notice should so disclose. In addition, the organization should provide alternative means to obtain access to the information collected and provide a mechanism to make corrections through another medium (i.e. hard copy corrections via the U.S. Postal Service).*

We are concerned that the requirement to maintain all personally identifiable information in retrievable form would create a new compliance burden, is not reflective of current industry practice and would ultimately result in less privacy protection to consumers.

One way that companies can protect privacy is to "retire" or "delete" data after a period of time. But this does not always mean that the data is literally eliminated from every possible location – there may be warehoused backup tapes, archived transactional records, etc. that contain copies of personal data. In many cases, tracking down and actually getting rid of every possible record containing the personal information would be impossible. As long as the data is made so that it is not retrievable in the ordinary course of business (which is how COPPA defines "delete"), then the user's privacy is protected.

Unfortunately, this would eliminate a valuable tool in protecting user privacy – companies would never attempt to retire or delete data if doing so, where there is some chance of some copy remaining in a non-retrievable form, would get them into trouble.

11. If an organization utilizes 'cookies' to gather any personally identifiable information and/or transaction-generated information, it should disclose this fact in a clear and conspicuous

manner. In addition, the organization should clearly and specifically disclose how the information, retrieved by the cookie(s), will be utilized. If this information is subsequently shared and/or sold to affiliates or other third parties, it should be disclosed to the user. The latter is already covered above. Moreover, the organization should clearly and explicitly explain how individuals may prevent this transfer of information, at any time, by opting-in or opting-out.

If the cookies are collecting PII, then the issues around disclosing the user and sharing of this PII should be the same as any other PII. Simply, there does not appear to be a need to create a separate rule for PII collected via cookies. The only requirement here should be to disclose the use of cookies, and how they are used to collect PII.

12. If access to any part of the site or service is conditioned on the disclosure of personally identifiable information the privacy notice should disclose this fact at the point of collection.

Online vendors routinely provide discounted goods and services in return for the use of PII. However, this principle would impose a new requirement on such vendors, while concomitantly adding to the complexity of the disclosure in the privacy notice. Further, it would make more for such a requirement to be disclosed in the user interface, rather than in the site's privacy statement.

16. *If information collected online is combined with data obtained from outside parties for purposes of an organization's marketing or any other affiliated or unaffiliated firm's marketing or for any other business endeavor, the privacy notice should disclose this fact in a clear and conspicuous manner.*

While there have been suggestions that this type of information be disclosed, we are unaware of any appended data disclosure best practice. Further, such a requirement would exceed anything required today by TRUSTe.

17. *For online businesses, the privacy notice should provide a special note regarding children. Organizations should follow the legal guidelines set forth by the Children's Online Privacy Protection Act (COPPA).*

While Microsoft fully complies with COPPA, we believe that grafting such requirements onto sites that are clearly aimed at adults is unnecessary and burdensome. For example, children's privacy issues are oftentimes deemphasized in business-to-business sites, or sites for highly technical audiences

c. Consent

1. Where an organization uses personally identifiable information for its own direct marketing, it should provide individuals with a choice concerning the direct marketing.

This guideline is not necessarily applicable or necessary in all direct marketing models. Oftentimes, the product or service that the user is requesting relies on direct marketing to support the service. Further, the user is likely to be fully aware that the direct marketing is

part of the service. Suppose, for example, that a user is offered an e-mail service for free if they agree to receive 10 marketing messages a week. In such cases, there should be no requirement that users be able to opt-in or opt-out of the direct marketing.

2. An organization should provide individuals a choice about the use of information about them that was not permitted in the privacy notice in effect at the time the information was collected or that is unrelated to the purpose for which the information was collected.

This guideline is overly broad, as it essentially requires the vendor to provide the user with a choice about all uses of data, except for the original customer request. Practically, this would mean that companies would have to offer choice with regard to a host of uses including analysis, administration, targeting, etc, regardless of whether PII data was used or whether anonymous data was used.

3. The organization should provide individuals with a choice regarding the transfer of information to outside parties or corporate affiliates operating under a different privacy notice.

Again, this guideline present significant administrative hurdles and additional complexity to consumers. For example, the "microsoft.com" privacy statement is different than the "MSN" privacy statement, which in turn is different than WebTV's privacy statement. As is often the case, there may be several different privacy notices across a company. However, as long as each affiliate that has access to the data abides by the limitations of the privacy statement under which the data was collected, then there should be no issue with regard to the privacy statement that the affiliate actually displays.

d. Access and Correction

1. An organization should have in place a process, unlimited by frequency or fee by which factual inaccuracies in information collected and maintained in retrievable form may be corrected upon request. In addition, the process should be easily utilized by the average individual. Any corrections should be amended in a timely manner.

This guideline goes well beyond the EU-safe harbor requirement, which directs companies to provide "reasonable" processes for the correction of factual inaccuracies of information. Indeed, most best practice guidelines and standards permit reasonable limits on access of information to prevent abusive of repetitive requests. These limits are especially important if the process is not an automated on-line process.

2. An organization should have in place a process for providing access by making all personally identifiable information maintained in retrievable form, available to the subject of that data upon request. If information is not readily retrievable, an organization should provide alternative means for accessing the information collected. In all instances, an individual should have the opportunity to review, correct, amend, delete and verify any and all information extracted by an organization for content and accuracy.

We are concerned that the use of the phrase "any and all" extends the requirement outside the boundary of PII boundary. Further, any access requirement should only apply to data that is readily retrievable. If the information is not readily retrievable, it stands to reason that companies wouldn't be accessing it, using it or transferring it. It is therefore difficult to understand what privacy issue would be raised under such circumstances.

3. An organization should have in place a process to authenticate the identity of a consumer who requests access or correction.

One of the continuing challenges for industry and regulators is how to promote access to information, without having to collect additional information from consumers. This principle highlights this dilemma. Oftentimes, the only way that an organization can have a meaningful process by which to authenticate the identity of a consumer requesting access, is to simultaneously gain access to that persons PII—the very practice that many privacy advocates continue to criticize. Further, the principle, is unclear as to whether the inability to adequately authenticate a person would give the organization the right to deny the request for access to the information

4. For all personally identifiable information to which an organization cannot provide access, either because it is not maintained in retrievable form, or it cannot meet any reasonable frequency or fee limits, the organization should provide:

d. an explanation why access cannot be provided,
e. a contact for further information, and
f. provide alternative means for accessing the information collected (i.e. hard copy review via U.S. Postal Service) in order to make any corrections.

Again, the access requirement should only apply to retrievable PII. Further, the hard-copy review requirement goes far beyond any existing best practices guidelines, and could only be implemented a tremendous cost to online vendors.

e. Security

An organization should take reasonable steps to ensure that all personally identifiable information is safe from unauthorized access, either physical or electronic. These steps should include at least the following:

1. The organization maintains logs to properly track information and assure that data is only accessed by authorized individuals.

Again, the scope of such a requirement is unclear. For example, would a company be required to provide notice to the individuals (customers or employees) who might be identified in these logs? Would the logs become subject to the access requirement?

3. The organization performs at least an annual review of its written data security policy.

Third party seal programs such as TRUSTe are tasked with continually reviewing a company's privacy and security practices. Further, any company that fails to protect the privacy and security of its customers information stands to lose significant good will and business among its current and potential customers. As such, we believe that any best practice guidelines should continue to rely on these third party seal programs to enforce compliance with their requirements.

f. Enforcement

2. Organizations should participate in privacy seal programs and adhere to the requirements and consequences set forth by such industry regulators.

While Microsoft continues to advocate reliance on third-party seal programs, we believe that such decisions should be the decision of the individual organizations. Due to cost however, privacy seal programs are not necessarily a one size fits all solution appropriate for every organization. For example, if an organization posts a privacy statement, the FTC and state AGs office can use existing enforcement authority to enforce compliance with the information practices contained in the privacy statement. In such cases, this existing enforcement authority would provide an adequate level of protection to consumers. However, if the consumer is unwilling to disclose information to sites that do not display third-party privacy seals, then he or she is perfectly capable of refusing to do business with that particular web site.

3. For businesses engaged in international business, there should be readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the European Union safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions should be sufficiently rigorous to ensure compliance by the organizations

As previously noted, Safe Harbor is relevant only for EU/US data transfers. The requirements in other international markets may be quite different, and it's should be left up to the individual organization as to whether it wants to take a consistent approach for its various international operations.

COMMENTS OF THE WASHINGTON RETAIL ASSOCIATION TO THE NATIONAL ASSOCIATION OF ATTORNEYS GENERAL ON CONSUMER PRIVACY PRINCIPLES

August 11, 2000

Executive Summary

During the past three decades governmental organizations have identified a wide range of principles that they believe are essential to protecting consumer privacy. The most recent set of privacy principles was put forward by the Federal Trade Commission ("FTC") in its May 2000 report, *Privacy Online: Fair Information Practices in the Electronic Marketplace.* The FTC identified five principles: notice, choice, access, security, and enforcement. The Washington Retail Association ("WRA"), while generally supportive of these principles in theory, is concerned that using these principles as the basis for new privacy laws would duplicate or even interfere with existing private-sector privacy protections already used by retailers, and the WRA is particularly wary of extending principles developed solely for one context—the Internet—to commerce generally.

In addition, the WRA believes that the FTC's five Internet privacy principles are incomplete and may disserve consumers if not supplemented with four additional principles:

1. Consumer Benefit—Laws and regulations intended to protect consumer privacy should maximize consumer benefits, including the many benefits that flow from the responsible use of personal information. Without reliable access to personal information, businesses cannot anticipate and meet consumer needs, and consumer service and convenience suffers. Maximizing consumer benefit, then, requires that privacy protection be balanced against the benefits that flow from accessible information, and that the government avoid restricting the practical ability of individual consumers to strike that balance for themselves.

2. Reasonableness—Laws and regulations intended to protect consumer privacy should be reasonable in their scope and consequences. Consistent with the First Amendment, privacy laws should apply only to information that is nonpublic and that threatens a specific harm.

3. Proportionality—Privacy protection should be commensurate with the harm threatened if personal data are misused. Proportionality is a constitutional obligation.

4. Convenience—Privacy protections should be convenient, easy to use, and predictable, and to the extent possible, should reflect reasonable consumer expectations.

These four principles not only supplement the FTC's, they also provide a more specific understanding of how the FTC's principles should be applied in practice. The meaning of notice, choice, access, security, and enforcement, and the means by which these principles are implemented, will depend significantly on the type of information involved, the context in which it is collected, and the use to which it is to be put. This is the very definition of "reasonableness" and "proportionality," and critical to assuring that privacy protections both maximize consumer benefits and reflect consumer expectations.

The WRA also proposes two additional principles concerning the role of the government in general, and of the States in particular, in enacting and enforcing privacy protections that we believe flow from the consumer benefit, reasonableness, proportionality, and convenience principles, but that are not addressed by the FTC:

1. Preemption—To the extent laws are necessary to enhance consumer privacy protection, those laws should be national in scope, and should preempt state laws on the same subject matter. However, States should continue to control access to their own public records, consistent with the First Amendment; advise the federal government on appropriate privacy protection; and share enforcement authority with federal agencies under federal privacy laws.

2. Interaction of Overlapping Laws—States and the federal government should work to avoid enacting laws and regulations that merely duplicate or conflict with existing privacy protections. Where such overlapping obligations already exist, States and the federal government should work to eliminate them, avoid enforcing more than one set of obligations against the same party for the same conduct, and treat compliance with the most restrictive of overlapping requirements as compliance with all of the lesser requirements.

Finally, the WRA wishes to stress that retailers already protect the privacy of their customers' information far more than any law or regulation requires. We believe that the greatest threat to consumer privacy today comes not from responsible businesses with significant investments in their reputations and customer relationships, but rather from the government and criminals, neither of which will be affected by new privacy laws and regulations. We strongly encourage NAAG to avoid proposing new laws or regulations that merely duplicate existing requirements or private-sector protections, or that burden responsible, law-abiding retailers and their customers in a well-intentioned but misfocused effort to control the behavior of other industries or parties.

COMMENTS OF THE WASHINGTON RETAIL ASSOCIATION TO THE NATIONAL ASSOCIATION OF ATTORNEYS GENERAL ON CONSUMER PRIVACY PRINCIPLES

August 11, 2000

The Washington Retail Association ("WRA") welcomes the opportunity to comment on principles for appropriately protecting consumer privacy, and it appreciates the invitation of Attorney General Gregoire, Immediate Past President of the National Association of Attorneys General ("NAAG"), to do so.

Existing Privacy Principles

There are many sets of "fair information practice principles" designed to protect consumer privacy. The first comprehensive set of these principles was articulated in 1973 by the U.S. Department of Health, Education and Welfare.[i] Since that time, additional versions of privacy principles have been put forward in 1977 by the U.S. Privacy Protection Study Commission;[ii] in 1980 by the Organization for Economic Cooperation and Development;[iii] in 1995 by the Privacy Working Group of the Information Policy Committee of the U.S. Information Infrastructure Task Force,[iv] the U.S. Department of Commerce,[v] and the European Union;[vi] in 1996 by the Canadian Standards Association;[vii] and in 1998 and again this year by the U.S. Federal Trade Commission ("FTC" or "Commission").[viii]

While these sets of privacy principles overlap, they are most noteworthy for the extraordinary variety in both number and content of what each of these organizations considered to be the core principles necessary to safeguard privacy. In addition, it is important to note that all of the privacy principles identified by U.S. bodies have been limited to protecting consumer privacy on the Internet or other electronic networks. No single set of basic principles has been put forward by any U.S. government agency for protecting consumer privacy in all contexts, perhaps reflecting the difficulty of doing so with precision.

The most recent set of privacy principles, and the set on which the WRA has been invited to comment, was put forward by the FTC in its May 2000 report, *Privacy Online: Fair Information Practices in the Electronic Marketplace.* The Commission identified five principles as undergirding the protection of privacy in e-commerce:

1. Notice—data collectors must disclose their information practices before collecting personal information from consumers;
2. Choice—consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;
3. Access—consumers should be able to view and contest the accuracy and completeness of data collected about them;
4. Security—data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use; and

5. Enforcement—the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices.[ix]

While the WRA is generally supportive of these principles in theory, we have four concerns about their use as the basis for new privacy laws. First, the principles' vagueness and their reliance on undefined terms, such as "reliable mechanism," have created uncertainty about how they will be implemented and applied. Second, we are also concerned that Attorneys General or courts may seek to apply to other contexts principles and FTC interpretive statements applicable to, and crafted solely in the context of, one context—the Internet. This is a significant concern given the substantial differences between the online and offline environments. Third, the FTC privacy principles are largely reflected by the private-sector privacy protections that many retailers already employ; the adoption of these principles into law would therefore duplicate or even interfere with existing privacy protections. Fourth, the WRA believes that this set of principles, however defined and applied, is incomplete. We therefore offer below a more complete set of principles for appropriately protecting consumer privacy, together with commentary about how we believe those principles should be applied in practice.

The Missing Privacy Principles

Notice, choice, access, security, and enforcement, depending upon how they are defined and applied, may protect privacy, but they may nevertheless disserve consumers. If the cost of implementing privacy principles causes the price of retail goods to rise without corresponding benefits to consumers, or makes it impossible for retailers to provide the services and convenience that consumers desire, privacy may be marginally protected but consumers will be harmed. Similarly, if government requires privacy protections that are ineffective or burdensome for consumers to use, consumers, commerce, and information flows will all have been burdened, but privacy will not have been advanced. The WRA therefore believes that four additional principles should guide the protection of privacy and the application of the five principles already identified by the FTC: consumer benefit, reasonableness, proportionality, and convenience.

1. Consumer Benefit—Laws and regulations intended to protect consumer privacy should maximize consumer benefits.

Consumers benefit from the efficient flow of personal information. As the Federal Reserve Board ("FRB") noted in its report to Congress on data protection in financial institutions, "it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."[x] Those benefits are shared both by each consumer about whom data are shared and by all consumers in the aggregate because, as FRB Governor Edward Gramlich testified before Congress in July 1999, *"[i]nformation about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy."* The more such information is available, he continued, "the more accurately and efficiently will the economy meet those needs and preferences."[xi] *Without reliable access to personal information, businesses cannot anticipate and meet consumer needs, and consumer service and convenience suffers.*

In 1998 FRB Chairman Alan Greenspan wrote to Congressman Edward J. Markey (D-Mass.):

> A critical component of our ever more finely hewn competitive market system has been the plethora of information on the characteristics of customers both

> businesses and individuals. Such information has enabled producers and marketers to fine tune production schedules to the ever greater demands of our consuming public for diversity and individuality of products and services. . . .
>
> Detailed data obtained from consumers as they seek credit or make product choices help engender the whole set of sensitive price signals that are so essential to the functioning of an advanced information based economy such as ours.[xii]

Unfettered use of personal information benefits consumers not only by allowing businesses to ascertain and meet their needs accurately, rapidly, and efficiently, but also because it:

- enhances customer convenience and service;
- permits consumers to be informed rapidly and at low cost of those opportunities in which they are most likely to be interested;
- improves efficiency and significantly reduces the cost of many products and services;
- facilitates a wide range of payment options, including instant credit;
- allows for real consumer mobility, so that consumers can obtain credit, write checks, enjoy frequent shopper recognition, return goods or have them serviced, and enjoy a wide range of other benefits when they travel or move;
- promotes competition by facilitating the entry of new competitors into established markets, reduces the advantage that large, incumbent firms have over smaller startups, and encourages the creation of businesses specialized in satisfying specific consumer needs; and
- facilitates the detection and prevention of fraud and other crimes.

These are real, tangible benefits that consumers enjoy every day and that are not possible without access to personal information.

Consumers also benefit from having the privacy of confidential or sensitive information protected. *The goal of all privacy law and regulation, therefore, should be achieving a balance between the value of open flow of information and the value of enhanced privacy protection to guarantee for consumers the maximum practicable benefit.* This balance is most likely to be reached if each consumer defines that balance for himself or herself. Consumers who value rapid convenient service more highly than absolute privacy should be free to make that choice. As discussed below, the WRA believes that this is at the very heart of the FTC's choice principle. Therefore, privacy protection tools should give maximum control to individual consumers rather than require the government to decided an appropriate level of privacy protection for all. *Maximizing consumer benefit, then, requires not only that privacy protection be balanced against the benefits that flow from accessible information, but also that the government avoid substituting its judgment for that of individual consumers.*

2. <u>Reasonableness—Laws and regulations intended to protect consumer privacy should be reasonable in their scope and consequences</u>.

Privacy protections, in order to deliver the maximum benefit to consumers, must also be reasonable. The Supreme Court has long asked in the context of constitutional privacy issues, such as Fourth Amendment challenges to government searches and/or seizures: What expectation of privacy is implicated by access and how reasonable is that expectation? When evaluating wiretaps and other seizures of private information, the Court has inquired into whether the data subject in fact expected that the information was private and whether that

expectation was reasonable in the light of past experience and widely shared community values.[xiii] *There should be no interference with information flows to protect privacy interests that are not reasonable.*

The precise determination of what privacy protections are reasonable often depends on the specific context in which they are applied, but courts and commentators have fashioned two bright-line rules to aid in the determination of reasonableness. The WRA recommends that NAAG follow these rules.

a. Information must be nonpublic to be considered private.

First, one longstanding corollary of the principle that the law should protect as "private" only information that one actually and reasonably believes is private, is the concept that private should necessarily mean "nonpublic." *No expectation of privacy may be reasonable if it involves information that is routinely and voluntarily disclosed or is available publicly.* This reflects not only the Supreme Court's interpretation of the Fourth Amendment, but also the common sense that the law should not impose costly or burdensome impediments to the collection and use of information that consumers willingly disclose and that is widely available in the marketplace. To do otherwise results in privacy protections that are nonsensical because they are hopelessly ineffective, contrary to the wishes of individuals, and unnecessary barriers to commerce and customer service.

b. Only information that threatens a specific harm should be regulated.

The second bright-line rule that flows from the reasonableness principle is that *the law should restrict information flows to protect privacy only when a specific harm is actually threatened.* When information poses a demonstrable harm, the value of that flow of information and the cost of restricting it must be measured against the severity of the harm threatened and the likelihood that the harm will actually result. Only when the latter outweighs the former would legally mandated privacy protections be appropriate.

This was the view of the U.S. Court of Appeals for the Tenth Circuit in U.S. West, Inc. v. Federal Communications Commission, which the Supreme Court in June 2000 declined to review, when it struck down the rules of the Federal Communication Commission ("FCC") requiring that telephone companies obtain affirmative consent from their customers before using data about their customers' calling patterns to market products or services to them. The court wrote:

> In the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict *specific and significant harm* on individuals such as undue embarrassment or ridicule or intimidation or harassment or misappropriation of sensitive personal information for the purposes of assuming another's identity. Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under *Central Hudson* [the test applicable to commercial speech] for it is not based on an identified harm.[xiv]

This principle is justified not only by the need to avoid unnecessary restraints on valuable information flows, but also because it is only by identifying the harm that a law is designed to prevent or remedy that a legislator, reviewing court, or citizen can judge whether the law is necessary and whether it does, in fact, respond to that harm.

The requirement that privacy protections respond to specific harms, along with the other principles identified here, heightens the importance of ensuring that privacy laws or regulations apply only where they are intended to—*i.e.*, only where a specific harm would otherwise be threatened.

3. Proportionality—Privacy protection should be commensurate with the harm threatened if personal data are misused.

Not only should privacy protections be designed to maximize consumer benefits, be reasonable, apply only to information that is in fact private, and respond to specific, articulated harms, they must also be proportional to the interest they are designed to serve. As a result, the standards used to protect sensitive medical information about specific individuals should be more rigorous than those applied to consumer preferences regarding clothes or household goods. Only in the former case are the cost and inconvenience imposed by those higher standards justified. *This correctly suggests that no one set of privacy measures will be appropriate in all contexts and that privacy principles should be tailored to the context in which they apply.*

This principle is not only suggested by a common sense regard for the benefits that flow from open information flows, but also is mandated by the First Amendment to the U.S. Constitution. When the government restricts information flows—for whatever purpose—it must do so as narrowly or, in some cases, in the least restrictive way possible. For example, when information is true and obtained lawfully, the Supreme Court repeatedly has held that the state may not restrict its publication without showing that the government's interest in doing so is "compelling" and that the restriction is *no greater than is necessary to achieve that interest.*[xv] Under this standard, the Court has struck down laws restricting the publication of confidential government reports,[xvi] and of the names of judges under investigation,[xvii] juvenile suspects,[xviii] and rape victims.[xix]

Even if the information is considered to be "commercial," its collection and use is nevertheless protected by the First Amendment. The Court has found that such expression, if about lawful activity and not misleading, is protected from government intrusion unless the government can demonstrate a "substantial" public interest, *and that the intrusion "directly advances" that interest and is "narrowly tailored to achieve the desired objective."*[xx] In U.S. West, Inc. v. Federal Communications Commission, the U.S. Court of Appeals for the Tenth Circuit specifically found that (1) the FCC's privacy rules limiting the use of personal information about telephone subscribers restricted speech and therefore were subject to First Amendment review; (2) under the First Amendment, the FCC bore the burden of proving that its rules were constitutional; and (3) that constitutional burden required the FCC to demonstrate that the rules were "'no more extensive than necessary to serve [the stated] interests.'"[xxi] Specifically, the appellate court found that the government's choice of means to protect privacy must reflect "a 'careful calculat[ion of] the costs and benefits associated with the burden on speech imposed by its prohibition.' 'The availability of less burdensome alternatives to reach the stated goal signals that the fit between the legislature's ends and the means chosen to accomplish those ends may be too imprecise to withstand First Amendment scrutiny.'"[xxii] *Proportionality is therefore a constitutional obligation.*

4. Convenience—Privacy protections should be convenient, easy to use, and predictable, and to the extent possible, should reflect reasonable consumer expectations.

The final principle flows naturally from the previous three: Privacy protections should be convenient and easy to use, predictable in their operation and effect, and intuitive to the consumer. If they are not, they inevitably and unnecessarily burden consumers and interfere with consumers obtaining the products and services they want. Very few consumers want to spend time protecting or worrying about their privacy. Privacy protections that force them to do so—that interfere with the rapid, reliable delivery of desired products and services—do not maximize consumer benefits and by definition are not reasonable. As a result, the principles undergirding privacy protection should not fundamentally differ from state to state or from setting to setting, unless something specific about a context justifies a distinction. This of course does not mean that all information will be protected equally, but that the means for protecting privacy, the terms used to describe those means, and the effect of using those means should be similar everywhere.

FTC Privacy Principles in Practice

These four principles—consumer benefit, reasonableness, proportionality, and convenience—not only supplement the FTC's privacy principles, they also provide a more specific understanding of how the FTC's principles should be applied in practice.

1-2. Notice and Choice

Notice and choice are widely regarded as the foundation of consumer privacy protections. Because they are so closely intertwined, we address them together. Unfortunately, despite their importance, the terms are often used imprecisely. This is particularly the case with "choice," which many participants in the current privacy debate use to refer only to whether a consumer consents to the collection and use of personal information and the method by which that consent is sought. The WRA believes that, while choice certainly includes consent (and we address this more specifically below), the choice principle is actually much broader. It includes the consumer's right to make his or her own choice about the proper balance between the value of the open flow of information and the value of enhanced privacy protection, and to act on that choice by choosing among businesses offering different privacy protections. *Choice requires that consumers have the right to choose among competing privacy policies, and obligates the government to preserve to the greatest degree possible a competitive market offering a variety of levels and means (and corresponding costs) of privacy protection.* As a result, the choice principle is central to interpreting all five of the FTC's privacy principles.

One element of choice, as noted, is the concept of consumer consent to the collection and use of personal information and the notice on which that consent is based. The WRA believes that notice and consent should be appropriate to the type of information being collected and used, the setting in which the collection takes place, and the nature of the intended use.

a. No notice or consent required

There are many settings in which U.S. law has already determined that notice of, and consent for, the information collection and use are not necessary and, in fact, may be counterproductive. Virtually anything that can be observed in public may be freely collected without consumer notice or consent. These laws reflect not only the First Amendment's limits on restricting data collection and use, but also broader social values concerning the open flow of

information. To be sure, the law sets some limits on the harmful uses to which that information may be put, but virtually none on the collection and responsible use of such information.

This same pattern is reflected in U.S. data protection law. For example, the Fair Credit Reporting Act imposes many limits on the use to which consumer reports may be put, but virtually no substantive controls on the collection of that information or its appropriate use in commercial markets.[xxiii] This reflects the conclusion that the value of the information being routinely assembled is so great (even to consumers who at the time of its collection might not consent), the cost of providing notice and requiring consent at each point of collection and use so high, and the privacy risk associated with that information's collection and responsible use so low that notice and consent should not be required. The WRA believes that there are many types and uses of information that so maximize consumer benefits and for which providing notice and obtaining consent would be so burdensome on consumers and businesses that the law should not require that notice be provided or that consent be obtained.

Neither notice nor consent should be required for the collection or use of information that is:

- publicly available
- not "personal" or is used only in the aggregate (without being tied to the identity of a specific individual)
- collected or used for security, fraud prevention, law enforcement investigations, or collection purposes
- disclosed to consumer reporting agencies under the Fair Credit Reporting Act[xxiv]
- necessary for the sale or purchase, or negotiation of the sale or purchase, of any portion of a business or the assets of a business
- necessary for analysis of business operations, inventory, auditing, and accounting purposes
- necessary for processing or defending against civil or criminal complaints or for the use of attorneys, investigators, or others protecting the legal interests of the business
- for product safety inquiries and product recalls
- otherwise allowed by law or regulation.

b. Implied notice and consent

For other types of information, when it is clear that personal information is being collected directly from a consumer, notice and consent should be implied from the consumer's choice to provide the information, open an account, or request a product or service. Often the "notice" principle is referred to as the "knowledge" principle, reflecting the fact that what is at issue is not whether the consumer has notice, but rather whether he or she has, or should have, knowledge about the data collection. Where it is clear that the consumer does have that knowledge, additional notice is meaningless.

Moreover, to stop and ask the consumer "did you mean to provide that information you just provided?" would be irritating to the consumer and yield little improvement in privacy protection. In addition, it is meaningless because the requested service or product cannot be provided without the information.

Implied consent is not affected by whether the information is used by a single merchant or whether it is shared among affiliates, closely related companies, licensees, or other businesses that provide a service to the merchant or directly to customers in the merchant's name. Few if

any consumers concern themselves with the corporate structure of the businesses with which they deal. When they provide their information to a company, it does not and should not matter for purposes of privacy protection how that company is organized, or whether it contracts with other businesses to provide the company or its customers with valuable services or products.

In addition, the sharing of information among affiliates and other closely linked companies, licensees, and contracting partners provides consumers with tangible benefits, including:

- customers receive information on products and services based on the consumers' demonstrated preferences;
- the ability of a diversified company to offer the services of one affiliate to the customers of another (for example, a retailer offering its customers the convenience of a credit card offered by an affiliate);
- customers being able to use credit cards issued by one retailer at, or to receive discounts and advance notice of sales and other opportunities from, other companies;
- consolidated account statements and one-call access to information about all of a customer's accounts or transactions;
- convenience of being able to arrange for the purchase, delivery, installation, and maintenance of a product with a single visit or call, and of being able to pay for all four services with one credit card or check;
- customer loyalty programs that allow a shopper to accrue benefits when shopping in more than one chain;
- cost-savings for consumers and businesses because affiliates can share information rather than pay to acquire it separately for each unit; and
- convenience and efficiencies of managing and updating information in a single system (for example, change of address, credit limits or customer preferences) across companies.

Whether a company meets consumer needs through affiliates, divisions, licensees, or contractual relationships with other businesses should not determine the level of privacy protection or dictate whether information may be shared. Notice and consent should therefore be implied whenever personal information is:

- necessary to process a transaction or provide a product or service requested by the customer
- necessary to service or administer a customer account or to resolve a customer complaint
- collected or disclosed at the direction of the customer
- disclosed to or by companies or businesses held by common ownership or under common control ("affiliates")
- collected by or disclosed under a third-party contractual relationship to licensees of a retailer or other contractors offering goods and services in the name or on the behalf of the retailer
- collected or disclosed in connection with a private-label credit card program
- disclosed under a third-party contractual relationship to or by contractors providing services related to a transaction (*e.g.*, delivery, repair, installation, warranty service, fabric protection, order fulfillment, and vendors directly shipping to consumers merchandise purchased from the retailer)

- disclosed under a third-party contractual relationship to or by contractors providing services to the retailer (*e.g.*, a mailing house, marketing company, or database manager), subject to appropriate privacy protections.

c. Available notice and "opt-out" consent

In the majority of other settings, notice should be available, but need not be provided directly to each consumer. Unless particularly sensitive information is involved or a serious harm is threatened, it should be adequate to post a notice or otherwise indicate that a copy of an institution's privacy policy is readily available without charge (for example, on its Web site, via a toll-free number, or at its customer service counters). To require more would burden consumers and increase the cost of providing products and services without achieving any commensurate additional benefit.

Similarly, in the majority of these settings, it is appropriate to give the consumer a reasonable opportunity to "opt-out" of providing information that is not essential to a transaction or of uses that may go beyond what are necessary to complete the transaction. "Opt-out" and "opt-in" both give consumers the final say about whether their information is used. Neither approach gives individuals greater or lesser rights than the other: Under either system, it is the customer alone who makes the final and binding determination about data use. Shifting from an "opt-out" system to an "opt-in" system does not increase privacy protection, yet it imposes significantly higher costs on consumers, businesses, and the economy as it restricts the flow of information on which we all depend. "Opt-out" is therefore an efficient, appropriate tool to let those consumers who choose (historically, a very small number) to express their desire not to allow their personal information to be used to provide them with better service, notice of upcoming opportunities, or other benefits.

In those settings where the social value in having the information is not so great as to remove the choice from the individual and in which consent cannot reasonably be implied, "opt-out" may be an appropriate mechanism for allowing consumers to choose for themselves—rather than have the government choose for them—how much privacy protection they desire. The maxim of the law is that "silence is consent." "Opt-out" reflects this maxim and the expectations of the vast majority of consumers who have responded to repeated surveys and demonstrated by their behavior that they are happy to have their personal information used for appropriate purposes so long as they are given an opportunity to "opt-out."[xxv]

d. Specific notice and "opt-in" consent

When very sensitive information, such as consumer-specific medical information, is involved, or when a specific harm is threatened, specific notice delivered to each consumer and affirmative "opt-in" consent may be required. This may be necessary to ensure that consumers are individually aware that the information is being collected and of the risks that may be presented by the use of that information, and that they did, in fact, consent to the collection and use. These situations are rare but important. Even in these settings, specific notice and "opt-in" are inappropriate if they prove fundamentally unfair or interfere with an important interest such as preventing or detecting fraud or other criminal activity or collecting on an unpaid debt.

Similarly, in a narrow set of contexts when a use *both* is far beyond that disclosed when the information was collected *and* threatens a specific harm, affirmative "opt-in" consent may be appropriate. It must be remembered, however, that "opt-in" is always more costly to administer than "opt-out," inevitably interferes with the provision of consumer services and products and

often makes them more expensive, and burdens consumers. "Opt-in" is an exceptional tool that imposes high costs and harmful unintended consequences, and should therefore be reserved for exceptional situations where the risk of those costs and consequences is justified, such as when young children (*i.e.*, under the age of 13) are involved. This was the recent conclusion of the Tenth Circuit as well: Before employing "opt-in" the government must first demonstrate that "opt-out" is not sufficient to protect against the specified harms that are the target of the privacy protection—a very high burden indeed.[xxvi]

3. Access

Most retailers today provide their customers with extensive access to their account records. To be required to go further as a matter of law threatens consumers in many ways. For example, how does an entity required to provide access to personal information assure that it is providing access to the right person, especially in light of the fact that all of the measures currently available for authenticating identity require that the individual provide even more personal information about themselves? Mandated access inevitably raises the specter of one individual obtaining access to, or even altering, personal information about another individual. Access then becomes the perfect tool for identity theft, and the government that mandates access the unwitting accomplice of identity thieves.

Mandated access may also require businesses to collect, store, and centralize more—not less—personal information. Today, many retailers structure their databases by transaction, rather than by consumer. This allows them to verify payment, collect inventory information, and provide critical information in the event of a product return, recall, service, or maintenance. But information about all transactions is often not brought together or organized on a consumer-by-consumer basis. If the law required access to all of this information, businesses would be compelled as a matter of law to restructure their data operations to bring together disparate sets of information so that it could be accessed on a consumer-by-consumer basis, thereby engaging in a practice that privacy advocates abhor, and greatly increasing both the risk of identity theft and the cost of data operations. In addition, access results not only in increased economic costs, but also in reduced service and convenience, higher prices paid by consumers, and a high volume of litigation over the terms of access and the need for, and adequacy of, corrections.

The WRA therefore believes that new legal requirements concerning access to personal information—in addition to those requirements already in place for access to account information—*should only be required when it is certain to be of sufficient value to warrant the expense and risk for consumers*. Access should only be required to personal information if all of the following four conditions are met. The information:

- identifies a specific individual
- is not publicly available
- is routinely associated with other information about a specific individual (*e.g.*, is organized according to individual, rather than by transaction or date or store)
- could reasonably be used to cause a specific, identified harm to a consumer

In addition, access should never be required where:

- it interferes with an important interest such as preventing or detecting fraud or other criminal activity or collecting on an unpaid debt
- it is fundamentally unfair, such as to personal information being used in a trial (other than through court-ordered discovery)

- it requires the collection or aggregation of additional personal information
- repetitive requests are being used to harass or annoy
- the information was calculated or inferred or where providing access would reveal proprietary business methods or processes
- the cost of providing access clearly outweighs the potential benefits that result from that access.

4. Security

Government regulation is least justified to protect the security of personal information because everyone involved in the responsible collection and use of such data shares a common interest in security. As much as any individual consumer fears he or she may lose if data is intercepted or wrongfully accessed, businesses also stand to lose if their databases are "hacked" or accessed inappropriately. This is why businesses have invested so heavily in security for information.

Moreover, the greatest threat to the security of stored personal information is not the business that is maintaining the information, but rather the consumer who is providing it. For example, online security experts argue that the greatest threats to the security of most Internet transactions is the consumer disclosing his or her password or leaving his or her system logged on to a network. As a result, consumer education—rather than new laws—may be the most critical component of data security. Laws applicable to retailers and other businesses would do little if anything to enhance security, and therefore would impose unnecessary costs on consumers and businesses alike.

In addition, security today is largely the result of technologies, which are rapidly changing. Any law or regulation that specified a specific security measured would be out of date before it ever took effect. Therefore, the effect of such a law or regulation would be, at worst, to decrease the standard of security for stored data or, at best, to increase the cost of protecting those data.

Finally, the WRA is concerned about how security is to be measured. The FTC itself ran into this problem during its most recent survey of corporate Web policies. The Commission staff treated a Web site as having adequate security if it contained a policy saying that it did.[xxvii] This may give comfort to consumers and government regulators, but it does little for enhancing consumer security.

Therefore, the WRA recommends against the adoption of laws or regulations attempting to require a specified security standard. This does not mean that retailers in any way lack commitment to protecting the security of the personal information they collect and store, but rather that we are already so committed to this task that no law or regulation could meaningfully enhance the security we already provide.

5. Enforcement

Enforcement should be designed to enhance consumer benefits at the least cost and burden to consumers and businesses as possible. Privacy is an area where a strong incentive is hardly necessary, because businesses already face such significant penalties in the nature of lost customer confidence and intensive press scrutiny if they fail to live up to their own privacy policies or to protect their customers' information.

Moreover, this is an area where many laws—ranging from the privacy provisions in the Gramm-Leach-Bliley Financial Services Modernization Act[xxviii] to general consumer protection laws such as Section 5 of the Federal Trade Commission Act[xxix]—already apply. A single use of personal information can become the subject of dozens of enforcement actions brought under a variety of laws. For example, the decision by network advertiser DoubleClick to purchase consumer database company Abacus has resulted in an FTC investigation and 15 individual and class action lawsuits. This type of enforcement scenario merely raises costs without in any way aiding consumers or enhancing compliance.

Therefore, the WRA believes that enforcement of privacy protections should, wherever possible, be through means other than resort to the courts, such as self-regulatory organizations. These alternatives are often less costly and more accessible for consumers, respond more quickly to changing circumstances, and yield faster decisions than traditional lawsuits.

When recourse to the courts is necessary, the WRA believes that enforcement should be through states Attorneys General, the FTC, or other government agencies, rather than through private actions. Private actions are often spurious, but they are nonetheless very expensive to defend, especially when brought seriatim. Moreover, while they are rarely successful, when they do succeed, they often result in unreasonably high judgments which are not commensurate with the alleged violation, and create little additional incentive to protect privacy while dramatically increasing the costs paid by, or eliminating the services offered to, other consumers. Finally, such actions enrich a single or a handful of consumers (or, more likely, their attorneys), at the expense of all other consumers.

Finally, where multiple legal requirements overlap, enforcement under all of those laws and regulations should take place through a single action. Moreover, compliance with the most restrictive of those requirements should constitute compliance with all of the lesser requirements.

Other Issues Concerning the Practical Application of Privacy Principles

The WRA proposes two additional principles concerning the role of the government in general, and of the States in particular, in enacting and enforcing privacy protections that we believe flow from the consumer benefit, reasonableness, proportionality, and convenience principles identified above, but that are not addressed by the five principles identified by the FTC.

1. Preemption

The States have played an historically important role in the development of laws, often serving as "laboratories" for legal regimes that are tested at the state level before being implemented nationally. In the case of personal privacy, however, the WRA believes that the States have a very limited role to play in creating new laws. Commerce in this country is inherently national and, especially with the advent of the World Wide Web, global. Many retailers operate in multiple states and would be greatly burdened by the need to comply with inconsistent privacy obligations. Moreover, consumers are increasingly mobile and, even those who live and work in a single State for an extended period of time, increasingly obtain products and services from across state lines. Moreover, the exponential growth in online commerce means not only that more consumers are making purchases via the Internet, but that online and offline transactions are increasingly interconnected. For example, a consumer may visit a retailer's Web site to find information about a product or service, but may make the purchase in a bricks and mortar store. Or a consumer may use the Web to access information about his or her

store account or to schedule a delivery, again, even though all purchases are made in the offline world.

If consumers are to be served effectively and efficiently, privacy rules need to apply across technological contexts and geographic boundaries. It is counterintuitive to the consumer, and costly and burdensome to a business, to face 51 inconsistent privacy laws. The cost of compliance not only results in higher prices paid by consumers, but also may threaten the very viability of that consumer service. *The WRA therefore believes that to the extent laws are necessary to enhance consumer privacy protection, those laws should be national in scope, and should preempt state laws on the same subject matter.* Neither consumers nor businesses are served by any other approach.

There may, of course, be exceptions to this general preemption principle. For example, we recognize that each State should retain the right to control access to state public records, consistent with the First Amendment. The WRA therefore lament passage of federal laws like the 1994 Drivers' Privacy Protection Act[xxx] and the Shelby Amendment to the 1999 Transportation Appropriations Act[xxxi] that intrude into rights of States.

Moreover, the WRA believes that States can and should continue to play a critical role in advising the federal government on appropriate privacy protection. We therefore applaud this current effort by states Attorneys General to identify those privacy principles that should undergird *federal* privacy protection.

Finally, the WRA recognizes that consumers are served by States retaining appropriate enforcement authority along with federal agencies under federal privacy laws. Much like enforcement authority is shared by states Attorneys General with the FTC under the Telemarketing Sales Rules[xxxii] and the Fair Credit Reporting Act,[xxxiii] the WRA believes that shared enforcement authority under other federal privacy laws is also in the public interest.

2. Interaction of Overlapping Laws

Despite preemption, retailers and other businesses are subject to a growing number of laws and regulations designed to enhance personal privacy. These laws and regulations impose a variety of legal requirements on businesses, many of which are either duplicative or inconsistent. Consumers are not served by overlapping legal obligations: Privacy protections that are duplicative or inconsistent do not enhance privacy, but they greatly increase the cost of compliance. Therefore, such laws and regulations require consumers to pay more for the same level of protection.

The WRA believes that it is the obligation of States and of the federal government to avoid enacting laws and regulations that merely duplicate or, worse, conflict with existing privacy protections. Where such overlapping obligations already exist, we believe that States and the federal government should work to eliminate them and should avoid enforcing more than one set of obligations against the same party for the same conduct. Finally, as noted above, the WRA recommends that compliance with the most restrictive of overlapping requirements should constitute compliance with all of the lesser requirements.

Conclusion

The FTC's five privacy principles—notice, choice, access, security, and enforcement—are an important beginning to crafting appropriate privacy protection for

consumer information. But it is critical to remember that these principles are deliberately vague and therefore subject to a wide variety of interpretations; that the FTC crafted them only for online commerce; and that, even for that limited context, they are not sufficient for ensuring either that consumers' privacy is protected or that other important consumer interests are served. Four additional principles—consumer benefit, reasonableness, proportionality, and convenience—are necessary to interpret the FTC's principles and ensure that consumer interests are fully served. To these nine principles must also be added two additional principles specifically concerning the role of the government in general, and of the States in particular, in enacting and enforcing privacy protections—preemption and the interaction of overlapping obligations.

Finally, the WRA wishes to stress that retailers already protect the privacy of their customers' information far more than any law or regulation requires. Such protection reflects retailers' own best interest in guarding against misappropriation or misuse of valuable data, strengthening customer relationships, and avoiding public criticism by consumer groups and the press. Moreover, the protection of privacy is an important element of many retailers' strategy for competing with each other and with other industries for consumers in the marketplace. We believe that the greatest threat to consumer privacy today comes not from responsible businesses with significant investments in their reputations and customer relationships, but rather from the government and criminals (often individuals operating offshore, masquerading as reputable businesses on the Internet), neither of which will be affected by new privacy laws and regulations. We strongly encourage NAAG to avoid proposing new laws or regulations that merely duplicate existing requirements or private-sector protections, or that burden responsible, law-abiding retailers and their customers in a well-intentioned but misfocused effort to control the behavior of other industries or parties.

NOTES

i. U.S. Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens* (1973).

ii. U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977).

iii. Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

iv. U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995).

v. U.S. Department of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995).

vi. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Eur. O.J. 95/L281) (1995).

vii. Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

viii. Federal Trade Commission, *Privacy Online: A Report to Congress* (1998); *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress* (2000).

ix. *Privacy Online: Fair Information Practices in the Electronic Marketplace, supra* at 4.

x. Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 2 (1997).

xi. Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 21, 1999) (statement of Edward M. Gramlich).

xii. Letter from Alan Greenspan to Edward J. Markey, July 28, 1998 (available at http://www.house.gov/markey/980728letterr.htm).

xiii. Katz v. United States,389 U.S. 347, 361 (1967) (Harlan, J., concurring); Terry v. Ohio, 392 U.S. 1, 9 (1968); Smith v. Maryland, 442 U.S. 735, 740 (1979).

xiv. U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 120 S. Ct. 1240 (2000) (emphasis added).

xv. Florida Star v. B.J.F., 491 U.S. 524 (1989); Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979); Landmark Communications Inc. v. Virginia, 435 U.S. 829 (1978); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

xvi. New York Times Co. v. United States, 403 U.S. 713 (1971).

xvii. Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978).

xviii. Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).

xix. Florida Star v. B.J.F., 491 U.S. 524 (1989); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

xx. Central Hudson Gas & Electric Corp. v. Public Service Comm'n, 447 U.S. 557, 566 (1980); Board of Trustees v. Fox, 492 U.S. 469, 480 (1989) (emphasis added).

xxi. 182 F.2d at 1235, quoting Rubin v. Coors Brewing Co., 514 U.S. 476, 486 (1995).

xxii. Id., quoting Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 417 (1993), and 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 529 (1996) (O'Connor, J., concurring) (citations omitted).

xxiii. 15 U.S.C. §§ 1681-1681t.

xxiv. Id.

xxv. *See, e.g.*, Personalized Marketing and Privacy on the Net: What Consumers Want, A Privacy & American Business Consumer Privacy Survey Questionnaire (Development and Report by Dr. Alan F. Westin, Fieldwork and Data Preparation by Opinion Research Corporation) (Nov. 1999). More than two-thirds of U.S. consumers—132 million adults—took advantage of direct marketing opportunities in 1998, accounting for more than $1.3 trillion in sales of goods and services. Direct Marketing Association, *Economic Impact: U.S. Direct Marketing Today* (4th ed.), 1998. The Direct Marketing Association provides a convenient way for consumers to "opt-out" of the use of their personal information by member companies. Over the past decade, however, fewer than 3 percent of U.S. adults availed themselves of that opportunity. Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 21, 1999) (statement of Richard A. Barton).

xxvi. U.S. West, 182 F.3d 1224.

xxvii. *Privacy Online: Fair Information Practices in the Electronic Marketplace, supra* at 18-19.

xxviii. Gramm-Leach-Bliley Financial Services Modernization Act (S. 900), 106 Pub. L. No. 102, 113 Stat. 1338, tit.V (1999).

xxix. 15 U.S.C. § 45(a).

xxx. Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified at 18 U.S.C. §§ 2721-2725).

xxxi. Department of Transportation and Related Agencies Appropriations Act, 2000, § 350, 106 Pub. L. No. 69, 113 Stat. 986 (1999).

xxxii. 16 C.F.R. § 310.7.

xxxiii. 15 U.S.C. § 1681s(c).