Testimony and Statement for the Record of

Marc Rotenberg, Director
Electronic Privacy Information Center

Hearing on S. 809
The Online Privacy Protection Act of 1999

Before the

Subcommittee on Communications
Committee on Commerce, Science and Transportation
U.S. Senate

July 27, 1999
253 Russell Senate Office Building

My name is Marc Rotenberg.1 I am the Director of the Electronic Privacy Information Center. EPIC is a public interest research organization that helped organize the campaign against the Clipper encryption scheme, published the first comprehensive report on Internet privacy policies, and continues to be involved in many of the leading debates concerning privacy and civil liberties.2

Thank you for the opportunity to testify today on S. 809, the Online Privacy Protection Act of 1999. I appreciate the efforts of the bill's sponsors and the members of this Committee to further efforts to protect privacy on the Internet.

Summary

First, the FTC Report to Congress on Privacy Online was disappointing in many respects. It said hardly anything about the problems consumers face today trying to protect their privacy on the Internet, or whether any of the trade group proposals for self-regulation are actually working. It failed to report on the handling of privacy complaints received by the Commission as well as the disposition of actions referred to the agency. The Commission made no mention of the recent rejection of the self-regulatory approach by the European governments. This was all the more remarkable since it obviously bears on the efforts of the FTC and the long-term implications for electronic commerce. Whatever one's views may be about how best to protect privacy on the Internet, I think most would agree that the FTC has a responsibility to provide more complete information than was contained in this recent report.

Second, the recent developments in the online industry make clear the need for privacy legislation. For those who are willing to look closely, there is little indication that self-regulation is working. Privacy policies read more like warning notices and disclaimers. The proposed merger of Internet advertising giant Doubleclick and the largest catalog database firm Abacus demonstrates many of the shortcomings of the self-regulatory approach. The merger would significantly undermine online privacy as advertising is radically transformed. In the absence of a legal framework for online privacy, Internet-based services are also being offered without privacy protections that

[1] Executive director, Electronic Privacy Information Center; adjunct professor, Georgetown University Law Center; editor, *The Privacy Law Sourcebook 1999: United States Law, International Law, and Recent Development;* editor (with Philip Agre) *Technology and Privacy: The New Landscape* (MIT Press 1998).
[2] The Electronic Privacy Information Center is a project of the Fund for Constitutional Government, a non-profit charitable organization established in 1974 to protect civil liberties and constitutional rights. More information about EPIC is available at the EPIC web site http://www.epic.org.

would otherwise be required. The Internet is quickly becoming a privacy-free zone, where companies can push new products past an unsuspecting public.

Third, S. 809 offers a very good starting point for real privacy protection on the Internet. While there are several changes that should be made to the bill, S. 809 could accomplish two significant goals. It could give consumers in the United States better assurance that their personal information will be protected against misuse and improper disclosure. It could also help resolve the ongoing dispute with the Europeans over privacy protection, at least with regards to the Internet. In fact, I am reasonably certain that if a modified version of S. 809 were enacted, European governments would view U.S. privacy protection for the Internet as "adequate" for most purposes. This could be critical to the future of electronic commerce.

Finally, I hope the Committee might also consider other steps that could be taken to protect privacy on the Internet. These could include the establishment of a privacy agency that could act as a genuine advocate for privacy protection within the federal government, the development of new privacy-enhancing techniques, and additional efforts to ensure implementation and enforcement of Fair Information Practices.

The FTC's Incomplete Report

The FTC Report "Self-regulation and Privacy Online: A Report to Congress" is one of the oddest reports on privacy ever produced by a government agency. It doesn't actually discuss any of the specific threats to privacy. It doesn't evaluate the effectiveness of the recommendations put forward. It doesn't report on the status of any of the thousands of privacy complaints that the FTC has received from American consumers, or even on the high-profile cases that have been widely reported in the national media. It makes no mention of the multiple polls that show public support for privacy legislation. Nor does it report the fact that the European governments have recently rejected the U.S. self-regulatory approach or what the consequences of this might be for international trade.

The report does, however, rely heavily on an industry-funded study that found industry is doing a good job protecting privacy. It does describe in some detail various industry programs and actually includes price information for prospective customers. It endorses a technical standard that will make it easier, not more difficult, to collect personal information.

To the extent that the FTC does actually offer an assessment of the current state of online privacy, the picture is not encouraging:

> The vast majority of even the busiest web sites have not implemented all four substantive fair information practices principles . . . the seal programs discussed below currently encompass only a handful of web sites.

But the FTC then quickly says "Thus, it is too early to judge how effective these programs will ultimately be in serving as enforcement mechanisms to protect consumers online privacy." The FTC could have said more simply and directly, "After several years of prodding and promoting, industry self-regulation today offers little in the way of meaningful privacy protection for consumers on the Internet. A legal framework that provides simple, predictable, uniform privacy safeguards would be more sensible."

The Georgetown Survey

The FTC's conclusion that self-regulation is working relies heavily on the "Georgetown Internet Privacy Policy Survey." That survey was paid for by several industry groups that are deeply involved in promoting industry-sponsored programs as an alternative to legislation. In fact, a related survey also described in the FTC report was specifically commissioned by the Online Privacy Alliance, another industry organization.

What did the survey find? The vast majority of web sites offer little more than a simple notice that personal information is being collected from web users when they go to a web site. Less than ten percent of the sites describe even a basic set of privacy principles, and of that group there is no indication whatsoever if any of these policies are followed in practices. This was described by the groups that sponsored the survey and by the FTC as "progress."

EPIC conducted the first comprehensive survey of web site privacy policies back in 1997. We reviewed 100 of the most frequently visited web sites on the Internet.3 We checked whether sites collected personal information, had established privacy policies, made use of cookies, and allowed people to visit without disclosing their actual identity.

We found that about half of the sites that we surveyed in 1997 collected personal information. This was typically done for on-line registrations, surveys, user profiles, and order fulfillment. We also found that few web sites had explicit privacy policies (only 17

[3] EPIC, "Surfer Beware I: Personal Privacy and the Internet" (1997) [http://www.epic.org/reports/surfer-beware.html]

of our sample) and none of the top 100 web sites met basic standards for privacy protection. We also noted that users were unable to exercise any meaningful control over the use of cookies. However, we noted that anonymity played an important role in online privacy, with many sites allowing users to access web services without disclosing personal data. We recommended that:

- Web sites should make available a privacy policy that is easy to find. Ideally the policy should be accessible from the home page by looking for the word "privacy."
- Privacy policies should state clearly how and when personal information is collected.
- Web sites should make it possible for individuals to get access to their own data.
- Cookies transactions should be more transparent.
- Web sites should continue to support anonymous access for Internet users.

I would agree that since the time of the EPIC survey in 1997 more web sites are posting privacy policies. But for reasons described below, these policies offer little in the ways of actual privacy protection. On the other critical issues identified by the 1997 EPIC survey – access to records, use of cookies, support for anonymity – the movement seems to be in the wrong direction: more detailed profiles are being created without permitting user access, cookies remain essentially impossible for users to control, and anonymity is increasingly under assault. The FTC report would have been more meaningful and more useful if these issues were also discussed.

Discussion of Industry Programs

Consider also the FTC discussion of Truste, one of several seal programs put forward as an alternative to privacy legislation. The FTC "Report to Congress" describes the Truste program in terms taken directly from Truste's own web site and marketing literature.4 The FTC describes the program as "comprehensive," mentions "monitoring and oversight" by Truste as well as a "complaint resolution procedure." The FTC states matter of factly that "licensees must provide consumers with a way to submit concerns regarding their information practices, and agree to respond to all reasonable inquiries within five days." Further on, the FTC states "Truste provides for public reporting of complaints, and in appropriate circumstances, will refer complaints to the Commission."

[4] The FTC does acknowledge in footnote 45 that the "information in this section is taken from materials posted on Trustee's web site, and from public statements by Truste staff." The items in my testimony were taken from news reports easily located on the Internet by using such search terms as "privacy" and "Truste."

What is remarkable about this summary is that there is no effort to evaluate any of these claims, even after problems have been widely reported in the national media and even after the FTC said complaints would be forwarded to the Commission.

There was for example the highly publicized question of whether Microsoft failed to comply with the Truste guidelines when it established a unique identification scheme that would have enabled widespread tracking of online consumers. Jason Catlett, one of the leading experts on industry self-regulation, filed a complaint with Truste after extensive evaluation of the privacy risks posed by the Microsoft scheme. Truste concluded that Microsoft did "compromise consumer trust and privacy," but did not breach Truste's licensing agreement. Consequently Truste did not require a third-party audit, nor did it impose any penalty beyond this verbal rebuke. Mr. Catlett called this an "utterly predictable failure of self-regulation" and asked the FTC to investigate Microsoft.

What is the FTC's evaluation of all this? Does it bother the FTC that Microsoft can "compromise consumer trust and privacy," but not violate a self-regulatory program intended to establish trust – called "Truste" – and protect privacy? Not a word on this is found in the FTC report.

This was hardly the first time that the effectiveness of the Truste program was called into question. A federal agency recently backed off plans to add a Truste seal after questions were raised about whether the seal program actually complied with the requirements of the federal Privacy Act. Earlier in the year, Truste awarded a seal to Geocities even though the company got into trouble for secretly selling personal information about users -- such as income and occupation -- to marketers in violation of its own privacy policy. And the original Truste effort to support anonymous transactions, which was supported by privacy advocates and experts, was dropped after industry objection.

It may be the case that, these problems aside, Truste is doing a good job overall and is on the right track. It may also be the case that the Truste program is seriously flawed and unlikely to produce any meaningful privacy protection for online consumers. That is a question that should be examined carefully and thoughtfully, but the FTC has offered no information that would allow the Congress or the public to begin that evaluation. We don't even know how many complaints from Truste were in fact referred to the Commission.

The reports on OPA and BBB Online followed a similar approach – reprint the materials available at the web site, offer little independent evaluation, ignore the widespread reports of abuse and problems in the national media or those lodged by the public with the Commission. I was so surprised by the lack of interest that the FTC showed in the actual operation of these programs and the problems that consumers face trying to protect their privacy on the Internet that we filed a Freedom of Information Act request with the FTC to obtain information about how in fact the FTC handles privacy complaints. .5 I will be pleased to provide this information to the Committee when we receive it from the Commission

Ignoring Privacy Experts, Academics, Consumer Groups and the General Public

For several years, the FTC has ignored the recommendations of experts, academics, and the public to examine seriously the adequacy of self-regulation to protect online privacy. In 1997, following an earlier recommendation on self-regulation, leading consumer and privacy organizations wrote to Senator McCain to object to a report submitted to this Committee. Those organizations wrote "the FTC preliminary assessment does not accurately reflect the substance of the hearings or the views of the consumer organizations that participated. We are both disappointed and troubled by the FTC report."6

Presciently, in light of recent developments, the groups wrote

> Instead of reporting the clear results of the survey research presented and the views expressed by groups representing consumers at the FTC hearing, the FTC chose instead to present the views of industry lobbyists as if they were the views of American consumers. . . . Second, the FTC letter goes to great length to applaud the efforts of a handful of companies to develop privacy policies. But nowhere in the letter is there any specific discussion of the specific threats to personal privacy by the on-line industry. . . . Third, the FTC endorses a series of vague proposals made by industry groups without any discussion of the adequacy, desirability, or consumer acceptance of these approaches. Virtually every industry

[5] Letter to FOIA/PA Officer, Federal Trade Commission, June 10, 1999 ("We request copies of all records concerning the FTC's investigation of privacy complaints. This request includes, but is not limited to, letters, electronic mail, web submissions, fax transmissions, and formal complaints. We are interested in (a) records regarding alleged privacy violations by a specific company or organization and (b) requests for general assistance in a privacy matter, whether or not a specific company or organization is indicated.")

[6] Letter to Senator John McCain, August 1, 1997 (from Center for Media Education, Privacy Rights Clearinghouse, Privacy Times, Electronic Frontier Foundation, Consumer Federation of America, EFF-Austin, Consumer Project on Technology, Electronic Privacy Information Center, Privacy Journal) [http://www.epic.org/privacy/databases/ftc_letter_0797.html]

recommendation put forward at the FTC workshop requires placing new burdens on consumers to protect their privacy. Many were roundly criticized by consumer groups. None of these problems were discussed in the letter to you.

A similar letter was sent to the Department of Commerce by more than seventy leading privacy advocates, scholars, consumer organizations and technical experts, urging a careful assessment of whether self-regulation would be an effective means to protect on-line privacy. The FTC has ignored that letter as well.

Finally, my own organization, which conducted the first comprehensive survey of web site privacy policies, warned in 1997 that it would be critical to assess the effectiveness of self-regulation to determine whether in fact it would provide privacy protection. Two years later, the FTC is still unable or unwilling to answer this central question.

The FTC wrote in the introduction to the Online Privacy Report that it would "present its views on the progress made in self-regulation since last June, as well as its plans to encourage industry's full implementation of online privacy protections." It did neither. In fact, this hardly seems a report to Congress from a federal agency concerned with privacy. It is rather a good industry briefing paper that was printed on FTC stationary.

The Lessons of Doubleclick

To understand what is happening with online privacy in the world of self-regulation, it is helpful to actually look at industry practices. Many of the problems with self-regulation can be understood by examining the recently announced merger of Doubleclick and Abacus. Abacus Direct manages the largest database of consumer catalog purchases in the U.S. It holds records from 1,100 catalogs direct marketers use to predict purchasing behavior in 88 million U.S. homes.

According to DM News, DoubleClick will be able to combine its ad placement technology used in 7,400 Web sites worldwide with data from Abacus' co-op database. Abacus in turn will use DoubleClick's technology to help its catalog customers attract traffic to their Web sites.7 Doubleclick has said that the merger would create "the worldwide leader in online advertising and database marketing."8

[7] DM News, Thursday, July 8, 1999, "Privacy Clouds Abacus-DoubleClick Merger's European Opportunities" [http://www.dmnews.com/articles/1999-07-05/4182.html]

In practical terms, advertising will be radically transformed. Where once advertisers could reach segmented markets and still allow potential customers who browsed a news magazine or watched a television show to safeguard their privacy, now advertisers will literally be watching potential customers even as those customers are reading web-based ads. Enormously detailed secret profiles of Internet users will be developed based on transactional records, purchase histories, and clickstream data.

This is all the more remarkable since the Doubleclick advertising network was widely touted as promoting anonymity and avoiding the collection of personally identifiable information. Doubleclick's privacy statement says that Doubleclick cookies are assigned a unique ID number, but do not collect personally identifiable information.9 This sample policy is published on more than a thousand web sites that are part of the Doubleclick network.

Here is a sample notice from the Dilbert site:

> Doubleclick uses cookies to make sure that you do not see the same advertisements repeatedly and when possible, shows advertising that is relevant to you based on what you have seen previously. Cookies are anonymous. Doubleclick does not know the name, e-mail address, phone number, or home address of anybody who visits the United Media site or any other site in the Doubleclick Network. All users receiving an ad from Doubleclick through the United Media site therefore remain entirely anonymous to Doubleclick; Doubleclick does not have any information to sell or rent to other parties.10

Here is the notice from one of the leading search engines:

> AltaVista is Anonymous
>
> Compaq Computer Corporation and our ad partner, Doubleclick, does not know the name, email address, phone number, or home address of anybody who visits

---

[8] "DOUBLECLICK INC. AND ABACUS DIRECT CORPORATION TO MERGE IN A $1 BILLION STOCK TRANSACTION- Merger Creates The World's Leading Online Advertising And Database Marketing Company," June 14, 1999 [http://www.doubleclick.net/company_info/press_kit/pr.99.06.14.htm]

[9] Doubleclick Privacy Statement - The Global Internet Advertising Solutions Company (visited Jun. 16th, 1999), <http://www.doubleclick.com/company_info/about_doubleclick/privacy/>.

[10] Dilbert TV, http://www.comiczone.com/comics/dilbert/tvshow/site/privacy.html.

> AltaVista. All users who receive an ad targeted by DoubleClick's Dart technology remain completely anonymous. Since we do not have any information concerning names or addresses, we do not sell or rent any such information to third parties. Because of our efforts to keep users anonymous, the information Doubleclick has is useful only across the Doubleclick Network, and only in the context of ad selection.11

It is also worth noting that Doubleclick is a leading member of both the Online Privacy Alliance and Truste, two of the organizations favorably reviewed by the Federal Trade Commission, that have touted self-regulation as an effective alternative to legislation.

Several lessons are clear. First, these privacy policies are essentially meaningless. How seriously should consumers take online privacy policies when a company can simply announce that they are "subject to change"? It's particularly lucrative for the company to post an enticing policy, gather the data, and then change its practices. This is exactly why legislation is necessary – to prevent the widespread deception that results from the lowering of privacy safeguards.

Second, consumers have no practical means to exercise privacy control with many of the major online players. What exactly would it mean for a consumer to exercise a privacy choice for "Doubleclick"? Customers do not actually buy any products from this company or have any direct commercial relations. Yet this company will quickly amass a more detailed profile of buying habits and personal preferences than virtually all of the companies that they might deal with directly.

Third, it should be obvious that without privacy restrictions, firms in the marketing field are going to merge. Why shouldn't they? The resulting databases of personal profiles have enormous commercial value. Consumers without any legal control over their data are in no position to object. And competitors of Doubleclick will be hard pressed not to follow suit. In the absence of a privacy baseline, companies trying to do the right thing are effectively punished in the marketplace. Self-regulation rewards bad actors.

Privacy rules would do a lot to reestablish fairness in situations such as the proposed merger. First, companies such as Doubleclick would be required to obtain consent from prospective customers under honest and accurate circumstances rather than being rewarded for their deceptive practices. Second, the firm would be required to make

[11] http://www.altavista.com/av/content/privacy.htm.

available to customers the profiles that would result from the merger. Consumers would have the right to see those profiles and to understand the decisions that affect their opportunities. Third, companies that are trying to uphold privacy policies would not be forced to compete with others that are cutting corners or lowering standards.

The FTC's silence on the Doubleclick-Abacus merger reflects not only a lack of understanding about the operation of Fair Information Practices but also a lack of concern for the future of online privacy. The recent experiment with self-regulation shows also that there is no real check on industry's information collection practices. The policy of self-regulation does not respond effectively to privacy concerns and will eventually erode all expectations of privacy on the Internet.

Comments on S. 809, The Online Privacy Protection Act

The Online Privacy Protection Act, S. 809 attempts to establish comprehensive privacy policies based on enforceable Fair Information Practices. These include a notice based on purpose specification so that people will know how their information will be used,12 the right to limit the disclosure of personal information to others,13 the right to obtain access to personal information,14 and the responsibility to ensure reasonable procedures to protect confidentiality, security, and integrity of personal information.15. This is a very good articulation of Fair Information Practices and it is consistent with many privacy laws in the United States and around the world.

The first set of problems with S. 809 will arise with the exceptions. For example, what is the purpose of subsection (b)(2) which lifts purpose limitation for transactional information, legitimate business activity, or an open-ended "to the extent permitted under other provisions of law"? These exceptions could easily undermine the very good intentions of the Act. Transactional information, for example, is elsewhere defined in the Act as "information generated in connection with the processing of requesting, accessing, or otherwise using the Internet." 16 This could include web logs, clickstream data, and a whole range of personally identifiable information that should be subject to Fair Information Practices, and destroyed or deidentified as soon as possible. It would be relatively easy to fix this problem by simply indicating that the requirements do not apply for transactional information "where identifiable information is removed." Perhaps this was the intent of the bill's sponsors. It would certainly be consistent with other privacy measures.

[12] Sec. 2(b)(1)(A)(i).
[13] Sec. 2(b)(1)(A)(ii).
[14] Sec. 2(b)(1)(B)(i)-(ii).
[15] Sec. 2(b)(1)(C).
[16] Sec. 8(7).

Also, subsection (b)(3) drops the access requirement for a whole range of data processing activities including transactional information, confidential information, data for internal use, information that is destroyed, and information that has no impact on the individuals.17 The problem with the exception for transaction information is as described above. Information that is essentially ephemeral is not generally subject to Fair information Practices. The remaining three categories are more problematic.

Companies clearly have a commercial interest in controlling disclosure of confidential information, but it is not clear that this interest should always trump the privacy interests of the data subject. If those confidential techniques are based on methods that are unfair or discriminatory, then consumers should know. It may even be the case that companies should be prepared to sacrifice some of their secrecy if they are developing extensive profiles on customers. Otherwise the claim of confidentiality will effectively become a screen to shield business practices, however privacy invasive.

The exception for internal use is also too broad. It is well understood that privacy protection is not just about limiting disclosure to third parties. Individuals retain the right to gain access to information even when it is not disclosed to others. This is the routine practice for educational and employment records and it will be appropriate as commercial records on individual consumers become more detailed and consolidation across industry sectors continues. If companies such as Amazon, AOL, and Microsoft develop detailed profiles for their customers across a range of transactions, why shouldn't those profiles be available to the customer? Without access to such information, customers will be unable to make meaningful choices about whether to do business with a large firm.

Generally speaking, the purpose of the access provision in Fair Information Practices is to avoid the risk of secret databases and to give individuals greater control over information held by others. If a firm has a detailed profile on a customer, what is the justification for not allowing that customer to see the profile?

While many in industry have complained that it may be too difficult or costly to comply with Fair Information Practices and therefore push for these exceptions, the Internet should make it much easier to follow standard privacy practices. Is there really any reason that companies cannot routinely make profile information directly available to their customers so that customers know what the companies know? There are many businesses on the Internet today, from airline companies to online trading and banking

[17] Sec. 2(b)(3)(A)-(E).

firms, that are giving their customers much greater access to the personal information that they collect and building trust and understanding in the process.

Ironically the firms and trade groups that most resist privacy rules are invariably the most secretive. They don't want their customers to know what they know about them or how they got the information. They don't want their customers to exercise any meaningful control over their personal information, and they are afraid that if you or the customers found out how they really operated – how much information they have on Americans and how it is used – they would be forced out of business.

Section 3 raises a different problem. It will allow companies to avoid the regulatory requirements of Section 2 by following a set of self-regulatory guidelines issued by industry and approved by the Federal Trade Commission. It is possible that at some point in the future such an arrangement could work, but I do not have confidence that it would work at this point. As things currently stand, the industry guidelines are too weak and the FTC is lacking the critical judgment to assess whether in fact the policies effectively protect privacy. These determinations should be subject to the Administrative Procedures Act or similar procedures and allow interested parties, most notably customers and prospective customers, the opportunity to report to the FTC any information that might be relevant to the FTC's determination.

Section 4 describes the procedures for state attorneys general to bring actions where regulations issued by the Commission may have been violated. It gives the FTC a significant role in the dispute, including the right to intervene. There is also a provision that allows those who have developed industry guidelines relied on as a defense to file an amicus curiae brief in district court.18 In the interests of equity, it would be appropriate to also allow any other party to file an amicus in the district court. Otherwise, the friend of the court provision will be viewed simply as a friend of the defendant provision.

There is a very serious problem in section 5 which is the preemption provision. Section 5(f). That provision states:

> Except as otherwise provided in this Act, this Act supersedes state law to the extent that it establishes a rule of law applicable to an online privacy section that is inconsistent with State law. Nothing in this Act supersedes State law with respect to prosecution of fraud.

[18] Sec. 4. (b)(3).

There is no basis to adopt this provision and it should be removed. As a general matter preemption is inconsistent with the structure of privacy law in the United States, and similar proposals have often killed important efforts to enact privacy legislation. But it is a particularly bad idea in this context where the FTC would have so much control over the establishment of regulation as well as the provision of safe harbor status. Inadequate regulations or inattention to industry practices by the FTC could not be remedied by state or local authorities. States must retain the right to develop new safeguards to protect the interests of their citizens.

Section 6 (review) should be amended to include an annual reporting requirement with specific, numeric information concerning the implementation of the Act as well as the work of the FTC. These formal reporting requirements would specifically require the FTC to report to the Congress on:

- The name and location of all companies that are deemed in compliance by the FTC
- The number of privacy complaints received by the FTC and the disposition
- The number of formal actions taken by the FTC under the Act and the disposition
- Any other matters concerning the effective protection of online privacy

Section 7 (effective date) allows an extraordinary delay from the time of passage of the Act. The Act requires at least an 18 month delay and the Commission could effectively put off implementation for two and a half years from the data of enactment. It seems unnecessary to allow for such a long delay particularly considering the rapid change in industry practices. It would not be unreasonable to expect that the Act would take effect 180 days after passage, but in no case should it be longer than one year.

Finally, I should point out that S. 809 as currently drafted transfers tremendous control to the FTC to set policies, issue guidelines, approve industry standards, intervene in state enforcement actions, and preempt state law, with little in the way of oversight or accountability. I would urge further revisions to S. 809 that would ensure greater accountability through annual reporting requirements, preserve state authority to develop privacy laws and pursue privacy investigations, and enable more opportunities for the public to comment on FTC decisionmaking and to participate in actions brought by the Commission. I am particularly concerned that the problems with the recent FTC report to Congress will be repeated in the future.

In summary, I would recommend the following changes:

- Narrow exceptions for access
- Narrow exceptions for purpose limitation
- Remove preemption provision
- Add annual reporting requirements
- Add a provision for independent civil action
- Permit public comment on Safe Harbor determinations
- Permit public filings as amicus curiae
- Reduce delay for effective date

Further Recommendations

Establish a privacy agency

Around the world government agencies routinely report on the handling of privacy complaints, the emergence of new privacy issues, and proposed measures to protect privacy. These reports help the public and the government understand the status of privacy protection in their country and develop new approaches to replace old ones. Privacy agencies are not just operating in Europe; they can be found from Hong Kong to the Canadian province of British Columbia.

But there is still no privacy agency in the United States. In many respects, this is surprising. The United States itself helped launch this effort with the publication of the HEW Report in 1973, the report of the Privacy Protection Study Commission in 1977, and various reports produced in subsequent years by the Office of Technology Assessment, the National Research Council, and the Institute of Medicine.

While the FTC is doing important work on privacy issues, it is still missing the focus and understanding of a privacy agency. The FTC report to Congress simply lacked the information necessary for the public or the Congress to make informed decisions in this area. It may be the case that Congress would decide that privacy legislation is not needed for the Internet, but the FTC had a responsibility to at least make the case for legislation, or failing that, to lay out the pros and cons of privacy legislation.

Some people will say that the last thing we need is a new federal agency making privacy policy. But the reality is that the federal government will make privacy policy whether or not there is a privacy agency. So the question simply becomes, how do you

make good privacy policy, how do you develop policies that respond to peoples' concerns as opposed to simply reflecting what industry is willing to do.

Promote Privacy Enhancing Techniques

Efforts to promote genuine privacy enhancing technologies should also be pursued. Successful development and use of these techniques will reduce the need for legislation and ultimately serve the long-term interests of consumers and businesses. But it is critical to understand that real Privacy Enhancing Techniques help minimize or eliminate the collection of personally identifiable information and ensure the enforcement of Fair Information Practices. Techniques that simply facilitate the collection of personal data through notice and consent are hardly privacy enhancing, and are probably better viewed as Privacy Extracting Techniques.

At this point, the FTC seems unable to tell the difference. But this distinction is crucial to the future of online privacy. I suspect that one of the additional benefits of legislation such as the Online Privacy Protection Act will be to promote the development of real Privacy Enhancing Techniques.

Conclusion

The key to protecting privacy on the Internet and off is to ensure the effective enforcement of Fair Information Practices and where possible to reduce or eliminate the collection of personally identifiable information. Virtually every privacy law in the United States takes this approach. To the extent that the Online Privacy Protection Act helps ensure the enforcement of Fair Information Practices, it will contribute significantly to online privacy for Internet users.

I appreciate the opportunity to testify today on this important legislation. I would be pleased to answer your questions.

Additional References

Articles, Reports and Web Sites

Mark E. Budnitz, "Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-regulation is Inadequate," 49 S.C. L. Rev. 847 (1998)

"Beyond Concern: Understanding Net users Attitudes About Online Privacy" [www.research.att.com/projects/privacystudy/

EPIC letter to FTC, Dec. 14, 1995 [http://www.epic.org/privacy/internet/ftc/ftc_letter.html]

EPIC, "Surfer Beware I: Personal Privacy and the Internet" (1997) [http://www.epic.org/reports/surfer-beware.html]

EPIC, "Surfer Beware II: Notice is Not Enough" (1998) [http://www.epic.org/reports/surfer-beware2.html]

FTC, "Online Privacy: A Report to Congress" (1999) [http://www.ftc.gov/reports/privacy3/index.htm].

Doubleclick page [http://www.privacy.org/doubletrouble/]

Junkbusters [http://www.junkbusters.com/ht/en/new.html#Ginsu]

Jerry Kang, "Information Privacy in Cyberspace Transactions," 50 Stan. L. Rev. 1193 (1998).

Joel R. Reidenberg, "Restoring Americans' Privacy in Electronic Commerce," 14 Berkeley Tech. L.J. 771 (1999).

Books

Phil Agre and Marc Rotenberg, eds., Technology and Privacy: The New Landscape (MIT Press 1997)

Colin Bennet, Regulating Privacy (Cornell Press 1992)

Fred Cate, Privacy in the Information Age (Brookings 1997)

David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (Chapel Hill 1989).

Priscilla M. Regan, Legislating Privacy: Technology, Social Values and Public Policy (University of North Carolina Press 1995)

Marc Rotenberg, The Privacy Law Sourcebook 1999: United States Law, International Law, and Recent Developments (EPIC 1999).

Paul Schwartz and Joel Reidenberg, Data Privacy Law: A Study of United States Data Protection (Michie 1996)

Peter Swire and Bob Litan, None of Your Business, World Data Flows, Electronic Commerce, and the European Privacy Directive (Brookings 1998)