Testimony and Statement for the Record of

Marc Rotenberg, Executive Director
Electronic Privacy Information Center

Hearing on

S. 2201
Online Personal Privacy Act

Before the

Committee on Commerce, Science, and Transportation
United States Senate

April 25, 2002
Russell Senate Office Building 253
Mr. Chairman, members of the Senate Commerce Committee, thank you for the opportunity to testify today on S. 2201, the Online Personal Privacy Act. My name is Marc Rotenberg. I am the Executive Director of the Electronic Privacy Information Center in Washington, DC. EPIC is a public interest research and advocacy organization that focuses on emerging civil liberties issues. I am also the chairman of Privacy International, a human rights organization based in London.

It is clear that the protection of privacy remains one of the top concerns in the United States today. Even with the dramatic events of the past year, Americans continue to make clear in opinion polls, news articles, and everyday conversation that one of the great challenges in our era of hi-tech convenience is to avoid the loss of personal privacy.

Today we get sports scores online, read news stories, send messages to friends and colleagues, participate in discussions, buy books and CDs, shop for home loans, make travel plans, and purchase gifts for our relatives. All of this is made possible because of a new computer network technology that has linked together the inexpensive desktop computers that we have in our homes. The benefits of the Internet are clear, but so too are the risks.

In many respects, this ongoing support for the right of privacy is not surprising. Privacy protection has a long history in the United States. Many countries have simply not afforded their citizens the right to use telephones without eavesdropping, to hold credit reporting firms accountable for inaccurate disclosures that impact a consumer’s ability to participate in the marketplace, to find a job, to obtain health insurance, or to buy a home.

New privacy laws have frequently been developed in response to the challenges of new technology. Congress enacted privacy laws for the telephone network, computer databases, cable television, videotape rentals, automated health records, electronic mail, and polygraphs. In each case, it was never the intent to prohibit the technology or to prevent the growth of effective business models. Instead, the purpose was to establish public trust and confidence in the use of new technologies that had the ability to gather a great amount of personal information and, if used improperly, to undermine the right of privacy.

With the Internet, a piecemeal approach has been taken. A law was passed to protect the privacy interests of minor children. The FTC exercised its section 5 authority for a limited number of privacy cases. Some US firms endorsed the Safe Harbor Arrangement, providing at least for their European customers, baseline privacy protection. Many companies also attempted to address public concerns about online privacy through the development of privacy policies, the hiring of privacy officials, and support for third-party accreditation services. Some progress has been made. But serious problems remain.

- Companies post privacy policies, enter into relationships with consumers, collect personal information, and then decide to change their policies.
• Companies create assurances of protection, run into financial troubles, seek protection under bankruptcy law, and then sell their customers’ data to the highest bidder.

• Companies post privacy policies that require the help of both an English major and a commercial lawyer to understand, and even then the policies are misleading and contradictory.

• Companies acquire information from customers for one purpose and then turn around and sell it for another without the customer’s knowledge and consent.

• And companies avoid the adoption of genuine Privacy Enhancing Technologies that could minimize privacy risk and promote the development of electronic commerce because there is no financial consequence to do otherwise.

In each of these examples, there is no market-based solution. And all of this takes place in an environment where the data-collection practices are far more extensive than in the physical world. In theory consumers could bring suit for breach of contract, but privacy harms are difficult to measure, class action lawsuits have not had much success, and even the FTC has struggled to find a way to apply traditional consumer protection law to the new challenges of online privacy.

The Online Personal Privacy Act seeks to establish trust and confidence in the disclosure of personal information in the online environment. This is central to the growth of electronic commerce and the online marketplace. The Act follows the approach of virtually every modern privacy law in the United States. The Act sets out “Fair Information Practices” for the collection and use of personal information provided by users of the Internet to those who operate commercial web sites or provide Internet services or online services.

As a general matter, the Online Privacy Protection Act contains the basic elements of an effective privacy law. There are provisions for access and for enforcement. There are security obligations and notice requirements. There are opportunities for enforcement. In many respects the Act also tracks the better practices followed by companies today as well as the Safe Harbor Arrangement that US firms have increasingly followed in their online commercial relations with customers in Europe and other countries.

Law Enforcement Exception

As with many privacy laws, the Act creates a presumption against the disclosure of personal information and then sets out limited circumstances when the information may properly be disclosed. For a privacy law to be effective, it is critical that these
exceptions be carefully drafted and as narrow as possible. In my opinion, the exception for disclosure to law enforcement agencies (sec. 103(e)) is too broad. In fact, I could not find another privacy law that would make it so easy for so many public officials to get access to personal information that would be otherwise protected in law.

The problem is the list of entities -- “law enforcement, investigatory, national security, regulatory agency, or Department of United States” -- coupled with the phrase “in response to a request or demand made under authority granted to that agency or department.” That formulation essentially defeats the Fourth Amendment purpose of ensuring that the judiciary plays a role where a lawful search is authorized. I urge you to stay with the standard in other privacy laws that grants authority to a “law enforcement agency” acting on a federal or state warrant, a court order, or a properly executed administrative order. This provides the government with a wide range of opportunity to obtain information in the course of a criminal investigation in a manner that ensures judicial oversight and minimizes the risk of abuse.

**Access Provision**

The access provision (sec. 105) follows a principle widely recognized in US privacy law and that is the ability of person to see the records held by others. Consumers receive access to credit reports, to medical records, and to cable billing information. Under the Privacy Act they are also able to obtain records of information about them held by federal agencies. But the provision in the Online Personal Privacy Act is narrower than it should be. Consumers generally know what information they have provided to companies. What they do not know is what information the company is providing about them to others. The access provisions should allow consumers to be aware of disclosures to third parties.

Also, the bill rightly ensures that copies of this information will be available at a reasonable fee and that the fee is waived in those cases where the consumer may not be able to pay or where there is fraud. A provision should also be included to provide free access in those cases where the provider or operator receives payment or consideration from a third party for the disclosure of the user’s information. This is a principle of fairness and equity that will make companies more respectful of the privacy interests of their customers.

**Enforcement**

Mr. Chairman, the section on enforcement raises several difficult problems. It rightly seeks to provide several ways to ensure actual implementation of the practices set out in Title I, but it is not clear whether these provisions individually, or taken together, provide an adequate means of protection.

It is likely that the primary means of enforcement will be through the Federal Trade Commission since any violation of the Act will be considered a violation of Section 5 of the FTC Act. However, the FTC Act does not provide any actual relief to
affected parties. The FTC will have the authority to enter into a consent decree to prevent the company from engaging in similar acts in the future.

The State Attorneys General retain significant authority to pursue actors that violate Title I but the FTC retains the ability to prevent these matters from going forward. Considering that the bill also preempts the authority of states to enact stronger measures to safeguard the interests of their citizens, this provision represents a significant transfer of authority from the states to Washington, DC.

Structurally, the Act places a great deal of faith on the ability of the FTC to pursue privacy violations. I believe that this can be made to work but it will require extensive public oversight. The critical role of the FTC becomes even clearer when you consider the private right of action created by section 203. Some of the industry lobbyists have claimed that this bill will open a floodgate of litigation. But a fair reading of the Act reveals that it will be remarkable if there is more than a trickle of cases.

Section 203 is drafted in such a way as to pile high all the hurdles of litigation without any of the benefits. Litigants will be required to establish “actual harm” which is difficult in privacy cases, and the reason that federal law typically provides for liquidated damages. They will be required to go into federal district court when violations have occurred but there will be no payment for a lawyer or costs incurred and very limited opportunity for damages if they prevail. It is hard to imagine who but the most affluent would be able to pursue such a case.

The private right of action provision in this bill is far narrower than any other privacy law with which I am familiar. Typically, a federal privacy law allows a person to recover actual damages not less than a set amount of at least $2,500, punitive damages, reasonable attorney fees and litigation costs, and such other relief as a court may determine. And even with these incentives, privacy cases are infrequent and damages, when they are awarded, are nominal. It takes an extremely determined plaintiff to pursue these cases.

At the very least, the Committee should either allow individual consumers to go into small claims court to seek relief for violations of the Act, as they are able to do currently under the Telephone Consumer Protection Act, or if they must go into federal court, the Act should provide for reasonable attorneys fees, costs, and such other relief as a court may provide. Even with this change, proving actual harm in a privacy case will remain very difficult.

Application to Congress and Federal Agencies

Mr. Chairman, I am pleased to see that Title III of the Act extends baseline privacy standards to federal agencies and to the United States Congress. This sends a clear message that Internet privacy protection should apply to both the public and private sector. Title III should also be made clear that nothing in this Act will alter the obligations set out in the Privacy Act of 1974, which applies to all federal agencies that
collect personal information on US citizens whether or not they are providers or operators under the definitions of the Act.

But here again I must point out that, unless the law enforcement access provision in Section 103 is narrowed, any federal agency could defeat the purpose of this Online Personal Privacy Act simply by granting itself the authority to routinely engage in actions that would otherwise violate the provisions set out in Title I. It simply does not make sense to pass a privacy law that seeks to impose privacy obligations on a federal agency and then leaves the agency with the authority, if it so chooses, to remove the obligations.

Definition of Sensitive Personally Identifiable Information

The Act makes an important distinction between Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). The first is generally subject to the opt-out approach, while the second would require opt-in. While many privacy experts, including me, have favored the opt-in rule for all transfers of personal information, I believe the approach set out in the bill can be made to work. It reflects a general recognition that there is a distinction between medical and financial information on the one hand and the type of paper towel or lettuce we buy on the other. It also follows an approach that is increasingly found in Europe and other regions of the world to make clear that a stronger privacy standard should apply to more sensitive personal information. The definition of Sensitive Personally Identifiable Information set out in the Act reflect both a commonsense understanding and the practice that is currently evolving.

The one additional subject area that I hope you will consider adding to the category of Sensitive Personally Identifiable Information is for matters of intellectual freedom and political belief. The United States in particular has a long tradition of seeking to safeguard the records of the books that people borrow in libraries, the video tapes they rent, and the cable programs they watch. In a recent case, a state Supreme Court made clear the high level of privacy associated with records of bookstore customers.

With the Internet in particular, there is a significant risk that a very detailed picture of a person’s political beliefs could be easily compiled and distributed with little regard for the right of privacy. I believe that if this were done by government actors it would implicate deeply held First Amendment values and should not be permitted.

Privacy Enhancing Technologies

Efforts to develop tools that will enhance online privacy and could diminish the need for further legislation should certainly be encouraged. The bill proposes P3P as one possible approach. I believe a better research program would focus on genuine Privacy Enhancing Techniques that enable online transactions and commerce, and minimize the risk of privacy loss. Such approaches include techniques for “authentication without identification,” which means simply that consumers could engage in verifiable
transactions with online merchants without disclosing their actual identities much as they do today in the physical world with cash and credit cards. Other research topics might include techniques for enabling online access that do not create additional security risks, developing methods for consumers to more readily track the subsequent disclosure of their personal information, and ensuring by technical measures that individuals will maintain greater control over the personal information they provide to others.

It is clear that a wide range of approaches will be necessary to safeguard online privacy. Technology has a critical role to play. But the privacy technologies must be designed with the central goal of protecting privacy.

Conclusion

In conclusion, Mr. Chairman and members of the Committee, the Online Personal Privacy Act is an important step forward in the advancement of privacy law in the United States. It responds to overwhelming public support for stronger privacy protection on the Internet. It seeks to ensure that the right of privacy will carry forward as new commercial opportunities are developed and new technologies emerge. I hope the Committee will take the steps necessary to strengthen the provisions in the bill so as to ensure that the intent of the sponsors is realized in practice.

Thank you again for the opportunity to appear before the Committee today. I would be pleased to answer your questions.