Know The Rules
Use The Tools

Privacy in the Digital Age:
A Resource for Internet Users

U.S. Senate Judiciary Committee
Orrin G. Hatch, Chairman

http://judiciary.senate.gov/privacy.htm

United States Senate

Dear Friends:

At any given moment, millions and millions of clickstreams are taking place all over the Web. As we conduct more of our daily activities on the Internet, from shopping to banking, information is constantly being gathered about us and our online behavior. Over the past several months, I have heard from many individuals who have expressed to me their growing concerns about the vulnerability of their private information on the Internet. At the same time, many businesses have shared with me the concern that ill-advised government regulation could interfere with the development of new technologies and hinder the expansion of the electronic marketplace.

The Internet industry needs to continue to take an active role in self-regulation, and I commend the industry for its efforts to date. The industry has taken a number of steps, through privacy seal programs and self-regulatory consortiums, to adopt standards to protect online privacy, such as the industry initiative known as P3P, which was publicly tested recently. P3P is intended to enable consumers to better control the release of their personally identifiable information on the Internet by automating the comparison of individual users' privacy preferences with the privacy practices of websites. I also praise the private sector for projects such as the Privacy Leadership Initiative announced recently, which involves executives from a wide range of companies, and which is intended to give consumers more control with respect to their online privacy through technology, company privacy practices, research and education.

I believe that by ensuring the protection of both individual privacy and the integrity of the Internet, consumer confidence will be enhanced and e-commerce can reach its astounding potential. I am committed to protecting consumers by curbing the fraudulent collection and dissemination of sensitive personal information, and to educating consumers about online privacy.

It is my hope that with greater awareness of how their personal information can be collected online and used, along with an understanding of the resources and technological tools available to them, consumers will be empowered to protect the privacy of their personal information in accordance with their individual needs. I also hope that once informed about this issue, consumers can begin to demand the level of privacy protection they desire from Internet businesses. This would enable the marketplace, rather than burdensome

government regulation to address privacy concerns. In addition, I encourage Internet companies to take an increasing role in educating the public about online privacy and to continue to make positive strides in respecting individual privacy preferences and expectations. Meaningful self-regulation by the industry, with the support of government enforcement against bad actors, is essential to avoiding heavy-handed government regulation in this area.

This handbook provides Internet users with information about protecting online privacy, including some of the resources and technological solutions available. With better informed Internet users and responsible conduct by Internet companies, we can all benefit from a prospering digital economy.

The Internet has had and will continue to have a profound impact on the way we live our daily lives. Along with the enormous promise of the digital age comes the responsibility each of us must accept to understand this medium and to take the necessary steps to ensure our safety and comfort in it. I hope consumers will find this handbook a good starting place for becoming more informed about online privacy and the options that are available for protecting it.
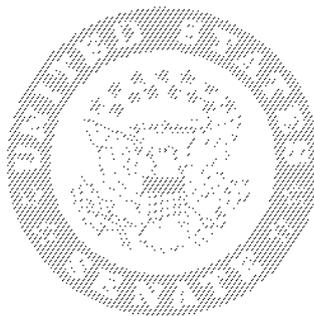
Sincerely,

Orrin G. Hatch
Chairman

Table of Contents:

Know The Rules Use The Tools

*Privacy in the Digital Age:
A Resource for Internet Users*

http://judiciary.senate.gov/privacy.htm

EXECUTIVE SUMMARY

The Senate Judiciary Committee, chaired by Senator Orrin G. Hatch, intends to continue to examine and develop public policy that considers the needs of consumers, law enforcement and online businesses; ensures continued investment in technological development in this important area; and enables e-commerce to reach its full potential. In furtherance of this goal, and in an effort to provide timely information, Senator Hatch has issued the following resource guide for consumers.

With online sales in the billions of dollars, it is clear that many consumers have embraced the digital marketplace. Retail electronic commerce (or "e-commerce") sales reached an astounding $5.3 billion in the first quarter of 2000. Analysts predict that online shopping could grow to $78 billion per year by 2003. With more than a third of all households in the United States online, consumers increasingly are using the Internet to conduct daily activities ranging from filling their prescriptions to personal banking to trading stocks. At the same time, businesses have recognized the tremendous potential the digital marketplace offers.

Yet, as Microsoft, a leader of the new economy, stated in an advertisement entitled "Happy e-Holidays," it is apparent that "not everyone is sold on Internet shopping. Still, many people are worried about sharing their credit card and other personal information over the Internet." The Senate Judiciary Committee staff finds that certain conduct is taking place online that could threaten to chill the continued rapid expansion of the digital marketplace: the extensive collection by websites of personally identifiable information about consumers, often without consumers' consent or knowledge.

• **First, Committee staff finds that many consumers are unaware that personally identifiable information is being collected about them while they surf the Net. For example, a recent study found that among *heavy Internet users*, 12 percent were uncertain about what a "cookie" was (a cookie is an electronic tag placed on an individual's hard drive by an Internet site to identify the individual while he surfs the Internet).**

• **Second, Committee staff finds that consumers are concerned about the collection and use of personally identifiable information. A study found that 87 percent of individuals using the Internet are concerned about threats to their personal privacy.**

• **Third, Committee staff finds that most consumers are not aware of technological tools and resources that are available to empower them to protect their privacy.**

• **Fourth, Committee staff finds that the expansion of e-commerce may be jeopardized if consumer concerns are not adequately addressed. A study conducted by the National League of Cities found that among Internet users who research products or services online (42 percent of all Internet users), only 24 percent actually purchase products or services online. The same study found that 73 percent of Internet users are not comfortable providing credit card or financial information to businesses online, and 70 percent are not comfortable providing personal information.**

Most Websites Collect Users' Information

The vast majority of websites collect personally identifiable information from consumers. Increasingly, these websites are posting privacy policies – statements that inform the consumer of the type of information the website collects and to whom such information is sold. Moreover, a number of individual companies have taken steps to respond to privacy concerns by asking for affirmative consent from consumers before collecting and selling personally identifiable information.

Consumer Education is Critical

To protect individual privacy online, consumers must understand at the outset whether websites collect personally identifiable information, and if so, the extent to which the websites use personally identifiable information. Consumers also must understand whether websites implement privacy policies, and if so, whether those policies protect or compromise individual privacy. In addition, consumers need an awareness of the various resources and technological tools that are available to them for protecting their online privacy. With this knowledge, consumers can make an informed judgment about whether to provide information requested by a particular website.

Resources Available to Consumers

A number of resources are available to consumers who want to protect their online privacy. Groups involved in the debate over online privacy, such as the Direct Marketing Association, the Electronic Privacy Information

Center, the Internet Alliance, the Online Privacy Alliance, the Platform for Privacy Preferences, and the Privacy Rights Clearinghouse, provide helpful information. Consumers may further protect their privacy online by utilizing websites that adhere to "seal programs," such as TRUSTe, BBB*Online*, CPA WebTrust, and Enonymous.com, which are independent, third-party organizations that monitor and/or rate the privacy practices of websites.

Technology Tools Can Empower Consumers

Consumers can be empowered to protect their privacy by understanding the technological tools that are available to safeguard their personally identifiable information. For example, consumers can take advantage of existing technologies (1) to alert them when a cookie is being placed on their hard drive by a website, or (2) to block or remove the placement of an unwanted cookie altogether. With both Netscape Navigator and Internet Explorer, the two leading Internet browsers, a consumer can choose to have an "alert box" flash on the screen to inform him whenever a server is trying to place a cookie on his system. Consumers can employ various software packages, such as NSClean, IEClean, AdSubtract, Cookie Cruncher, Cookie Jar 2.0, and Internet Junkbuster Proxy to filter and block cookies in accordance with a consumers' individual preferences.

Various consumer information is instantly available to websites when consumers visit them. To prevent the flow of this information, consumers can use "identity scrubbers" (such as Anonymizer, Crowds and Enonymous), which are tools developed to allow Internet users to remain anonymous while surfing the Internet. Consumers also can use technologies known as digital identity managers or preference organizers (like Digitalme or MS Passport) to better control the manner in which their information is shared, used, and maintained online.

Consumers can assert greater control over their personally identifiable information by using infomediaries, which typically are websites that act as a "go-between" for consumers who visit websites but want to control the personally identifiable information that is shared at each website they visit. Some infomediaries operate by having the consumer create a detailed personal profile; the infomediary then negotiates with websites over the release of his personal information.

Furthermore, technologies exist to enable consumers to trade their personal information for something the consumer finds valuable, such as

product offers and information, sweepstakes entries, or cash. An example of this kind of consensual trading of information trading is called "permission marketing," such as that provided by Yesmail and Brodia, in which the consumer provides personal information in order to receive offers and buying information on products and services in his areas of interest.

Technologies Available to Businesses to Respect Consumer Privacy

Some tools enable online businesses that collect consumer information to ensure respect for consumer preferences with respect to personally identifiable information. One area of privacy concern is online advertisement delivery, in which massive, sophisticated and detailed databases of customer profiles are developed that enable highly targeted advertising. To the extent that some advertisement delivery services keep consumer information impersonal (identifying consumer profiles by number rather than by name, for example) consumers can maintain a certain level of anonymity and privacy protection while receiving valuable advertising information. Customer relationship management software provides highly-targeted marketing based on a consumer's buying habits. This software can be provided, however, with services and software to implement personal data protection, including consumer choice (opt-in or opt-out), auditing, and security. While it is up to online businesses to implement these business-to-business tools, consumers – armed with information – can demand that retailers use such tools and respect their privacy preferences.

Avoiding Heavy-Handed Government Regulation

Consumer confidence in e-commerce will permit our digital economy to continue to grow and thrive. Consumer confidence in e-commerce will increase as consumers learn about and use the tools that are available to protect their privacy online to the extent they want. Online businesses and the government can help by continuing to educate consumers regarding the manner in which personally identifiable information is collected and how it is used. In addition, online businesses must continue to develop and post meaningful privacy policies, undertake measures to respond to consumer concerns about privacy, and engage in meaningful self-regulation in order to avoid heavy-handed government regulation.

Know The Rules Use The Tools

Privacy in The Digital Age: A Resource for Internet Users

http://judiciary.senate.gov/privacy.htm
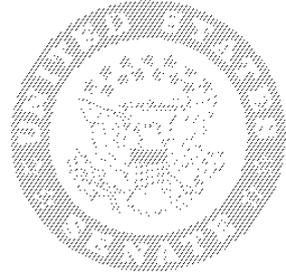
I. INTRODUCTION.

Internet usage has grown remarkably in recent years. More than 80 million American consumers are using the Internet. Over one-third of all households in the United States are "online"—the top two ranked websites, Yahoo and AOL, averaged approximately 30 million visitors every month during the first quarter of 1999, and more than 150,000 new domain names are registered every week.[1] The Internet is providing more and more consumers with a new and unparalleled digital marketplace. In this digital marketplace, consumers have the opportunity to conduct a wide variety of online activities, from buying books and filling prescriptions to banking, trading stocks, listening to music and participating in auctions. The United States Department of Commerce announced that online sales tripled from approximately $3 billion in 1997 to approximately $9 billion in 1998.[2] "During the first quarter of 1999, fifty-six million individuals (70 percent of the online population) shopped online, and 23.5 million (28 percent of the online population) made at least one purchase."[3] The Census Bureau reported that e-commerce sales were $5.3 billion in the first quarter of 2000.[4] Analysts predict that online shopping could grow to $78 billion a year by the year 2003.[5]

With this unprecedented explosion of commerce on the Internet (sometimes referred to as "e-commerce") attention is being drawn to the issue of online privacy. This report assesses the current state of privacy on the Internet and provides information regarding technological tools that are designed to safeguard individual privacy when using the Internet.

---

[1] *See* Erran Carmel, et al., *The Digital Economy Fact Book* (1st ed. 1999); *see also* www.pff.org.

[2] *See* Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress* (1999).

[3] *See* Carmel, supra note 1; see also www.pff.org.

[4] *See* http://www.census.gov/mrts/www.current.html.

[5] *See* Carmel, *supra* note 1; *see also* www.pff.org.

II. THE ONLINE PRIVACY ISSUE.

A. What Is Online Privacy?

Companies are able, because of recent technological advances, to collect a vast amount of personally identifiable information about online consumers, often without that consumer's knowledge or consent.[6] For example, Internet websites can collect a range of personal information from individuals who visit their websites through registration and survey forms, as well as through tracking software called "cookies" that record an individual's preferences and buying habits. With "nearly all transactions computerized, the Internet makes it easy for corporate and public computers to merge their files—compiling financial, consumer, medical, legal, lifestyle, and public information" on individuals.[7]

Consumers are beginning to express concern about the collection of personal information and the use to which such information will be put. For example, a recent survey shows that a major concern among consumers who provide personal information on the Internet is whether that information will be shared with third parties and, if so, whether it will be provided in a personally identifiable way.[8] Another survey indicates that 64 percent of consumers are unlikely to trust a website even if the site has posted a privacy policy statement.[9] Some consumers are so fearful of losing their privacy that they avoid engaging in e-commerce altogether.[10] When Jupiter Strategic Planning services recently asked consumers to "identify the top two factors that would positively affect their trust in websites with regard to their privacy,"[11] an alarming 37 percent responded that they "simply did not trust websites with their privacy." According to a FOX News Opinion poll conducted June 7-8 and released June 26, 2000, 69 percent of respondents said that they are "very" concerned about their ability to keep things such as medical or financial records private, and 90 percent said that it is getting harder to keep such information confidential. If consumer concerns about online privacy are not adequately addressed, then consumers will be less likely to use the Internet, whether for information or commerce, and the ability of the Internet and the commerce conducted on it to reach its maximum potential will be hampered. If this were to hap-

---

[6] *See* Michael deCourcy Hinds, *Protecting Our Rights: What Goes on the Internet?* (Nat'l Issues Forums 1999).

[7] *See id.*

[8] *See* Lorrie Faith Cranor, et al., *Beyond Concern: Understanding Net Users' Attitudes about Online Privacy* (AT&T Apr. 14, 1999) (available at http://www.research.att.com/projects/privacystudy).

[9] Jupiter Communications, *Proactive Online Privacy, Scripting an Informed Dialogue to Allay Consumers' Fears* (June 1999).

[10] *See* Hinds, *supra* note 6.

[11] *See* Jupiter, *supra* note 9.

pen, today's online privacy "concerns" could become an unfortunate online privacy "problem."

B. An Old Problem With A New Twist.

The risk to privacy resulting from the collection of personally identifiable information is not new. The collection of personal information and the tracking of customer preferences has occurred for many years in many settings. For example, when a consumer calls a toll free number, or when a business uses caller ID technology, the consumer's telephone number is revealed to the business. Additionally, buying habits are recorded in a host of contexts, such as when consumers place catalog orders, make purchases utilizing credit cards, fill prescriptions, and join grocery store customer loyalty clubs. Thus, the privacy concerns that stem from the collection of personally identifiable information are not new and are not caused by the Internet. However, the facility with which the Internet and other new communication technologies enable the collection of such information to occur, along with the rapid growth of e-commerce, has prompted enhanced scrutiny of this privacy issue. Some have expressed concerns that:

the automated collection and distribution of personal information is forcing Americans to live in a virtual fishbowl. The increased acces-sibility, on the Internet, of personal details about our lives will erode other American liberties: people will think twice before consulting a doctor, joining a political organization, or sending e-mail, when the information winds up in an online database.[12]

C. Online Privacy Distinguished From Online Security.

"Online privacy" is sometimes erroneously used in the media to describe what actually is "online security." Online privacy and online security are distinct. Online privacy concerns often arise through a website operator's collection and dissemination of personally identifiable information about an individual consumer who has visited the particular website. Specifically, privacy concerns arise when consumers' personally identifiable information is collected online without the consumers' consent or knowledge and/or is sold to third parties without their consent or knowledge. Thus, online "privacy" relates to the affirmative conduct of the website visited by the consumer.

In contrast, online "security" relates to the integrity of the entire Internet infrastructure (including individual websites) and the system's ability to secure against the conduct of unauthorized third parties, such as hackers, who attempt to access the website's stored information which could include a consumer's person-

---

[12] *See* Hinds, *supra* note 6.

ally identifiable information. While the Committee also is committed to ensuring the security and integrity of the Internet, this report specifically addresses consumer concerns related to "privacy" rather than to security.

D. What are "Cookies," and How Do They Impact Online Privacy?

Many consumers have the mistaken impression that their conduct on the Internet is anonymous. This is often not the case. Many websites utilize various technologies, such as "cookies," to collect information from consumers as they visit the website. "Cookies" are electronic tags that are placed on the hard drive of an individual user's computer by Internet sites while the individual is on the Internet. Cookies can store information about the individual user, such as the user's name, credit card numbers, websites visited, e-mail addresses, personal preferences or spending patterns.[13] Although, this information generally is collected and stored (on the hard drive in a cookie file), and is used benignly to personalize a consumer's visit to a website, it is often collected without the knowledge or consent of the user. Once a cookie is in place, the user's Internet browser checks every time the user visits a particular site to see if there are any cookies for that site. If there are, the browser sends the

cookie information to the site.

The Cookie Central[14] website provides a brief outline of the different ways companies utilize cookie technology:

• Targeted Marketing: Cookies allow sites to build a profile on where individuals go while on the Internet, the advertisements they click on, and their primary interests, and then target specific advertisements to particular consumers based on the profile.

• Website Tracking: Using cookies allows sites to track where consumers go while on the web, enables them to count accurately how many people have visited a site (distinguishing between 25 individuals and one person hitting the reload button), and lets sites see which users may have left the site because there were no interesting links.

• Online Ordering Systems: Known as "shopping baskets," some cookies store information on individual buying preferences. When a consumer enters a site and spends time selecting items but exits abruptly without ordering, the items selected will be stored in cookies for weeks or even years.

• Site Personalization: Cookies also are used to customize websites, such as news sites, for the user. These cookies allow a user to select articles in subject areas of interest, such as news or sports.[15]

---

[13] For additional information on "cookies" and how to determine whether they are on your hard drive, *see* http://www.w3.org/Security/faq/wwwsf7.html#Q66.

[14] *See* www.cookiecentral.com/cm002.htm.

[15] *See* www.cookiecentral.com.

In addition to these widely used and often beneficial applications of cookie technology, other uses are conceivable and have been reported. For example, cookie technology could track and enable the sale of information regarding an individual's Internet research on sensitive matters, such as a medical condition.

The World Wide Web Consortium has explained:

Cookies cannot be used to "steal" information about you or your computer system. They can only be used to store information that you have provided at some point. To give a benign example, if you fill out a form giving your favorite color, a server can turn this information into a cookie and send it to your browser. The next time you contact the site, your browser will return the cookie, allowing the server to alter background color of its pages to suit your preferences.

However cookies can be used for more controversial purposes. Each access your browser makes to a website leaves some information about you behind, creating a gossamer trail across the Internet. Among the tidbits of data left along this trail are the name and IP address of your computer, the brand of browser you're using, the operating system you're running, the URL of the Web page you accessed, and the URL of the page you were last viewing. Without cookies, it would be nearly impossible for anyone to follow this trail systematically to learn much about your web browsing habits. They would have to reconstruct your path by correlating hundreds or thousands of individual server logs. With cookies, the situation changes considerably.[16]

E. What Do Consumers Think About Online Privacy?

Over the past year, a number of studies have provided insight into consumers' sentiment regarding online privacy. From these studies, it is apparent that while consumers generally are concerned about online privacy, they largely are unaware of the collection of personally identifiable information about them that is gathered online.

A recent survey conducted by AT&T indicates that 87 percent of individuals using the Internet are concerned about threats to their personal privacy.[17] A national study by the American Association of Retired Persons in 1998 found that 91 percent of members age 50-69 would mind if personal information about them was sold by a website, with 81 percent of older members, ages 70 and above, objecting to the sale of their personal information.[18] On the other hand, a survey conducted by

---

[16] *See* http://www.w3.org/Security/faq/wwwsf7.html#Q66.

[17] *See* Cranor, *supra* note 8.

[18] *See* Public Policy Institute, *AARP (American Association of Retired Persons), Members' Concern About Information Privacy,* Data Digest No. 39, (February 1998).

Jupiter Communications indicated that 78 percent of individuals were primarily concerned about the security of their credit card information, with only 58 percent of the individuals primarily concerned with any type of third-party information selling.[19] This same survey revealed a lack of consensus on the specific online privacy concerns that consumers consider most important, with "third-party information selling," "anonymity," and "information selling without identifying data" all registering as concerns of consumers. A study by the Center for Democracy and Technology found that 42 percent believed the sale of personal information is the most pressing issue.[20]

Fifty-two percent of respondents to a recent survey of heavy Internet users indicated that they were concerned about cookies and 56 percent said they had changed their cookie settings to something other than accepting all cookies without warning.[21]

However, it is important to note that 78 percent of respondents said they would definitely or probably agree to websites using persistent identifiers to provide a customized service; while 60 percent would agree to the use of such an identifier to provide customized advertising.

Statistics indicate that consumers use the Internet to research products but are hesitant to purchase products. The National Consumers League states that 42 percent of Internet users do so to research products or services, while only 24 percent of those individuals actually purchase products or services online.[22] The same study shows that 73 percent of Internet users are uncomfortable providing credit card or financial information to businesses online, and 70 percent are uncomfortable providing personal information.[23] Consumer reluctance to disclose credit card information to online retailers ("e-tailers"), presents a challenge to e-commerce because there is not yet a true cash-equivalent available on the Internet. In the physical world, consumers can make purchases with a variety of payment options, and for the greatest amount of privacy, a consumer can use cash, which requires no disclosure of personal information. In contrast, anonymity is not available when making a credit card purchase—the primary means of payment on the Internet—because the purchaser, the item purchased, and the time and date of the transaction are all recorded.[24]

Consumer fears appear to continue to be a hindrance to the unfettered expansion of e-commerce. As consumers become more aware of the privacy issues implicated by the use of the Internet and begin to understand the ramifications of the collection of personally identifiable information, the

[19] *See* Jupiter, *supra* note 4.
[20] *See* Center for Democracy and Technology, *Behind the Numbers: Privacy Practices on the Web (1998); see also* http://www.cdt.org/privacy/990727privacy.pdf.
[21] *See* Cranor, supra note 8.
[22] *See* Louis Harris & Associates, Inc., National Consumers League, *1999 National Consumers League, Consumers and the 21st Century* (1999) (available at www.natlconsumersleague.org/FNLSUM1.PDF).
[23] *See id.*
[24] *See* Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 Nova L. Rev. 13 (1998).

expansion of e-commerce could be further jeopardized, unless consumer concerns are adequately addressed.

III. WHAT IS BEING DONE TO ADDRESS CONCERNS ABOUT ONLINE PRIVACY?

A. Senate Judiciary Committee Work.

The Senate Judiciary Committee held its first hearing on April 21, 1999, entitled "Privacy in the Digital Age: Discussion of Issues Surrounding the Internet."[25] Six distinguished experts in the field of Internet privacy and technology testified: Katherine Borsecnik, Vice President of Strategic Business at America Online; Michael Sheridan, Vice President for Strategic Business at Novell, Inc.; Dr. Irving Wladawsky-Berger, General Manager of IBM's Internet Division; Jerry Berman, Executive Director of the Center for Democracy and Technology; Russell Bodoff, Senior Vice President and Chief Operating Officer of the BBBOnline; and Greg Fischbach, Chairman and CEO of Acclaim Entertainment.

The purpose of the hearing was to educate the public and congressional members on the privacy issues surrounding consumer use of the Internet, and to begin a dialogue with those having an interest in privacy issues. Ultimately, the Committee seeks to facilitate a development of a public policy that takes into consideration the needs of consumers, law enforcement and industry, and that ensures continued technological development in this important area and enables electronic commerce to reach its full potential.

In his statement before the Committee, Chairman Hatch encouraged government, industry and consumer groups to work together to address consumers' concerns regarding privacy on the Internet and to ensure that new digital technology reaches its full potential:

As Americans spend more of their lives on the Internet, they are more concerned about the ability of Websites, both government and commercial, to track their "digital steps." There is no question that in order for the Internet to reach its maximum potential as a viable avenue for transacting commerce, consumers must be assured that personally identifiable information that is collected online is afforded adequate levels of protection. But the question remains how do we best do that. How do we do it without chilling the development of new technologies or the expansion of the marketplace?[26]

There already have been over 50

[25] http://www.senate.gov/~judiciary/.
[26] *See* Statement of Orrin G. Hatch Before the United States Senate Committee on the Judiciary, "Privacy in the Digital Age: Discussion of Issues Surrounding the Internet," (Apr. 21, 1999) (attached hereto as appendix "A").

legislative proposals offered in the Senate and the House of Representatives addressing the issue of privacy. In the Chairman's view, self-regulation needs to play a large role in addressing privacy concerns, in order to avoid excessive or ill-advised government regulation. Burdensome government regulation or a regulatory framework is not the answer to protecting individual privacy on the Internet. Rather, government efforts should support and compliment private sector initiatives. As the Chairman recently stated:

> *Over the past year, as I have observed the self-regulation of the industry, I also have been examining different self-enforcement systems that have proved successful in other industries, and that might serve as a useful model for the protection of privacy on the Internet. In my opinion, both industry and the public will be well-served by . . .giv[ing] the industry appropriate flexibility to establish its own practices with respect to privacy while providing consumers with appropriate assurances regarding the protection of their personal identity.*[27]

B. What Progress Is Being Made By Industry In Protecting Online Privacy?

A 1999 Georgetown University study on Internet privacy found that 92.8 percent of websites surveyed were collecting personally identifiable information from consumers, yet only 9.5 percent of those sites contained the four elements of fair information practices[28] called for by the Federal Trade Commission—notice, choice, access and security.[29] On the other hand, evidence suggests that "businesses are providing significantly more notice of their information practices than they were in the past."[30] There has been an increase in the posting of privacy policies on websites, with 19 percent of the top 100 sites posting privacy policies containing disclosures of the four elements.[31] Industry stands to benefit from this trend: research shows that 28 percent of a group of heavy Internet users polled said they would be more likely to provide information if a site had a privacy policy, and 58 percent said they would be more likely to provide information if a site had both a privacy policy and a seal

---

[27] Sen. Orrin Hatch, "What is the best way to ensure online privacy? Let Industry Enact Privacy Measures," Roll Call, March 27, 2000.
[28] The Code of Fair Information Practices, although never enacted into law, provides a widely recognized set of principles that serve as a useful measure for assessing Industry privacy practices. See United States Dep't of Health, Education & Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973).
[29] *See Georgetown Privacy Policy Survey: Report to the Federal Trade Commission* (June 1999) (available at www.msb.edu/faculty/culnanm/gippshome.html).
[30] *See* Federal Trade Comm's, *supra* note 2.
[31] See Mary J. Culnan, Ph.D., *Privacy and the Top 100 Web Sites: Report to the Federal Trade Commission* (Online Privacy Alliance, June 1999).

of approval from one of the well-known seal programs.[32] Individual companies are taking a variety of initiatives to respond to privacy concerns. For example, several industry leaders such as IBM, Microsoft and Disney have led the effort to require websites to post privacy policies, by refusing to advertise on sites that fail to post them.[33] Such market-based solutions play an important role in both educating Internet users regarding their online privacy and ultimately in increasing consumer confidence in transacting e-commerce. It is our hope that more and more companies will see the wisdom of implementing market-based solutions and adopting privacy policies.

C. The Need To Empower Consumers To Protect Their Privacy.

To protect their privacy online, consumers must understand how their privacy can be jeopardized. The Committee seeks to enhance consumer awareness about how personal data is collected. In addition, the Committee seeks to empower consumers by providing information about the tools available to protect online privacy.

Although consumers indicate they are concerned about the possibility of their private information being traded to third parties, research shows a continued trade-off by Internet users between privacy and security on the one hand, and utility and price on the other.[34]

Again, it is important to remember that while technological advances have made the collecting, storing and disseminating of personally identifiable information on the Internet easier and faster, dealing in personally identifiable information is not a new business and does not occur solely on the Internet. By using a credit card at a store or visiting an automatic teller machine ("ATM"), consumers constantly leave a trail of information behind that may be valuable to third parties. It is also important to note that the collection of such information also allows for customized services which consumers prefer.

When consumers understand the extent to which personally identifiable information is collected and used, they then can make an informed judgment about whether to provide the information.

It is clear that consumers are willing to trade personal information under certain conditions in exchange for something of perceived value. Some websites provide benefits such as discounts on products or services, free e-mail, a free website, free Internet service, or even a free computer in exchange for personal information. A recent study found that 86 percent of

---

[32] *See* Cranor, *supra* note 8.

[33] *See* Ted Bridis, *Microsoft Requiring Privacy Pledges* (Assoc. Press Online June 23, 1999); *see also* K. Oanh Ha, *Microsoft Plans Net Privacy Policy*, San Jose Mercury News (June 23, 1999).

[34] *See* Jupiter, *supra* note 9.

Americans believe that participation in such information-for-benefits is a matter of personal choice.[35]

In another study, consumers admitted the most significant factor that would motivate them to trade information about themselves with a website would be a guarantee that the information would not be misused. This was followed by the possibility of winning a prize or sweepstakes, regular e-mail updates on products or services, access to more or better content/information online, affinity points such as frequent flier miles, and the ability to receive targeted advertisements.[36]

Website privacy policy statements that clearly and effectively notify consumers as to what personally identifiable information is collected and how such information will be used are important. Consumers then may determine whether to visit a site based upon his or her informed consent. This approach (absent deceptive practices by websites) gives the consumer the control to make a reasoned choice based on a website's privacy policy.

D. What Can Consumers Do To Protect Their Privacy?

While some progress is being made by websites, the state of affairs is far from optimal from both a consumer and an e-commerce perspective. Consumers can best protect their personally identifiable information by having a better understanding of the information, resources and technologies available to them.

The remainder of this Report provides summary information for Internet users on various resources available to them, both in terms of organizations that can provide privacy information and other technology-based tools. For a glossary of Internet and online terms you may refer to the Internet Alliance website (a trade association representing the online industry).[37]

IV. RESOURCES.

A. Technologies Available to Consumers.

In the dynamic arena of Internet technology, a wide variety of exciting technological solutions exist to safeguard personally identifiable information and new ones are continually being developed. This Report's discussion of the available technologies is not intended to be a comprehensive one, but rather is intended to give consumers a sampling of the tools currently available to consumers that help empower them to safeguard their privacy to the extent they wish. The Committee's decision to describe particular technologies should not be interpreted as an endorsement of any technology.

---

[35] *See* Opinion Research Corp., *Study for Privacy & American Business,* (1999) (available at http://www.pandab.org/).

[36] *See* Jupiter, *supra* note 9.

[37] *See* http://www.Internetalliance.org/project-open/about.html.

The product and service descriptions listed below are short summaries based upon information received from the respective organizations, for the purpose of providing consumers with a starting point for learning about some of the technology options available to them. They are not intended to replace independent consumer inquiry into full and complete product and service information, and they do not constitute an endorsement or recommendation of any kind.

The Committee invites the public and technology companies to forward additional privacy technology tools that might be helpful to Internet users to the Committee via e-mail or written correspondence. We will take the efforts to update this technology resource periodically with new technologies.

1. Ways of Handling Cookies.

Again, "cookies" are electronic tags that are placed on the hard drive of a user's computer by websites he or she visits. (See section II. D. of this Report). Currently available to users are a number of options to: (1) alert them as to when a cookie is placed on their hard drive, (2) block the placement of a cookie altogether, or (3) remove cookies from the user's hard drive. A few of these options are described below:

a. Internet Browser Settings.

New technology permits Internet users to see when a cookie is about to be planted on their system and make an informed choice about whether to accept it or reject it. With current versions of leading browsers such as Netscape Navigator[38] and Internet Explorer,[39] a user can select to have an alert box flash on the screen to inform them whenever a server is trying to place a cookie on their system. Some sites, however, send cookies for every object the user clicks on the page, requiring the user to reject cookies dozens of times for a single web page.[40]

---

[38] A basic description of how to work Netscape Alert: Go to the "Advanced" section of the Netscape Preferences Menu (found on the "Edit" pull-down menu). There you can "accept" all cookies, accept only cookies that get sent back to their server of origin, or disable cookies. You can also ask to be warned before accepting a cookie. Description provided courtesy of Dr. Lee Hollaar, Professor of Computer Science at the University of Utah.

[39] To operate the cookie alert system on Microsoft's Internet Explorer, go to "Internet Options" under the "View" menu. On the "Advanced" tab you will find options to prompt you before accepting a cookie, disabling cookies, and always accepting cookies. Description provided courtesy of Dr. Lee Hollaar, Professor of Computer Science at the University of Utah.

[40] As the World Wide Consortium points out, many cookies are benign attempts to improve your web browsing experience, not intrusions on your privacy. Netscape Navigator 4.0 provides a new feature that allows you to refuse cookies that are issued from sites other than the main page you are viewing. . . .To access this option, select Edit >Preferences->Advanced, and select the appropriate radio button from the cookies section. Some people might want to allow transient cookies (ones active only during a browsing session) but forbid persistent ones (ones that store user identification information over an extended period). On Unix systems, you can do this easily by creating a symbolic link between the Unix 'bit bucket' device, /dev/null and the cookies file. See http://www.w3.org/Security/faq/wwwsf7.html.

b. Manual Deletion Of Cookies Using Browser Files.

Internet users can locate and delete cookies that already have been placed on their computer by websites. In Netscape Navigator, the cookies are stored in a single file called "cookies.txt." This file generally is in the directory the user previously designated for Netscape to use for storing user profiles. To delete all cookies, find the "cookies.txt" file, highlight it, and delete it. To delete a specific cookie, open the file "cookies.txt" with an editor or word processor, and delete the line corresponding to the cookie you wish to delete.

For Internet Explorer, find the directory called "Cookies." To delete all cookies, delete all the files in the directory. To delete a specific cookie, find the file in the directory corresponding to the cookie and delete that file.

c. Cookie-Cutters.

Various technology-based tools exist for coping with unwanted cookies. Examples of these include "NSClean"[41] and "IEClean" for Windows 95/NT programs, "AdSubtract" for Windows, MacIntosh and Unix, "Cookie Jar 2.0" for Unix, "Internet Junkbuster Proxy" for Windows 9X and Windows NT, "Cookie Cruncher," "Cookie Manager," and

"Privacy Companion."

i. Netscape Cookie Manager.

Developed by America Online, Netscape Cookie Manager, a feature of the new Netscape browser, allows users to view, block, and delete cookies based on their individual privacy preferences. For example, Cookie Manager permits a user to determine who may and who may not set cookies on his or her computer, edit and delete any of the cookies placed, and review a list and description of all of the cookies placed on the user's computer.

Other privacy technology developed by America Online includes AOL Parental Controls[42] and AOL Instant Messenger.[43] AOL Parental Controls permits parents to determine who their children may or may not communicate with when they use AOL by initiating specific privacy settings. AOL Instant Messenger allows a user to control his or her own privacy by limiting who is permitted to know when the user is online and who is permitted to make contact with the user.

ii. Privacy Companion.[44]

Developed by Idcide, Inc., Privacy Companion is a browser software application that is intended to enable users to detect and block third party cookies, while allowing them to

---

[41] *See* http://www.nsclean.com.
[42] *See* http://www.aol.com/info/parentcontrol.html.
[43] *See* http://www.aol.com/aim/home.html.
[44] *See* http://www.idcide.com.

benefit from personalized services from the websites that they are visiting. Privacy Companion automatically detects and blocks cookies from third party advertisers and profiling companies which can be used to track a user's browsing behavior as he or she moves from website to website. It also provides statistics on sites which may have tracked a user's browsing behavior.

iii. NSClean Privacy Software.

NSClean Privacy Software[45] provides products that permit the end-user to turn off the cookie warnings, accept cookies while online, and then remove them from their hard drive. "Owing to the need for legitimate cookies to be kept for the convenience of users for legitimate sites," the new NSClean products permit users control over cookies, enabling them to select which cookies they find useful and desire to keep and remove all other cookies automatically at their option.[46]

iv. AdSubtract.

AdSubtract[47] offers filtering to eliminate unwanted advertisements, animated images, cookies, pop-up windows, background music, and the like. By eliminating unwanted pages,

AdSubtract speeds up web page download time. The downloadable software provides the user with statistics showing items filtered.[48]

v. Cookie Jar 2.0.

Cookie Jar 2.0 software allows users control over which sites can send cookies to the user's computer. Using the Internet browsers, the user sets up a configured file allowing only specified sites to send cookies. Sites which have not been selected by the user are silently discarded. This technology also offers the ability to stop browsers from sending revealing information to web servers, and to block connections to certain sites.[49]

vi. Cookie Cruncher.

Like Cookie Jar, Cookie Cruncher works with the user's Internet browser to give the user control over the cookies that are accepted by and eventually stored on a system. Cookie Cruncher blocks cookies before they are placed on the user's hard drive by automatically and transparently accepting or rejecting cookies from specified servers without user interaction once the user has specified preferences. In addition, Cookie Cruncher informs the user of the cookie's spe-

---

[45] *See* http://www.nsclean.com.
[46] Testimony of Kevin McAleavey for the Federal Trade Commission's Workshop on the issues of privacy on the Internet (June 1997) (available at http://www.ftc.gov/bcp/privacy/wkshp97/comments2/nsclean.htm).
[47] *See* http://www.adSubtract.com.
[48] *See* http://www.adSubtract.com/pro/features.html.
[49] *See* Eric Murray, *Cookies Jar 2.0, Filter Ads and Cookies from the Web* (available at http://www.lne.com/ericm/cookie_jar/.

cific purpose, such as advertisement tracking, online shopping or site tracking. It also can compile a list of all the cookies that have been accepted or rejected during the course of an online session, and gives the user the option to save the list for later use.[50]

vii. Internet Junkbuster Proxy.

Internet Junkbuster Proxy is free software tool that gets rid of banner ads and cookies while individuals surf the Internet. The software only accepts cookies from sites which the user pre-selects. The software also prevents the disclosure of other personal details, such as information about the page clicked on and the user's computer software and hardware configuration. Users have the option to block whole sites or block ads. Junkbuster's features can be optionally disabled or altered.[51]

2. Identity Scrubbers.

Various user information is instantly available to websites when users visit them.[52] Identity scrubbers are tools developed to allow users of the Internet to remain anonymous while surfing the Internet. While a number of companies offer different options for consumer, the following is a sampling of identity scrubbing tools that are available.

a. PrivadaControl.[53]

Privada is a digital privacy service created for Network Service Providers. PrivadaControl, operated on a user's personal computer, permits the user to browse the Internet anonymously and to send and receive emails anonymously. While using PrivadaControl during Internet use, a user's webpage requests are encrypted and sent to the Privada Network. The Privada Network then retrieves the webpage and returns it to the user. Additionally, PrivadaControl allows users to manage the placement of cookies, which are assigned to the user's individual profile on the Privada Network rather than on the user's computer. As a result, the user may take advantage of the benefits of customized browsing without privacy concerns. Users may disable PrivadaControl's privacy protections in order to share personal information with those websites they choose. PrivadaControl also allows a user to send and receive email anonymously by permitting the user to create a separate identity and to establish an anonymous email account with that identity on the Privada Network. A user may then send and receive email from this account without disclosing his or her

---

[50] *See* http://www.thelimitsoft.com/cookie.html#overview.

[51] *See* http://www.internet.junkbuster.com/.

[52] To view a sampling of the information that is generally available to the Websites you visit, *see* http://www3.anonymizer.com/3.0/index.shtml.

[53] *See* http://www.privada.com.

personal identity. Email messages sent by the user to the Privada Network are encrypted, and the user may choose to have the Privada Network assign his or her sent messages a random delay of 30 minutes to four hours.

b. Incogno SafeZone.[54]

Developed by Incogno Corporation, Incogno SafeZone is a patent-pending technology that enables Internet merchants to offer anonymous checkout services to privacy-sensitive buyers. Using Incogno SafeZone, customers buy directly from the merchant's site and receive product shipments without revealing their names, addresses, email addresses, or credit card information to the merchant. Additionally, because the merchant does not receive, store, or transmit the customer's credit card information in unencrypted form, the risk of credit card fraud is reduced. In using Incogno SafeZone, a merchant can request that customers disclose their personal information, but any such disclosure is fully voluntary. Incogno SafeZone currently is in the market trial stage.

c. Freedom.[55]

Developed by Zero-Knowledge Systems, Inc., Freedom works in conjunction with the Freedom Network, which is a series of globally distributed, independently hosted servers. Freedom is intended to ensure a user's online privacy and security by encrypting all email and browsing communications. Users of Freedom manage their online activities with the help of pseudonyms or "nyms." Each nym has its own email address and "cookie jar," thus each nym can build its own pseudonymous reputation capital—allowing users to take advantage of targeted on-line marketing material when desired. According to Zero-Knowledge, Freedom is created in such a way that no one, not even Zero-Knowledge, can trace a nym to its actual owner.

d. Anonymizer.com.[56]

Recognizing that each time an Internet user enters a website, he or she could provide certain personal information, including viewing habits, geographical location, addresses, e-mail and credit card numbers, Anonymizer.com enables users to visit sites while concealing their identity. Anonymizer protects consumer privacy by acting as an intermediary between the user and a particular website. The following are a few of the services offered by Anonymizer.com:

• "Anonymizer Surfing" offers a free and nominal-fee based system that allows users to browse the web through using an intermediary to pre-

[54] See http://www.incogno.com.
[55] *See* http://www.zeroknowledge.com.
[56] *See* http://www.anonymizer.com.

vent unauthorized parties from gathering personal information. The system is web-based and does not require software or upgrades.

• Anonymizer Window Washing is a fee-based program that automatically cleans up the user's browser, cache, cookies and other online history.

• Anonymizer Pipeline protects the user's Internet activity with encryption between consumers and the Anonymizer network. It enables customers to use e-mail, news, and the web anonymously from their personal computer. The Internet service provider, and anyone between the individual and the Anonymizer network, sees only scrambled data, with all activity appearing to come from the Anonymizer subnetwork located in California.[57]

e. Crowds.[58]

Developed by AT&T Research, Crowds allows users to blend into a virtual crowd on the Internet by hiding an individual's actions within the actions of many users. Users are placed into a large and geographically diverse group, or "crowd," which collectively issues requests on behalf of its members. The end server is unable to identify the initiator of the request because the initiator is indistinguishable from any of the other "crowd" members.

3. Privacy Preference Technology.

Privacy preference technology allows the user to select his or her own privacy preferences, to modify those preferences, and to compare how particular websites' privacy policies match his or her own preferences.

a. AT&T Research.

AT&T Research,[59] in conjunction with Microsoft Corporation, is developing browser software technology to be used with Microsoft's Internet Explorer. When installed by the user, this technology will add a privacy button to the top of his or her browser window. By clicking on this button, a user will be able to set his or her privacy preferences, check how well a website's privacy policy matches the user's preferences, and view a site's actual privacy policy. AT&T's technology currently is in the development stages.

b. PrivacyRight.[60]

PrivacyRight's Unified Customer Permissions platform (UCP) is a server-side privacy solution which may be accessed by consumers at any point during their visit to a website, and with which they may set privacy preferences governing the use of their personal information. The UCP platform allows the interpretation and enforcement of persistent rules as-

---

[57] *See* http://www.anonymizer.com.

[58] *See* http://www.research.att.com/projects/crowds/.

[59] *See* http://www.research.att.com.

[60] *See* http://www.privacyright.com

signed to personal information and facilitates consumer-approved data exchanges between applications within an organization and from business-to-business.

4. Digital Identity Managers/ Preference Organizers.

In part a convenience tool for individuals who shop online, digital identity managers, or preference organizers as they are also called, provide Internet users with customized profiles of their personally identifiable information, enabling them to better control the sharing of that information.

a. Microsoft Passport.[61]

Microsoft Passport offers consumers on the Internet two services, a "single sign-in" service which enables users to have one name and password at all participating websites and a "wallet" service to make online purchasing more convenient and safe. The consumer's password is only stored in Passport's secure database and no other website is provided with access to it. In addition, Passport incorporates security features to help protect the user's personally identifiable information from hackers and others who might attempt to pose as the consumer.[62] With regard to the "wallet" service, the consumer can securely store a number of credit cards and shipping addresses in the online wallet and select from them when placing an order. The information is then sent over a secure connection to the seller. Consumers' personally identifiable information is protected by encryption technology, and consumers are empowered to control which sites have access to their information.

Microsoft also has developed Kids Passport[63], which is designed to help parents protect their children's online privacy. The Children's Online Privacy Protection Act (COPPA), enacted by Congress in 1998, requires that operators of online services or websites obtain parental consent prior to the collection, use, disclosure, or display of the personal information of children. The Kids Passport service is designed to help parents control what information their children can share with websites and what those sites can do with that information. With a Kids Passport account, a child is provided with a password to access participating online sites and services. When the child attempts to sign on to a participating site or service that requires personally identifiable information, the child must request consent from a parent or guardian before sharing the information. The child may make this request through the Kids Passport ser-

---

[61] *See* http://www.passport.com.

[62] Passport uses a computer-generated key rather than the Passport sign-in name to track the consumer when he or she enters a site, making it more difficult for hackers and others to obtain access to a consumer's personally indentifiable information. Participating websites also refresh the key regularly making it more difficult for someone else to pose as the consumer.

[63] *See* http://www.passport.com.

vice. The parent or guardian then receives the request and may either select a specific level of consent, or deny consent for the site or service.

b. Iprivacy Identity Manager.[64]

The Iprivacy Identity Manager is software designed to permit users to browse, shop, and receive correspondence over the Internet in privacy. Users download the Iprivacy Identity Manager from trusted third parties, such as their credit card issuers, in order to generate proxy identities, financial, and shipping information for use on a purchase-by-purchase basis. The software is designed to prevent the gathering of information about a user's Internet behavior, as well as to prevent the creation and sharing of data bases with a user's personal and financial information without the user's express permission. According to Iprivacy, it will never know the identity of the individuals who use its service.

c. Digitalme.[65]

Digitalme is Novell's identity management service that enables Internet users to take control of how their information is shared, used and maintained on the Web. Using Digitalme, an Internet user is empowered to control his identity on the Web and enjoy conveniences such as single-click buying.

With Digitalme, individuals personalize their digital identities by using "mecards," which only exist in the digital world. The "mecard" contains a customized profile of personally identifiable information that the individual user puts together. Individuals may develop more than one "mecard" to be used in different situations. For example, business "mecards" may only contain professional information such as a work address, phone number, and e-mail address. Another "mecard" may contain a home address and credit card number for personal online purchases. By leveraging the ability of Novell Directory Services technology to track identities on the Web, Digitalme gives individuals and businesses more control over their personal information and decreases the need for numerous passwords and user names.

Once implemented, "mecards" can be exchanged with business associates, personal contacts and businesses over the Internet. When an individual updates or changes information on a particular "mecard," the changes automatically will be provided to all holders of the card, preventing an individual from having to inform all of his or her contacts of an address change.[66]

In addition, Digitalme prevents users from having to fill out forms every time they want to make an

---

[64] *See* http://www.iprivacy.com.
[65] *See* http://www.digitalme.com.
[66] *See* http://www.digitalme.com/Learn_More/.

online purchase. Under Digitalme's Auto-Form-Fill-in, information from a users Digitalme card account will automatically provide their personal information to any websites requesting online registration. Moreover, with each transaction, consumers will be able to make a determination as to how much information may be shared.[67]

5. Infomediaries.

Infomediaries act as a "go between," to enable individuals to have control over what personal information is shared at each website they visit while on the Internet. Some infomediaries operate by having users create a detailed personal profile in accordance with the infomediary technology which negotiates the release of his or her personal information. Infomediaries can act as a "go between" for users with websites to protect user privacy.

a. Orby Privacy Plus.[68]

Developed by YOUpowered, Inc., Orby Privacy Plus permits users to develop their own privacy preferences and to decide how, when, and where to share their personal information. It also matches websites' privacy policies to the user's privacy preference settings, provides feedback to users regarding a particular

website's privacy policy and behavior, and allows users to manage cookies—such as permitting a user to accept or deny cookies while browsing. YOUpowered's Consumer Trust[69] is a software application for businesses that is intended to compliment the use of Orby Privacy Plus by consumers. Consumer Trust assists business users in developing, publishing, and managing privacy policies that are understandable to a wide variety of consumers. It also is intended to help match a website's privacy policy with consumers' privacy preference settings.

b. Persona, Inc.[70]

Persona is a third-party guardian of consumers' personal information. The company is dedicated to facilitating e-commerce and personalization opportunities between consumers and businesses through tools and services that join the two in a mutually beneficial environment. Persona's technology includes Persona, a consumer-driven information broker between the consumer and a website, PersonaValet, a customized toolbar which includes tools to assist the consumer in optimizing their personal data, and Persona Profile Access Kit (PersonaPAK), which enables businesses to communicate with consumers.

---

[67] *See* http://www.digitalme.com/Press_Center/Press_Materials/Backgrounder/.

[68] *See* http://www.youpowered.com.

[69] *See* http://www.youpowered.com.

[70] *See* http://www.persona.com.

c. Lumeria.[71]

Lumeria's infomediary technology targets the ability of web businesses to create profiles of users' movements, purchases and sensitive information on the Web. Lumeria's technology allows individuals to organize, securely access and selectively share personally identifiable information with companies, and to profit from the sharing of that information.

Specifically, Lumeria assists individuals in organizing their personal information into a profile for eventual sale over the Internet. While maintaining control of their own information, consumers can profit by selectively sharing it for a fee.[72] The exchanging of one's personally identifiable information for a fee, or "I-Commerce," as Lumeria calls it, strives to give control of personal information to individuals.[73] In order to help educate and inform consumers about privacy issues, Lumeria has launched a web publication called PrivacyPlace.com that provides information, discussion groups, and access to technology.[74]

d. PrivaSeek.[75]

PrivaSeek is another tool which allows individuals to have control over their personally identifiable information. Users create a "Persona"

by inputing data such as name, e-mail address and phone number. The consumer may provide additional information, such as hobbies and interests. Once personal data is entered, a password protects the information so that only the user can change it. Additionally, individuals may "grant permission" to specific companies that may access their data. In exchange, the company may provide a personalized web experience, discounts or special offers. Once a user has created a "Persona" he or she can use "PersonaValet" technology to automatically fill out online forms, such as those used to register at a website or to make purchases.

e. Respond.com.[76]

Respond.com is an Internet infomediary site that connects buyers to sellers. The transaction begins when a buyer fills out a request form on a product or service that they wish to buy. The buyer submits the request to Respond.com, which in turn delivers it to registered sellers via e-mail. Interested sellers respond to the buyer's request through Respond.com, and the sellers' responses are then forwarded to the buyer. Respond.com allows buyers to remain anonymous to the sellers until they choose to contact the seller directly. Using this approach,

---

[71] See http://www.lumeria.com.
[72] See id.
[73] See http://www.superprofile.com.
[74] *See* http://www.privacyplace.com.
[75] *See* http://www.privaseek.com.
[76] *See* http://www.respond.com.

the buyer controls whether to eventually contact a seller, and the buyer avoids disclosing personal information to sellers in the process. The service is provided free to buyers, while sellers must pay a nominal fee to be registered with Respond.com.

6. Permission Marketing.

Permission marketing is an example of the "trade" of personal information that some Internet users are willing to make in exchange for something of value to them. YesMail[77] and Brodia[78] are both examples of permission marketing that provides the consumer with certain benefits in exchange for profile information.

7. Business To Business Technologies.

a. Ad Delivery Services.

A growing method of advertising and marketing to consumers over the Internet involves the development of massive, sophisticated and detailed databases of customer profiles which enable highly targeted advertising in terms of content and audience. Privacy concerns are implicated for consumers when information is collected from them so profiles can be developed. On the other hand, consumers can benefit from the targeted nature of the advertisements because they will receive advertising information on areas of interest and largely avoid others. To the extent that some ad delivery services keep consumer information impersonal (identifying consumer profiles by number rather than by name, for example), consumers can maintain a certain level of anonymity and privacy protection. Businesses find these services useful because they are able to develop highly tailored ad campaigns, and evaluate and even modify them while they are in progress. However, where such profiling is done without notice to Internet users and divulged to third parties, it has raised serious privacy concerns for consumers. Examples of ad delivery services include Adforce,[79] DoubleClick,[80] Engage,[81] and Encirq.[82]

i. Encirq.[83]

Encirq Corporation is an online marketing services company which assists companies in the delivery of individualized consumer-centered content over the Internet. At the same time, Encirq's technology seeks to assist companies in preserving consumer privacy. The technology is delivered to consumers through busi-

---

[77] *See* www.yesmail.com.

[78] *See* http://www.brodia.com.

[79] *See* http://www.adforce.com/.

[80] *See* http://www.doubleclick.net/.

[81] *See* http://www.engage.com.

[82] *See* http://www.encirq.com.

[83] *See* http://www.encirq.com.

nesses that have online relationships with consumers, such as banks, credit card companies, brokerage firms, and utilities. According to Encirq, neither marketers nor Encirq itself sees the marketing data collected from consumers. Instead, the data resides on each consumer's personal computer. The technology seeks to determine the interests and behavior of the individual user, assist marketers in delivering relevant messages to targeted consumers, and filter out irrelevant content before it reaches consumers.

b. Customer Relationship Management.

NCR offers data warehousing and customer relationship services to companies operating online (or offline). A software application called "NCR's Relationship Optimizer" develops a detailed analysis of individual consumers' behavior and then helps companies determine what, how and when to communicate with the consumer.

As various customized marketing services raise privacy concerns, NCR offers software tools to implement personal data protection. Consumer choice (opt-in or opt-out), auditing and security are all facilitated by the data warehouse and by setting up varying "views" into the data warehouse. For instance, marketing would not have access to personal data for those consumers who have opted against the use of such data for marketing purposes.

i. ID Vault Privacy Network.[84]

ID Vault's Privacy Network is a B2B framework that enables companies to send and receive electronic IDs containing personal data across company boundaries. It is intended to provide a secure network that enables organizations to send and receive IDs while respecting the privacy rights of individuals. The Privacy Network provides a system for storing individuals' privacy preferences, a web portal for individuals to modify their privacy preferences, and a B2B network that brokers privacy agreements and enables organizations to send personal data pursuant to those agreements. The Privacy Network currently is in the implementation stage.

ii. Privacy Statement Wizard.[85]

Developed by Microsoft Corporation, the Privacy Statement Wizard is designed to help small and medium sized businesses develop their own privacy policies. A business user answers a series of questions about the company's information practices and related issues. Based on these answers, the Privacy Statement Wizard then provides the user with a draft privacy policy which can be amended or supplemented by the user. According to Microsoft, over 19,000 entities have used Privacy Statement Wizard to date.

---

[84] *See* http://www.idvault.com.
[85] *See* http://www.bcentral.com.

iii. SecureWay Privacy Manager.[86]

Developed by Tivoli Systems, an IBM subsidiary, the SecureWay Privacy Manager is intended to help e-businesses implement effective privacy policies and protect their customers' personally identifiable information. SecureWay Privacy Manager also assists businesses to centralize the definition and enforcement of their privacy policy. As a result, when an organization's privacy policy changes, its rules need only be changed centrally, rather than require modification to each individual application that is affected by the change.

iv. Digital Handshake.[87]

Developed by Ilumin Corporation, Digital Handshake is a patent-pending digital signature technology with privacy enhancing features. Available as an add-in service for e-business applications and websites, Digital Handshake enables multiple parties to interact and facilitate the closure of legally binding transactions using digital signatures. Such transactions include buying a home, selecting car and health insurance, initiating an online trading account, or obtaining a loan. Using multiple levels of encryption technology for access control, identity authorization, and confidentially of sensitive legal documents, Digital Handshake ensures data security and privacy to

enable only designated parties access to confidential documents.

v. Private Payments.[88]

Developed by American Express, Private Payments allows consumers a more secure way to pay online using a random, unique number for each online transaction. Available to American Express consumer and small business card holders, Private Payments generates a unique number with an expiration date that is randomly created. The card member transfers this information into a merchant order form to complete his or her purchase. The card member's actual card account number is not sent over the Internet, thus ensuring the user's credit card security. The Private Payments number is designed to be used for a single purchase and to expire after the merchant authorization process is completed. Upon expiration, the Private Payments number cannot be used again if stolen. Tools also are available to online businesses that collect consumer information, to ensure that consumer preferences with respect to personally identifiable information are respected. While it is up to the online businesses to implement these business-to-business tools, as more consumers become aware of privacy issues, they will likely begin to demand that retailers respect their privacy preferences. These tools better able

---

[86] *See* http://www.tivoli.com.

[87] *See* http://www.ilumin.com.

[88] *See* http://www.americanexpress.com.

businesses to respond to consumer privacy preferences, or to comply with certain self-regulatory privacy requirements.

8. Impermanent Email Technology.

Impermanent email technology permits users to send email messages using the digital equivalent of disappearing ink—the messages become permanently unreadable after a predetermined period of time. This technology also permits organizations to extend their paper document management policies to email messages.

a. Disappearing Email.[89]

Developed by Disappearing Inc., Disappearing Email allows a user to send and receive email messages that eventually become unreadable. The user thus retains control over the life of an email message sent, even after it leaves his or her outbox. When a user sends a message using Disappearing Email technology, the message is encrypted, and it passes through regular email channels as unreadable text. When a recipient opens the message, they "borrow" the unique key that was used to encrypt the message. After a set period of time determined by the user (minutes, hours, days, or months), the key is destroyed, rendering all copies of the message permanently unreadable. If the recipient of the message uses

Disappearing Email technology, the sent message appears as ordinary email. For recipients without the technology, however, the Disappearing Email message contains information to clarify to the recipient that the message will become unreadable after a specified time period.

B. Website Seal Programs.

Third-party enforcement programs known as "seal programs," provide another way to monitor company practices and enforce privacy policies. By clicking on the "seals" such as TRUSTe, BBBonline, Webtrust, and Enonymous.com on a particular website, a user is immediately linked to the site's privacy statement. The purpose of the seal programs is to create name and sight recognition for the seals so that consumers will see them and know that they are visiting a site they can trust. Seal programs are designed to provide protection to consumers, by allowing web companies to standardize privacy policies.

1. TRUSTe.

TRUSTe[90] is an online privacy seal program designed to enhance consumer confidence that privacy in the information they provide to companies online will be protected. To obtain the TRUSTe seal, a website must have a privacy policy with sev-

---

[89] *See* http://www.disappearing.com.

[90] *See* http://www.truste.org. Companies that participate in the TRUSTe program also must enter into a licensing agreement and pay a fee of at least $299 as determined by the company's annual revenue.

eral components.[91] The policy must disclose what personal information is being gathered about the consumer, how the information will be used, whether the information will be shared with a third party, and what choices the consumer has with regard to the use of collected information. In addition, TRUSTe requires the website to disclose the existence of safeguards to protect the consumer from loss, misuse or alteration, and information on how the consumer can update or correct inaccuracies in their personal information.[92] Once a website receives the TRUSTe seal, the site is reviewed periodically to ensure that it is complying with its privacy policy and the TRUSTe program requirements. In addition to conducting its own monitoring, TRUSTe relies on users to report violations and privacy concerns.[93] In addition, the TRUSTe website provides consumer information on privacy protection.

2. BBBOnline.

BBBOnline,[94] a wholly owned subsidiary of the Council of the Better Business Bureau, is designed to be an accessible tool to increase consumer confidence in accessing and using the Internet. For a website to qualify for a BBBOnline seal, it must submit an application and complete an assessment process. This process investigates various aspects of the applicant's information practices regarding privacy notice, content and placement, corporate structure, security measures, transfer and merger of information, access and correction. BBBOnline requires website's privacy notices to be "one click away" from the site's home page and every other page on which personally identifiable information is collected.[95]

According to the BBBOnline website, its privacy program:

•   *Awards an easily recognizable and affordable "seal" to businesses that post online privacy policies that meet the required "core" principles, such as disclosure, choice and security;*
•   *Provides consumer-friendly dispute resolution services; and*
•   *Monitors compliance through rigorous requirements for participating companies.[96]*

3. CPA WebTrust.

CPA WebTrust[97] is a third-party seal program that uses a licensed Certified Public Accountant ("CPA") to examine a company's website to ensure that its transactions meet certain standards. To potential customers, the seal

---

[91] According to TRUSTe's website, "TRUSTe awards its trustmark only to Websites that adhere to established privacy principles and agree to comply with ongoing TRUSTe oversight and consumer resolution procedures." http://www.truste.org/users/users_watchdog.html.

[92] *See* http://www.truste.org/users/users_watchdog.html.

[93] *See* http://www.truste.org/users/users_watchdog.html.

[94] *See* http://www.bbbonline.org.

[95] *See* http://www.bbbonline.org/businesses/privacy/eligibility.html.

[96] *See* http://www.bbbonline.org/business/privacy/self-regulation.html.

[97] *See* http://www.CPAWebTrust.org.

provides assurance that the particular site conforms in three key areas:

1) Business Practices & Information Privacy: The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with those practices.

2) Transaction Integrity: The entity maintains effective controls to provide reasonable assurance that transactions using e-commerce are completed and billed as agreed.

3) Information Protection: The entity maintains effective controls to provide reasonable assurance that private information obtained as a result of e-commerce is protected from uses not related to the entity's business; and addresses privacy and security matters such as encryption of private consumer information, protection of information once it reaches the entity, requests for consumer permission to use personal information, and a consumer's approval before storing, altering, or copying information on their computer.[98]

C. Organizations Involved In Online Privacy Dialogue.

A number of organizations involved in the online privacy dialogue have taken steps to increase consumer awareness of privacy issues and assist in privacy protection. Some of the key groups involved in the online privacy discussion, ranging from privacy advocacy groups to industry groups, and the resources they can provide are discussed below:

1. Center for Democracy and Technology.

The Center for Democracy and Technology ("CDT")[99] is a non-profit, public interest organization which seeks to promote democratic values and civil liberties on the Internet. With experience in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet. In addition, CDT promotes its own policy positions in the United States and globally through public policy advocacy, online grassroots organizing with the Internet user community, public education campaigns, litigation, and through the development of technology standards and online information resources.

CDT's website includes several tools designed to aid users in protecting their privacy, including:

a. Operation Opt-Out.[100] A central resource for individuals who would like to remove their names from mailing and telemarketing lists, and limit online tracking and sale of personal information by businesses.

---

[98] *See* http://www.CPAWebTrust.org/consumer/index.html.

[99] *See* http://www.cdt.org.

[100] *See* http://opt-out.cdt.org.

b. Guide to Online Privacy.[101] An informational resource detailing the privacy debate in the U.S. and throughout the world with helpful information for consumers and businesses.

c. Privacy Watchdog.[102] A tool designed to help consumers read and understand privacy policies. Privacy Watchdog also assists consumers in contacting websites with insufficient or non-existent policies.

2. Direct Marketing Association.

The Direct Marketing Association ("DMA")[103] is the largest trade association for businesses involved in interactive marketing, databases and electronic commerce. DMA recently introduced two self-regulatory policies, "Privacy Promise"[104] and "E-mail Preference." Privacy Promise requires member companies who market to consumers to adopt the mail and telephone preference services. Consumers are given the power to remove their names from a national marketers' list,[105] and companies are required to notify customers of any transfer of information to third parties, allowing consumers the choice to opt-out. "E-mail prefer- ence" (not yet initiated) will operate in a fashion similar to "Privacy Promise," giving consumers the ability to remove their e-mail addresses from marketing lists. In addition, DMA provides access from its website to a "Privacy Policy Generator," a tool to assist companies in creating customized privacy policy statements, in keeping with DMA's position that online marketers should prominently display their information policies to consumers.

3. Electronic Privacy Information Center.

The Electronic Privacy Information Center ("EPIC")[106] is a public interest research center whose goal is "to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values."[107] Established in 1994, EPIC advocates the aggressive enforcement of Fair Information Practices as an important way to address privacy protection.

4. Internet Alliance.

Internet Alliance (IA)[108] is a trade association representing the online

---

[101] *See* http://www.cdt.org/privacy/guide/introduction.

[102] *See* http://watchdog.cdt.org.

[103] *See* http://www.the-dma.org.

[104] Privacy Promise information can be found at http://www.the-dma.org.

[105] To remove themselves from participating national mailing lists, consumers can send their name and home address to: Mail Preference Service, Direct Marketing Association, Inc., P.O. Box 9008, Farmingdale, New York, 1735-9008. To remove themselves from participating national telemarketing lists, consumers can send their name, home address, and home telephone number to Telephone Preference Service, Direct Marketing Association, Inc., P.O. Box 9014, Farmingdale, New York, 11735-9014.

[106] *See* www.epic.org.

[107] *See* http://epic.org/#about.

[108] *See* www.internetalliance.org.

industry. It has worked with the National Consumers League and Internet companies to develop Project OPEN (The Online Public Education Network).[109] Project OPEN was created to develop an educational program to encourage safe online experiences for Internet users. Project OPEN offers useful consumer educational materials including an online consumer guide entitled "How to Get the Most out of Going Online."[110] A portion of the brochure provides helpful advice for users who want to protect their privacy, including the following:

1. Find out about your service provider's privacy policies and exercise your options for how your personal information may be used. 2. Recognize that when you communicate with others online, they may be able to find out how to communicate with you. Posting your name in a member directory, posting messages to a bulletin board, automated mailing list or newsgroup, or participating in a chat session will make your e-mail address available to strangers. Some may share your interests and provide you with useful information. But others may send you messages that you don't want. 3. Protect your password. Pick a password that's difficult for someone else to guess and change it frequently. Never divulge your password to anyone
who asks for it online. 4. Tell your children not to give out their names or other personal information online. Instruct them to ask your permission before responding to online surveys. 5. Take advantage of new software tools that give online users more ways to protect their privacy.[111]

5. Online Privacy Alliance.

The Online Privacy Alliance ("OPA")[112] is made up of over 70 companies and associations. OPA member companies have pledged to extend certain levels of protection to personally identifiable information and develop customized privacy policies. OPA generally requires its members to abide by five common standards: adoption (each member organization must adopt and implement a privacy policy), notice and disclosure (the policy must state the reason the information is being collected and to whom the information will be disseminated), choice and consent (the policy must state how the information will be disseminated and provide the consumer with either opt-out or opt-in choices), data security (the member organization should take reasonable measures to assure that personally identifiable information is protected from loss, misuse or alteration), and data quality and access (data should be accurate, complete,

---

[109] *See* http://www.Internetalliance.org/project-open/about.html.
[110] *See* http://www.Internetalliance.org/project-open/brochure.html.
[111] *See* http://www.Internetalliance.org/project-open/priv-broch.html.
[112] *See* http://www.privacyalliance.org.

current and protected against accidental or unauthorized alteration).[113]

The OPA website outlines basic rules that will allow consumers to better control their personal information from both a privacy and a security standpoint.[114] Specifically, OPA recommends that an Internet user do the following when entering a website:

• Look for a privacy policy that specifies exactly what information is collected and if the information will be shared. It should inform the user about the security used to protect their personal information and how they can access the information collected and maintained.

• Look for a privacy seal (discussed below) for indication that the site is adhering to its privacy policy. The seal programs are also set up to handle complaints by consumers who believe a site has violated their privacy.

• Do not give your password to anyone, use different passwords at different sites, and change it often. When choosing a password, never select a password that is in any way similar to your real name or to an online name. The safest passwords are ones that contain a mix of letters and numbers, are six characters or more, and that do not represent a word in any language spelled forward or backward.

• Use a secure browser which will scramble information when a purchase is made online.

6. Platform For Privacy Preferences.

The Platform for Privacy Preferences, or P3P, is a project undertaken by the World Wide Web Consortium[115] to develop technology to promote user privacy and confidence in the Internet by facilitating the disclosure of privacy practices with respect to data collected through web interactions. "P3P applications will enable sites to automatically declare their privacy practices in a way that is understandable to users' browsers. Privacy practices are embedded within the Website and users can rely upon their client to ensure their privacy concerns are respected."[116]

Thus, P3P technology would permit individuals to control their personal information and make decisions based on their individual privacy needs. Essentially, the P3P project enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine-and human-readable formats) and to automate decision-making based on these practices

---

[113] http://www.privacyalliance.org.

[114] *See* http://www.privacyalliance.org/resources/rulesntools.shtml.

[115] *See* http://www.w3org/P3P

[116] Press Release, "W3C Publishes First Public Working Draft of P3P 1.0," (May 1998) (available at http://www.w3.org/Press/1998/P3P.html).

when appropriate. They can also compare P3P policies with privacy preferences set by the user and take appropriate actions. P3P can perform a sort of "gate keeper" function for data transfer mechanisms such as electronic wallets and automatic form fillers. Thus, users will not need to read the privacy policies at every site they visit. Although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personally identifiable information, it does not provide a technical mechanism for making sure sites act according to their policies.

7. Privacy Rights Clearing-house.

The Privacy Rights Clearing-house ("PRC")[117] is a nonprofit consumer information and advocacy program established in 1992, that provides useful information for consumers interested in protecting their privacy online. For example, it suggests that consumers make themselves aware of what happens to their information when they give it out during everyday transactions and find out what personally identifiable information is already maintained by major industry and government da-

tabases. In this regard, PRC recommends that consumers annually check things such as credit reports and insurance company-generated medical reports once a year for accuracy.[118] PRC offers a hotline to report abuses and request information on ways to protect privacy, and fact sheets such as "Privacy Survival Guide," "How Private Is My Medical Information?" and "Privacy in Cyberspace: Rules of the Road for the Information Superhighway."[119]

V. Conclusion.

While new technologies that enhance consumer privacy continue to be developed and appear on the market,[120] the foregoing provides a sampling of some of the tools available to Internet users to protect their privacy. Users can choose from a variety of tools in order to achieve a desired individual level of comfort with respect to engaging in Internet commerce. Internet sites should continue to take proactive steps to further develop and post privacy statements, undertake measures to respond to consumer concerns about online privacy, and engage in meaningful self-regulation. Clearly, increased efforts to educate consumers with regard to the privacy implications of Internet use and how

---

[117] *See* www.privacyrights.org.

[118] *See* http://www.privacyrights.org/FS/fs1-surv.htm.

[119] *See* http://www.privacyrights.org/FS/services.htm.

[120] For example, IBM recently announced its development of new PC models (IBM PC 300 PL) that contain an embedded security chip that supports functions such as key encryption for privacy. According to IBM, " the chip also supports user privacy because it is designed to have the user control personalization and trust relationships, and no identification number is placed on the PC." While the PCs were developed for use by businesses, they are priced for consumer affordability, and provide an option for consumers concerned about privacy and security. *See* IBM Press Release, *"IBM Breaks Out the World's Most Secure Business PCs,"* (Sep. 21, 1999).

they can best protect their privacy online are necessary. Ultimately, effective industry self-regulation is essential to avoiding excessive government regulation in this area. An appropriate role of government with regard to ensuring Internet privacy is one that encourages and compliments the efforts of the private sector, and that will help Internet commerce continue to flourish.

At the same time, once informed of the issues, consumers need to take an active role in safeguarding the privacy of their personal information on the Internet by using the information and tools available. The Committee hopes that when consumers are empowered with the knowledge and tools to take steps to meet their privacy needs, consumers will have enhanced confidence in e-commerce. By taking an active role in protecting their own personally identifiable information, more and more consumers can enjoy the many benefits of the Internet while protecting their privacy, and Internet commerce can continue to grow and thrive.