

**Subj:** Online Privacy: Perspectives of America Online  
**From:** Jen Jacobsen, America Online, 202-530-7888, jgjacobson@aol.com  
**To:** Internet Caucus Advisory Committee

## Privacy and Consumer Confidence

### Issue Overview

Online privacy is one of the most important issues facing the Internet community today. While the online medium provides previously unforeseen opportunities for personalized interactive experiences that benefit consumers, it also brings with it concern about the protection of personal information that may be collected online. For AOL, protecting our customers' privacy is essential to earning their trust, which is crucial to the success of our business.

Recognizing the importance of this issue, AOL has taken a number of steps to create an environment where our members can be certain that their personal information and their choices regarding the use of that information are being respected: from creating and implementing our own privacy policies and educating our members about them, to promoting best practices among our business partners, to engaging in industry-wide initiatives and enforcement mechanisms that will raise the bar for all companies who do business online..

The tremendous growth of e-commerce has brought the online privacy issue to the fore, as consumers, policymakers, and businesses work to determine how best to protect the personal information of online users. In addition, online privacy has become the subject of international debate, as the U.S. and the European Union negotiate over the appropriate implementation of the European Directive on Data Protection, which imposes strict requirements on the handling of personal data and could ultimately disrupt data flows between the EU and U.S. if policy differences are not resolved.

### Where are We Now?

AOL is committed to protecting our users' privacy and building consumer confidence in the online medium. Building on the lessons we've learned and the input we've received from our members, we have adopted privacy policies that clearly explain to our users what information we collect, why we collect it, and how members can exercise choice about the use of that information.

We have based our policies on core principles that reflect consumer needs and expectations. For example, we will not read a member's private email; we will not disclose to anyone any information about where a member goes online; and we will not give out a member's phone number, credit card information, or screen name without consent. We also make sure that our policies are well understood and implemented by all our employees. We provide training about our privacy policy and require all employees to sign and agree to abide by the policy, as a condition of employment. We continually review state-of-the-art technology to ensure we use the most advanced technologies possible to defend our customer data security.

AOL takes extra steps to protect the safety and privacy of children online. We do not collect personal information from children without their parents' knowledge and consent. We have created a special environment just for children -- our "Kids Only" area -- and we carefully monitor all of the Kids Only chat rooms and message boards to make sure that a child does not post personal information that could allow a stranger to contact the child offline. Furthermore, through AOL's "Parental Controls," our members are able to safeguard their children's privacy by setting strict limits on whom their children may interact with and what they see online. AOL supported the Child Online Privacy Protection Act (COPPA), which became effective on April 21 of this year, as an important step toward protecting children online, because we believe that extra safeguards are necessary when it comes to the highly sensitive area of children's data.

In addition to adopting and implementing our own policies, AOL is committed to fostering best practices among our business partners and industry colleagues. One of the strongest examples of this effort is our "Certified Merchant" program, which guarantees that our members will be protected and satisfied when they are within the AOL environment. Through this program (which currently has nearly 200 participating merchants), we offer a money-back guarantee program to dispel consumer concerns about shopping security and to increase consumer trust in this powerful new medium. We believe that the more we are able work with our business partners and require high standards of them, the more likely it is that these standards will become the marketplace norm. Indeed, we think that protecting privacy is just one piece of our larger responsibility to help ensure that consumers are treated fairly and safely when they go online. AOL and several other industry leaders have created the Electronic Commerce and Consumer Protection Working Group, which is working to draft a code of online business practices that we hope will be endorsed by all companies doing business online.

The online industry as a whole has taken positive steps toward protecting online privacy in recent months. To strengthen industry's commitment to online privacy, AOL joined with other companies and associations in 1998 to form the Online Privacy Alliance (OPA), which has since grown to include more than 85 recognized industry leaders. A study conducted last year by Georgetown University Professor Mary Culnan shows that, in a sample drawn from a pool of the 7500 most visited websites, more than 65% of the sites have posted a privacy policy or a statement about their information practices. This number demonstrates a tremendous increase from the number of sites posting policies just one year earlier, when the FTC conducted a similar study.

### **Where Do We Go From Here?**

We believe that private sector leadership in developing fair information practices is the right approach to assuring broad privacy protection online, but we also realize that there is still more work to be done. In order to build on our preliminary success, the OPA has renewed its commitment to reach out to businesses nationwide to explain the importance of protecting online privacy and posting meaningful privacy policies.

As technology becomes faster and better, privacy protection will become even more essential, since information will be collected and processed at an even faster rate. In part, we think that technology holds the key to ensuring a safe and secure online environment. We believe it is critical for us to provide the most sophisticated security technologies to our

members so that they can take steps to protect their own privacy online. That's why we will continue to advocate the widespread availability and use of strong encryption, both in this country and abroad.

Industry initiatives are helping to craft the "rules of the road" that will dictate online business practices, and we believe that it is important to see how those rules will develop, rather than imposing a sweeping regulatory framework on the Internet and electronic commerce. The challenges that lie ahead will give us the chance to prove that we can work together to promote effective online privacy through industry-led, market-driven initiatives. In the meantime, AOL remains committed to protecting the privacy of our consumers and taking part in industry efforts to promote online privacy, security, and consumer confidence.

**Subj:** Online Privacy: Perspectives of Microsoft  
**From:** Bill Guidera, Microsoft, 202-263-5914, bguidera@microsoft.com  
**To:** Internet Caucus Advisory Committee

### Privacy In The Online World

Americans are in love with the Internet. Three-quarters of Americans under the age of 60 have used the Internet at work or at home, and 72 percent say the Internet has made their lives better. Meanwhile, Americans sent an estimated \$15 billion to \$20 billion last year online.

At the same time, Americans are becoming increasingly concerned that their privacy is at risk on the Internet. According to a Forrester Research survey of online users, 67 percent said they were "extremely" or "very" concerned about releasing personal information over the Web. Forrester estimates that those fears may have resulted in as much as \$2.8 billion in lost sales for Internet retailers in 1999.

Over the last year, the ability of Web sites to collect, combine, analyze and disseminate data has hit the radar screens of the public, government officials, the technology industry and the media in a huge way. Recently, considerable attention has been focused on the privacy practices and policies of many well-known companies, including Microsoft.

As a New York Times editorial last month noted: "Unless businesses can protect privacy, the erosion of trust could seriously harm e-commerce as well as cause the public to become wary about using the Internet for education, research and other important noncommercial functions." If that were to occur, it would be a shame, not only for consumers, but also for the high-technology industry.

As Microsoft continues to monitor and improve our own Web practices and policies, we are also committed to developing technologies and tools that will help lead the way in placing power and choice in the hands of consumers regarding the collection and use of their personal information. We are working with government leaders, industry, and nonprofit organizations like getnetwise.org, TRUSTe and BBBOnline, to find the best solutions for addressing the public's legitimate concerns. A key component is educating online users and helping them take advantage of current privacy tools and new ones as they are developed.

Microsoft believes that everyone has a right to know how their personal information and their Internet activity is used by the Web sites they visit. This commitment is built within a framework known as Fair Information Practices, which forms the foundation of our collection, storage, use and distribution of customer information. The Fair Information Practices, which are endorsed by the Federal Trade Commission (FTC), privacy advocacy groups and a growing number of technology companies, incorporate five key principles: notice, choice, access, security and enforcement.

To encourage other Web site operators to adhere to the Fair Information Practices, Microsoft has established a policy that we will only place corporate advertising on U.S. Web sites that conform to these practices. A growing list of other industry leaders, including IBM,

Disney, Novell and Compaq also have established policies designed to encourage Web businesses to disclose their information management practices.

On the technology front, we have worked with TRUSTe to create a privacy Wizard that has been used by more than 12,000 Web sites to create privacy statements that comply with the Fair Information Practices.

Next month, we will be launching Kids passport, a service to help parents manage the information their young children can provide to Web sites, and help online businesses comply with the Children's Online Privacy Protection Act of 1998. We are also working with the World Wide Web Consortium to create open standards for a new technology — called P3P — that will enable Web sites to automatically transmit details of their privacy policy and allow users to send back personal information only to sites with which they want to share that information.

In Washington, D.C., and in state legislatures, numerous proposals have been introduced to study the range of issues involved in the privacy discussion, or to regulate information practices. The Federal Trade Commission has convened a cross-section of industry and privacy advocacy groups, including Microsoft, to review two of the most important issues: access and security. The FTC also continues to survey how the industry is adopting Fair Information Practices.

At Microsoft, we recognize that protecting privacy is not only good for consumers; it is also good for the long-term viability of e-commerce. Given the diversity of views on how to tackle these issues, and the rapid pace of innovation and change on the Internet, a consensus view on a one-size-fits-all solution will be difficult to achieve. Working with our partners, others in the industry and with policy-makers, however, we are striving to make sure that both consumers and the high-technology industry come out as winners on these challenging issues.

***This is one in a series of essays on technology and its impact on society. More information is available at [www.microsoft.com](http://www.microsoft.com).***

**Subj:** Online Privacy: Perspectives of Progressive Policy Institute  
**From:** Shane Ham, Policy Analyst, Progressive Policy Institute, 202-608-1284,  
sham@dlcppi.org  
**To:** Internet Caucus Advisory Committee

**DoubleClick and Online Privacy**  
***The Risks of Overreaction, March 2000***  
**by Shane Ham and Robert D. Atkinson**

Online privacy is making headlines this month, with the revelation that DoubleClick, a leading provider of banner advertising for some of the most popular sites on the World Wide Web, is now capable of linking an individual's web surfing history to his or her name, mailing address, and shopping habits. The controversy has created some of the strongest calls yet for legislation to protect consumer privacy online.

The Progressive Policy Institute (PPI) believes that online profiling of web users is a valid business model, as long as protections are in place to give web users sufficient notice that profiling is taking place and adequate opportunity to choose not to participate. If Congress gives in to this latest wave of privacy hysteria, advertising revenues to Internet business could be significantly diminished and, as a result, the Internet as we know it—an almost limitless collection of freely accessible sites and services—may be crippled as it struggles to realize its full potential. We believe that if the Internet advertising industry adopts a stringent self-regulatory code, it will address consumer privacy concerns and obviate the need for legislation.

### **DoubleClick and Abacus Direct: The Facts**

DoubleClick operates as an advertising sales representative and placement service, delivering banner ads to more than 15,000 web sites. As with advertisers in more traditional media, a premium is placed on ads that can be delivered to specific audiences; the television commercials shown during **Monday Night Football** are much different than the ones shown during **Oprah**. DoubleClick engages in similar targeting, using Internet browser "cookies" to track web users as they visit web sites in the DoubleClick network and building a profile of the users' interests in order to target the ads more effectively. Until recently, DoubleClick kept these profiles completely anonymous, with no personally identifiable information collected or used.

That policy changed in November 1999, when DoubleClick acquired Abacus Direct Corporation. Abacus originally was organized as a cooperative between catalog retailers and direct marketers. The Abacus member companies combine the purchasing histories of their customers into one central database, creating detailed customer profiles—complete with names, addresses, and purchases—from which member companies draw in order to better target their marketing efforts. Abacus delivers to its customers a list of individuals who meet certain criteria, but the personal data is held as proprietary and is never shared with other companies.

With the acquisition of Abacus, DoubleClick plans to merge the online web surfing profiles with the purchase history profiles for even more accurate targeting. To do so, they will request that the web sites in their Abacus Online alliance forward personally identifiable information that users might enter when filling out surveys, making purchases, or accessing sites that require registration. DoubleClick will also collect personally identifiable information from their proprietary web sites, such as NetDeals.com. This profile data will be given voluntarily by the user (users have the ability to "opt out" of this data collection) and DoubleClick will not sell or transfer the profiles (i.e., John Smith visits skiing web sites and bought a snowboard last year) to any third party. The use of personally identifiable information represents a significant change from their prior privacy policies.

### **The Case Against DoubleClick**

DoubleClick has been the target of several lawsuits and complaints alleging that it engaged in deceptive and possibly illegal trade practices by not requiring their network of web sites to reveal their relationship with DoubleClick. If web users do not have proper notification that DoubleClick has placed a cookie on their browsers and is watching them surf the Internet, critics charge, users can neither give their informed consent to data collection nor opt out of that collection. Moreover, many privacy advocates believe that linking personally identifiable information with an individual's web surfing habits is a violation of an inherent right to privacy while online.

Needless to say, web users are upset and DoubleClick has suffered a hailstorm of negative publicity. Privacy interest groups such as the Electronic Privacy Information Center (EPIC), which filed a complaint against DoubleClick with the Federal Trade Commission, say that DoubleClick's actions constitute a failure of self-regulation in the privacy arena and call for legislative and regulatory action to clamp down on the collection and use of personal data by Internet web sites and advertisers. But rushing to write laws in the wake of this case would be a mistake.

### Putting the Problem in Perspective

Public concerns about online privacy are driven by several factors: unfamiliarity with Internet technology such as cookies, the rapid commercialization of the World Wide Web, and alarmist rhetoric by privacy advocates. Before making public policy decisions, it is important to consider the privacy issue in context.

The practices decried by privacy interest groups—delivering personally identifiable data on preferences and habits to marketers, without the knowledge or affirmative consent of the consumer—have been around for a long time. Buy a pair of khakis from a catalog and your mailbox will soon be flooded with competing clothing catalogs. Subscribe to an opinion magazine and you be swamped with solicitations from political action committees. Contribute to an environmental group, and you will be asked for money to save every animal from whales to kittens.

This free flow of personal data, even sensitive data such as political preferences and charitable giving, is widely considered to be little more than a nuisance, a junk mail problem rather than a privacy problem because it is understood that the personal data is used only for direct marketing and not more sinister purposes. While the Internet makes the collection and use of that data more efficient; the practice is not more malicious simply because it takes place in cyberspace. If anything, the Internet has made it easier than ever for consumers to opt out of the data collection. As long as the information is used only for marketing, and web users are able to opt out, it is hard to view this activity as a major threat to personal privacy.

Moreover, targeted advertising provides clear benefits to the consumer. The Internet is the most powerful consumer tool in history, providing not only vast amounts of information on which products are the best, but also the ability to shop all around the world for the best price without ever leaving home. But web users can only take advantage of that power if they know where to look. Advertising targeted at personal preferences and interests is one way to help consumers find web site needles in the Internet haystack.

Most importantly, there are myriad ways for web users to protect their privacy while online. Web browsers allow users to block some or all cookies from being deposited on their hard drives. There are also many programs, available for free on the Internet, that allow users to examine their cookies and delete any that they don't want. Special connections, or proxies, allow users to connect to the Internet anonymously, and are also free. Individual web users have more than enough tools to protect their own privacy without burdening those who are willing to make the trade-off between privacy and convenience.

### The Risks of Overreaction

Of course, concerns about privacy cannot be dismissed, and DoubleClick should be punished if their practices are found to be unfair or deceptive. At the same time, it is important that the federal government not react to the public furor over DoubleClick with unwise or overburdensome laws and

regulations. Consumer privacy interests must be balanced against the likely outcome of government action, and any government action must be undertaken with this central fact in mind: targeted advertising is critical to the continued growth of the Internet.

Many of the most important and useful sites on the Internet, from newspapers to search engines, rely on advertising to support their online operations. While generalized banner ads provide some revenue, their small click-through rates and the high odds of wasted impressions make them less valuable to advertisers. Targeted ads, on the other hand, are likely to have much higher rates of return, and advertisers will pay considerably more to place them.

Maintaining a high-quality web site is neither easy nor inexpensive—witness the large number of Internet sites that operate at losses of millions of dollars per year. As the high-flying technology stocks indicate, investors believe that the Internet will eventually shake out the best business models and become profitable. For the time being, however, the situation is precarious and the market is beginning to lose patience with the mounting losses. Without the revenue that targeted advertising is expected to bring, some of the best sites on the Internet may either start charging for access (an Internet death sentence) or close down altogether. If the former occurs, this will exacerbate risks of a digital divide, as only middle- and upper-income individuals will be able to afford access to many web sites.

More importantly, rushing to pass legislation in the wake of a high-profile case like DoubleClick is inherently risky. A highly politicized debate may result in excessively broad restrictions, swatting the privacy fly with a regulatory sledgehammer and crippling the growth of the Internet in the process by reducing the revenues available to Internet publishers. A number of bills have been introduced or are under discussion in Congress that aim to restrict the collection of personal data by marketers, but contain ill-advised provisions that will unduly tamper with the revenue potential of web publishers. The publicity surrounding the DoubleClick case makes the passage of such ill-considered legislation a real possibility.

### Industry Best Practices: Give Self-Regulation a Chance

In March 1999, PPI issued a paper on online privacy standards. In that paper, we argued that:

“[The federal government] should give the private sector time to build robust self-regulatory programs that give consumers greater control over the uses of their personal information ... If after a significant trial period self-regulation is not adopted by a large share of Web sites engaged in e-commerce, if consumer concerns regarding privacy on the Internet do not diminish, and if a record of significant abuses emerges, Congress should pass legislation empowering the Federal Trade Commission to protect consumer privacy in both online and direct marketing transactions.”<sup>1</sup>

A year has passed, and while the rise of online profiling raises potentially troubling new issues, we do not believe that it is time to throw in the towel on self-regulation. On the other hand, the organic development of a set of industry best practices is proceeding too slowly. The slow pace is shaking consumer confidence in electronic commerce and turning up the heat on lawmakers to take action. If Internet businesses want to avoid legislation, now is the time to develop an industry-wide privacy code for online profiling. At this early stage in the development of the Internet, the small number of online advertisers makes it possible to develop a self-regulatory code for online profiling that reaches 100 percent of the affected companies.

DoubleClick and its competitors have formed the Network Advertising Initiative (NAI) to develop such a code, but we believe the guidelines under discussion appear to be inadequate to address legitimate privacy concerns. Any online profiling privacy code should include, at a minimum, the following provisions:

---

<sup>1</sup>Randolph Court and Robert D. Atkinson, *On-Line Privacy Standards: The Case for a Limited Federal Role In a Self-Regulatory Regime* (Washington, DC: Progressive Policy Institute, March 1999).

- **Clear notice on every web site telling users what personal information may be collected by whom and how it will be used.** If a web site partners with marketing companies, such as DoubleClick, the name and URL (Internet address) of those companies should be clearly displayed, not merely referred to as “third parties.”
- **Prohibitions on selling or sharing personally identifiable profiles with other companies or third parties.** Advertisers should not under any circumstances share personally identifiable profiles with other companies, even with their business partners.
- **Clear and simple procedures to opt out of data collection.** Though some privacy advocates prefer that users “opt in” by giving affirmative consent for data collection, such a burden could mean the death of the targeted advertising business model. Many consumers do not mind if their personal information is collected and used, but would not go out of their way to give their permission to do so. If the opt out procedures are easy to find and execute, the protection should be sufficient for most consumers. Those who want more protection can set their browsers to refuse cookies or use any of the other freely available tools to make their web surfing completely anonymous.
- **Stringent guidelines on the collection of sensitive personal data.** Some personal data—such as credit card numbers, financial history, and medical information—are too sensitive to be used for marketing purposes. Such data, if collected by a web site, should be held to a higher standard of privacy and should not be used to develop profiles without explicit consent (opt in) from the consumer. Moreover, web sites should never collect data from children without express consent from a parent or guardian.
- **Notification on updates to privacy policies.** Frequent changes in privacy policies, especially changes that allow for more permissive use of personal data, tend to undermine consumer confidence in electronic commerce. When a web site changes its privacy policies, clear notification should be given to consumers to allow them to reevaluate their decision to permit data collection or to opt out.
- **Prohibitions on the use of data collected under more stringent privacy policies.** It would be inappropriate for a company to collect data from a web user under one policy and then use the data under a different policy. If a company engaged in online profiling decides to become more permissive in the use of the data collected from web users, that company should “reset the clock” and use only data that is collected going forward. Web users who no longer want their data to be used by a company because of changes to the privacy policy should be allowed to opt out retroactively, preventing the use of previously collected data even if that data is to be used strictly in accordance with the privacy policy under which it was collected.

### Conclusion

Every day thousands of people log on to the Internet for the first time. The technology is so powerful and so complicated that concern about online privacy is natural and healthy. But it is also easy to panic unnecessarily, especially when cases like DoubleClick raise important issues about data collection and anonymity. It is important for the future of a free and freely available Internet that we resist the urge to panic and demand government intervention. If, however, the industry is unable or unwilling to implement a sufficient self-regulatory regime, congressional action and federal regulation may be the only answers. But if such action is needed, it should be limited, specifically targeted at online profiling, and follow the guidelines above.

*Shane Ham is technology policy analyst at the Progressive Policy Institute, and Robert D. Atkinson is director of PPI's Technology & New Economy Project.*

Subject: Perspectives of the Center for Democracy and Technology  
From: Ari Schwartz, Center for Democracy and Technology, 202-637-9800,  
ari@cdt.org  
To: Internet Caucus Advisory Committee

PREPARED STATEMENT OF  
DEIRDRE MULLIGAN, STAFF COUNSEL  
THE CENTER FOR DEMOCRACY & TECHNOLOGY  
BEFORE  
SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY  
COMMITTEE ON THE JUDICIARY  
U.S. HOUSE OF REPRESENTATIVES  
OVERSIGHT HEARING  
ON  
"PRIVACY AND ELECTRONIC COMMUNICATIONS"  
Thursday, May 18, 2000

Mr. Chairman and members of the Committee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about the important subject of privacy on the Internet. CDT is a non-profit, public interest organization that is dedicated to developing and implementing public policies to protect civil liberties and democratic values on the Internet. CDT has been at the forefront of efforts to establish and protect the very high level of constitutional protection that speech on the Internet has been afforded by the United States Supreme Court in the *Reno v. ACLU*<sup>2</sup> decision, and to develop sound public policies and technical solutions to protect individual privacy.

Mr. Chairman, the Internet is at a critical junction in its evolution. Although as a popular mass medium the Internet is less than ten years old, it is already entering into a period of significant transformations. Today I would like to address the privacy issues facing individuals -- in their roles as citizens and consumers -- on the Internet.

## I. PRIVACY

The critical starting point on the privacy questions is the current state of privacy (and citizens' expectations of privacy) and the ways in which the evolution of the Internet may threaten privacy principles. As many of you know, the Center for Democracy & Technology has long been an advocate for protecting privacy on the Internet, and we have previously had the privilege of addressing this Subcommittee on privacy issues. This morning I will briefly summarize our analysis of privacy issues on the Internet.<sup>3</sup>

CDT believes that a key privacy consideration should be individuals' long-held expectations of autonomy, fairness, and confidentiality, and policy efforts should ensure that those

---

<sup>2</sup> *American Civil Liberties Union v. Reno*, 929 F. Supp. 824, 844 (E.D. Pa. 1996), *aff'd*, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

<sup>3</sup> For a fuller exploration of these issues see, e.g., Testimony of Deirdre Mulligan, Staff Counsel of the Center For Democracy & Technology, Before the Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation, July 27, 1999.

expectations are respected online as well as offline. These expectations exist vis-à-vis both the public and the private sectors. By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified. Fairness requires policies that provide individuals with control over information that they provide to the government and the private sector. In terms of confidentiality, we need to continue to ensure strong protection for e-mail and other electronic communications.

As it is evolving, the Internet poses both challenges and opportunities to protecting privacy. The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals' use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints could reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy.

## **II. PROTECTING PRIVACY ON THE INTERNET REQUIRES A MULTI-PRONGED APPROACH THAT INVOLVES SELF-REGULATION, TECHNOLOGY, AND LEGISLATION.**

On self-regulation, we must continue to press the Internet industry to adopt privacy policies and practices, such as notice, consent mechanisms, and auditing and self-enforcement infrastructures. We must realize that the Internet is global and decentralized, and thus relying on legislation and governmental oversight alone simply will not assure privacy. Because of extensive public concern about privacy on the Internet, the Internet is acting as a driver for self-regulation, both online and offline. Businesses are revising and adopting company-wide practices when writing a privacy policy for the Internet. Efforts that continue this greater internal focus on privacy must be encouraged.

On the technology front, while the Internet presents new threats to privacy, the move to the Internet also presents new opportunities for enhancing privacy. Just as the Internet has given individuals greater ability to speak and publish, it also has the potential to give individuals greater control over their personal information. We must continue to promote the development of privacy-enhancing and empowering technology, such as the World Wide Web Consortium's Platform for Privacy Preferences ("P3P"), which will enable individuals to more easily read privacy policies of companies on the Web, and could help to facilitate choice and consent negotiations between individuals and Web operators.

On the public policy front, we must adopt legislation that incorporates into law Fair Information Practices -- long-accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared."<sup>4</sup> Legislation is necessary to guarantee a baseline of privacy on the Internet, but it is

---

<sup>4</sup> Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967) 7. The Code of Fair Information Practices as stated in the Secretary's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, U.S. Dept. of Health, Education and Welfare, July 1973:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

not one-size-fits-all legislation. Privacy legislation must be enacted in key sectors such as privacy of medical records. For consumer privacy, there needs to be baseline standards and fair information practices to augment the self-regulatory efforts of leading Internet companies, and to address the problems of bad actors and uninformed companies. Finally, there is no way other than legislation to raise the standards for government access to citizens' personal information increasingly stored across the Internet, ensuring that the 4th Amendment continues to protect Americans in the digital age.<sup>5</sup>

### III. CONCLUSION

The history of the Internet, in general, is that policy regimes are first created by consensus among a broad cross section of the community. CDT is committed to participating in any process that helps to build a new social contract embodying democratic values in the emerging online world. The work of the Federal Trade Commission – through its public workshops, hearings, and its recent Advisory Committee on Online Access and Security – provides a model of how to vet issues and move toward consensus. We look forward to working with this Committee, as well as others, the industry and the public interest community to build a cohesive system of privacy protections for the online environment. Thank you for the opportunity to participate in this timely hearing.

---

4. There must be a way for the individual to correct or amend a record of identifiable information about him.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

The Code of Fair Information Practices as stated in the OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data [http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV\\_EN.HTM](http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV_EN.HTM):

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.

5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and, in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

<sup>5</sup> See, Testimony of Deirdre Mulligan, Staff Counsel of the Center for Democracy & Technology, before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, March 26, 1998, at 11-13 (concerning disclosure of subscriber information to the U.S. Navy).

**Subj:** Online Privacy: Perspectives of San Francisco Bay Area Network on Disability (SF BAND)  
**From:** Jean Nandi, SFBAND, 202-530-7888, jeannandi@aol.com, <http://members.aol.com/jeannandi/HOMEPAGE/SFband.html>  
**To:** Internet Caucus Advisory Committee

### Is The Internet Generally Eroding or Enhancing Individual's Privacy?

Persons with disabilities are increasing their use of the Internet for researching information about their disabilities and illnesses. We are using the Internet to access government websites for information about laws and regulations that affect their lives. We use the Internet to acquire an education, formally or informally. Wherever possible, we use the Internet to pay bills, to fill out government forms, to shop for medical supplies, for books, for travel services, even for groceries. We use the Internet increasingly for socializing and for supporting each other in coping with their disabilities.

People who are significantly disabled have found the Internet a boon for carrying out these everyday occupations, and may indeed be entirely dependent on the Internet for doing these things. This makes us potentially extremely vulnerable to Internet practices which result in private information about the websites we frequent and purchases we make, as well as email addresses, social security numbers, credit card numbers, and the like being accessed by programs run by commercial enterprises seeking to make a profit by the use or misuse of this information. Worse, members of the disability community have been increasingly suspicious of proposals by government agencies to collect genetic information, data on births of persons with various "defects," and other medical information purportedly sought for research purposes. While the Internet has a potential for assisting in providing medical information or purchases of prescription drugs and the like, patients are leary of having their private medical information or medical records stored where they can be accessed online for potentially unscrupulous purposes.

As SF BAND member Maggie Dee has stated, "Privacy means protection from the unwanted invasions by medical, professional and legal entities that do not belong in my life. I want to be in control over who gets my information and for what purpose. To think that my privacy could be violated! And now I realize that it has. Why offer the world (the Internet) to a person, otherwise confined to a day-in-day-out one-room existence, only to have that small private space no longer under the control of the person living in that space? Rather it is filled with filth, with loan offers to the poverty stricken--shams, advertisements that have nothing to do with anything in your own life. And the more you share of a person's life, the more an entity can keep digging for more. It is a disgrace that anyone should have access to my personal information. Yet, I am realistic. I know that every time I sign up for anything online I suddenly get a slew of advertisements that I did not ask for, nor would have asked for."

Even more ominous is this additional thought, indicating a fear of the utterly unscrupulous accessing personal information. "The more I hear on TV about youngsters cracking corporate and government computers, the more I stop and think about the harm such violators can cause....always building the better mouse trap."

But is there anything, really, to be done about this? For the most part, "caveat emptor" would seem to be the only practical approach--forewarned is for the most part forearmed. However, when Internet Service Providers sell their subscriber lists, here is a recommendation from one of our members: "The service providers should be taxed heavily for selling these lists and should be required to notify people that this is being done and required to offer at the same price service that does not send cookies."

For advocacy groups operating news groups and listservs, the leader of a nonprofit promoting independent living for persons with disabilities (SF BAND member Patrick Connally) has this to say: "One of the big concerns this week in California's disability community, has been that studies by psychologists, social science types, and marketing people have been based on spying in chat rooms and email lists. I don't mind. My policy is that email lists, chatrooms, and the Internet are not ways to share confidential information. They are very open media sources and, like commercials on TV, a cultural monitor."

"The non-profit organization I am with (Disability Rights Enforcement, Education and Services, or DREES) hosts an unmoderated email listserv (drees@marin.org). We tell new members that posting to the list is like writing letters to the editor, their emails are published as if in a newspaper or magazine. What is written and posted on the listserv already can reach a hundred people, and can reach all of disabilitydom if it is good enough. A good piece might be passed on to thousands of others in local newsletters and other lists."

"It is certainly in bad form to spy in Internet spaces which are open to all. If I were doing the research I would introduce myself and outline my project. However, when it comes to moderated or limited access Internet spaces, such as support groups, I think spying or not telling people that they will be studied is very wrong. It works against competent therapy or preventive interventions because it undermines the basic trust in any practicing professional. I do not know what to do about marketers, but social scientists should not tolerate it. On the other hand, look at the good side of the Internet for the 'studied' classes. For the first time large numbers of people with disabilities, their families and their supporters can be reached without going through a service agency. The Internet is direct to the people."

"As a person with a disability, I often feel like a study object. I often think that the Internet would make it possible to develop a convenient template survey answer so I do not have to keep answering the same questions on every disability consumer survey. It would be rather like a resume, and every year my friends and I could worry about updating our survey template. There would be workshops and training on how to making your survey attractive to potential researchers. We could even hire each other to fill-out the forms! An annual survey could begin a whole regulatory process with office staff to ensure that only real institutional providers submitted proper survey forms as part of a comprehensive plan to stop patient abuse. Makes as much sense as all the current Medi-Cal paperwork which purports to stop fraud, or the 25 years of studies, pilot programs and surveys I have witnessed about personal assistance, attendants, home health aids or whatever the funders and regulation-huggers want to call these important people. Studies are still being funded and rotten wages are still being paid to workers. The Internet has not changed the fact that the money is there to study, but not to pay workers or to provide needed technology and other assistance."