



ELECTRONIC PRIVACY INFORMATION CENTER

Prepared Testimony and Statement for the Record of

Marc Rotenberg, Executive Director,
Electronic Privacy Information Center
Washington, DC

on

S.809 Online Privacy Protection Act of 1999
S.2606 Consumer Privacy Protection Act of 2000
S.2928 Consumer Internet Privacy Enhancement Act of 2000

before the
Senate Commerce Committee

Washington, DC
Tuesday, October 2, 2000

My name is a Marc Rotenberg.¹ I am the Executive Director of the Electronic Privacy Information Center (EPIC) in Washington DC and an adjunct professor at Georgetown University Law School where I teach information privacy law.² I am grateful for the opportunity to appear before the Committee today. I also appreciate the Committee's ongoing efforts to explore the important issue of Internet privacy.

I will focus my comments on the need to ensure strong privacy safeguards for the Internet based on Fair Information Practices. These guidelines are the basis for almost all privacy laws, and provide the framework to evaluate the proposals currently before the Committee.

I will address specific provisions of the Online Privacy Protection Act, the Consumer Privacy Protection Act, and the Consumer Internet Privacy Protection Act. I will recommend that the Committee adopt strong, sensible provisions that safeguard the interests of consumers and provide clarity and a level playing field for businesses. I will also address some of the issues that are not addressed directly in the legislative proposals, such as the need to protect online anonymity.

STATUS OF INTERNET PRIVACY

Mr. Chairman, at the outset, I wish to make three brief points concerning Internet privacy. First, we believe that there is widespread public support for legislation in this area and also that industry recognizes that such legislation is appropriate and necessary. Polling data routinely shows that the public believes that privacy laws for the Internet are needed.³ And although industry groups have objected as a general matter to government regulation of the Internet, in the area of online privacy I believe most will concede that legislation is likely.⁴

Second, while we recognize that commercial web sites have made progress in developing and posting privacy notices, we do not believe that these policies alone

¹ Executive director, Electronic Privacy Information Center; adjunct professor, Georgetown University Law Center; editor, *The Privacy Law Sourcebook 2000: 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>

³ Business Week/Harris Poll: A Growing Threat, March 20, 2000, [http://www.businessweek.com/2000/00_12/b3673010.htm]. The poll found that 57 percent of people surveyed supported laws governing the collection and use of personal information online while only 15 percent supported letting industry groups develop voluntary standards. Georgia Tech Graphic, Visualization, & Usability Center's Tenth WWW User Survey (October 1998) [http://www.gvu.gatech.edu/user_surveys/survey-1998-10/graphs/privacy/q59.htm] This poll found that 41% agreed strongly and 31% agreed somewhat with the statement: "There should be new laws to protect privacy on the Internet."

⁴ "Mixed Views on Privacy Self-Regulation," DM News, October 2, 2000 [<http://www.dmnews.com/articles/2000-10-02/10780.html>]

protect online privacy. In fact, privacy notices without other substantive rights operate more like warning labels or disclaimers than actual privacy safeguards. Although it would be tempting to pass legislation based simply on the notice requirement, we believe such a bill over the long term would reduce the expectation of privacy and the level of online protection. A substantive privacy measure must provide more than notice.

Third, we believe that enforcement mechanisms must remain flexible. Any legislation that leaves a central agency in the position to limit enforcement at the local level or prevents an individual from pursuing a privacy complaint in court could significantly undermine the protection of privacy interests. And to the extent that the FTC plays a central role in overseeing the enforcement of privacy, it is vitally important that formal reporting requirements be established so that this Committee, the Congress, and the public will be able to evaluate the effectiveness of privacy protection in the United States.

PRIVACY LAWS AND THE ROLE OF FAIR INFORMATION PRACTICES

The basic goal of privacy legislation is to outline the responsibilities of organizations that collect personal information and to provide rights to those individuals that provide the personal information. These rights and responsibilities are commonly referred to as "Fair Information Practices." Fair Information Practices ensure that consumers have control over their personal data and that companies abide by ethical business practices.

Fair Information Practices have provided the basis for privacy legislation across both the public and private sectors. The Fair Credit Reporting Act of 1970 placed requirements on credit reporting agencies, restricting their ability to disclose information about individual consumers and providing a right of access so that individuals could inspect their credit reports and determine whether decisions affecting their ability to obtain a loan or receive credit were based on accurate and complete information.⁵ Since 1970, privacy laws based on Fair Information Practices have covered educational records⁶, cable subscriber records⁷, email⁸, video rental records⁹, and telephone toll records¹⁰. The recently passed Children's Online Privacy Protection Act¹¹ requires parental consent before information is collected from minors and access to any information already collected.

For more than twenty-five years, the United States has established privacy laws based on Fair Information Practices directly in response to the development of new technologies, such as computer databases, cable television, electronic mail, movies on video tape, and fax machines. Far from discouraging innovation, these baseline privacy

⁵ Fair Credit Reporting Act (1970) 15 U.S.C. § 1681.

⁶ Family Educational Rights and Privacy Act (1974) 20 U.S.C. § 1232g.

⁷ Cable Communications Policy Act (1984) 47 U.S.C. § 551.

⁸ Electronic Communications Privacy Act (1986) 18 U.S.C. § 2510.

⁹ Video Privacy Protection Act (1988) 18 U.S.C. § 2710.

¹⁰ See Telecommunications Act (1996) 47 U.S.C. § 222.

¹¹ Children's Online Privacy Protection Act (1999) 15 U.S.C. § 6501.

standards have promoted consumer trust and confidence as new services have emerged. Privacy laws have also provided businesses with clear rules and a level playing field.

Fair Information Practices have also contributed to the development of privacy laws around the world. Important international agreements such as the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the recently concluded Safe Harbor arrangement have been built on Fair Information Practices¹². These international guidelines have become more important as we move toward a global economy where US firms seek to sell products online in other countries and US consumers have increasingly made their personal information available over the Internet to companies operating all around the world.

Because of the central role that Fair Information Practices have played in the development of privacy law in the United States and the increasing importance of these principles for online commerce going forward, I believe they provide the appropriate framework to evaluate the bills now pending before the Committee.

FAIR INFORMATION PRACTICES PRINCIPLES AND CONSUMERS

Strong legal protections built on Fair Information Practices satisfy the basic, common sense privacy expectations of consumers. The bills under consideration today follow the rubric of notice, "choice," access, security, and enforcement when discussing Fair Information Practices. While this is not a complete list of the obligations that can be found in US privacy law, it is a useful framework for evaluating privacy measures. All three bills present various approaches towards upholding Fair Information Practices and establishing baseline standards for Internet privacy.

Notice

The first principle of privacy protection is that a consumer should be provided notice of the collection, use and dissemination of his or her personal information. A privacy notice or a privacy policy should tell a consumer when his or her personal information will be collected, the purpose it will be used for and whether it will be disclosed to a third party. Simply put, a privacy notice should be a basic description of what information a company collects and for what purposes.

The problems with current privacy policies have been brought up by the Committee in earlier hearings. They tend to be long, confusing, and full of obscure legal language. It is ironic that a principle intended to make consumers aware of privacy practices has been subverted to one that misleads and frustrates consumers on a regular basis. There is the additional problem that companies have found it too easy to change privacy policies when they wish. This was the problem with Doubleclick that gave rise to the FTC investigation.

¹² <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>

Furthermore, although notice is an important part of a privacy policy it does not by itself constitute privacy protection. Notice must be accompanied by the other principles of Fair Information Practices. This point was made clear in EPIC's recent report "Surfer Beware 3: Privacy Policies Without Privacy Protection". This study found that while the vast majority of high-traffic e-commerce sites had privacy policies none of those sites displayed a privacy policy that provided the full range of Fair Information Practices¹³.

S. 2928, the "Consumer Internet Privacy Enhancement Act", has the most extensive discussion of notice in comparison to S. 809 and S. 2606. However, it is possible that the amount of information that this bill requires to be disclosed will likely overwhelm the average Internet user. The speed and convenience of shopping online will quickly hit speed bumps if all consumers are expected to read such notices before transacting business. Consumers should be assured that baseline principles to safeguard their privacy apply to every site they visit. They should not be burdened with having to examine and comprehend each line of a privacy policy before they decide whether or not to transact business with that specific company.

The notice provisions of S. 809, the "Online Privacy Protection Act of 1999", and S. 2606, the "Consumer Internet Privacy Enhancement Act", are less burdensome but neither are perfect. While S. 2606 specifies that notice should be "clear and conspicuous", S. 809 prudently requires that contact information is provided. While the legislative construction would be difficult, notice should be able easily understood by most consumers. Of course, contact information should be included as well.

In addition to this basic analysis of notice, S. 2606 properly addresses a growing trend of Internet companies that unilaterally change privacy policies on their customers. The requirement of notice of a policy change and consent before information can be used in accordance with the new policy would ensure that companies could not change terms on their customers. Furthermore, it would force companies to think more carefully the first time they write their privacy policy.

Consent

The principle of consent is based on the view that if a consumer provides information for a particular transaction it should not be used for another purpose without first obtaining the consent of the consumer. The purpose of this requirement is to ensure fairness and transparency and to prevent the type of "bait and switch" that can easily result if a consumer is led to believe that a disclosure of personal data is necessary for a transaction when it will in fact be used for another purpose. If I provide my name and mailing address so a book I ordered online will arrive at my house, the information should not be used for another purpose without my permission.

¹³ <http://www.epic.org/reports/surfer-beware3.html>

Opt-in means asking the consumer's permission before information is collected or used. Opt-out means that a consumer will have to go through a long, burdensome process to tell a company that she doesn't want information used in a particular way. Which one will help a consumer control her information? Which will encourage companies to make it as difficult as possible to let her exercise that control?

We support opt-in as a common-sense standard that will give consumers a fair chance at controlling their personal information. The affirmative consent requirement that would be established by S. 2606 is a "consumer friendly privacy standard" that allows for individuals to rightly decide how their information held by others should be used.

The exceptions in S. 809 for consent present an issue that the Committee should consider. S. 809 excludes "transactional information where identifiable information is not removed" from its consent requirement. While S. 2606 establishes that personally identifying information may only be collected and used with consent, a great deal of information is collected and tied to unique identifiers.

While it does not establish an opt-in, only S. 809 recognizes that "transactional information" or clickstream data should be considered personal information. Within the bill, personal information includes "information that is maintained with, or can be searched or retrieved by means of" other identifiers. Transactional information is data generated by online movements – pages visited, searches conducted, links clicked – and has been at the center of recent privacy controversies over online profiling. Not including this information as part of an online privacy bill and protecting it would overlook a major concern of Internet consumers.

Access

One of the critical requirements of genuine privacy protection is to ensure that consumers are able to see the information about them that is collected. The right of access, which can be found in laws ranging from the Fair Credit Reporting Act to the Privacy Act to medical privacy laws across the country, is oftentimes the most effective way that individuals have to monitor the collection of their data and to object to inappropriate uses of personal information.

Businesses sometimes object to providing access because they claim that it is too costly. But it is also possible that many organizations simply don't want to actually show their customers how their personal information is actually used. This is a risky strategy that we believe online companies should avoid.

In the online world it is much easier to provide access to profile information. Many websites today, from airline reservations to online banking, are making information that they have about their customers more readily available over the Internet. Many of these companies realize the importance of ensuring the information they have is accurate and developing a transparent and accountable business-customer relationship.

But we need a much broader right of access in the online world because some bad actors are taking advantage of technological tools that are beyond the knowledge of most Internet users. The online world enables far-reaching profiling of private behavior in a way that is simply not possible in the physical world. This became clear during the past year over the debate with Doubleclick and it is today a critical issue with Amazon.

Any company that creates a persistent profile on a known user, or that could be linked to a known user, should be required to make known to that user all of the information that is acquired and how it is used in decisions affecting that person's life. The profile should always be only "one-click" away — there is no reason on the Internet that companies should force users to go through elaborate procedures or pay fees to obtain this information about them.

It would also be appropriate in many cases to give individuals the right to compel a company to destroy a file that has been created improperly or used in a way that has caused some harm to the individual. Data could still be preserved in an aggregate form, but individuals should be able to tell a company that they no longer have permission to make use of the personal information that they have obtained.

S. 2606 provides the most robust right of access. Providing "reasonable" access to personally identifying information and the ability to correct or delete information allows the consumer to control what happens to her data.

S. 809 is better than S. 2928 on access, though the numerous exemptions create several problems. Transactional information, especially where identifiable information is not removed, has received some of the greatest recent attention as mentioned above via online profiling. Personal information that is used internally or confidentially is the type of information that should be most subject to access since it is used outside the realm of normal customer interaction. If one of the goals of access is transparency, the information which is most hidden should be brought to light. The other exceptions for discarded data and data that has no impact seem redundant or unnecessary. The presumption of access is that if personal information is held by a company, it should be provided to the consumer. Discarded data is not held by a company and whether data has impact should be a question the consumer should answer.¹⁴

Enforcement

Perhaps the most important element of Fair Information Practices is enforcement. Absent an effective means to ensure compliance, privacy principles will have little impact on business practices.

¹⁴ For further comments on S. 809, see 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, [http://www.epic.org/privacy/internet/EPIC_testimony_799.pdf]

The key to enforcement is the independence of the enforcer. Self-regulation has been an incomplete solution to privacy protection due to this lack of independence. A company overseeing its financial supporters will not be effective or independent. In our view, the Safe Harbors created by both S. 809 and S. 2928 lack sufficient oversight to ensure privacy protection. Privacy advocacy groups like EPIC have documented reasons to be concerned through its “Surfer Beware” reports.¹⁵ If self-regulation had been effective, the FTC would not have reluctantly made its recommendation for legislation earlier this session and we would not be discussing three potential Internet privacy laws today.

All three bills allow State Attorneys General to police unethical companies that harm the consumers in their jurisdiction. However, all three allow the FTC to intervene in proceedings and permit its actions to take precedence over the actions of State Attorneys General. While we recognize the important role of the FTC in the protection of consumers, it still remains unclear whether it is the appropriate agency to safeguard privacy interests. Rather than putting roadblocks in the way of State Attorneys General, we should allow consumers to be protected by local authorities and other independent agencies that are available.

It is also important to ensure that individual consumers are able to pursue privacy complaints. For that reason, a right to private action with a provision of liquidated damages should be provided. This preserves the right of consumers to pursue privacy complaints when necessary. While S. 2928 does establish a fixed level of civil penalties, S. 2606 establishes a private right of action, liquidated damages attorney's fees, and punitive damages.

None of the bills provide for the establishment of a privacy agency. S. 2606 goes furthest in establishing a FTC Office of Online Privacy but like the other bills rely on the existing section 5 authority of the Federal Trade Commission. The reliance of privacy guidelines on the FTC Act prohibiting unfair and deceptive business practices has not provided an adequate basis for the protection of privacy interests and has failed to develop simple dispute resolution procedures that could assist both consumers and companies resolve privacy problems.

Most consumers are not lawyers, computer experts, or privacy advocates. For that reason, many countries have created independent data protection agencies that answer questions and follow up on consumer complaints. In addition to providing invaluable assistance for consumers, a privacy agency can bring the consumer perspective to other government agencies and business groups. These agencies are also generally responsible for public education and international coordination with privacy agencies in other

¹⁵ 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>]; EPIC, "Surfer Beware III: Privacy Policies without Privacy Protection" (1999) [<http://www.epic.org/reports/surfer-beware3.html>].

countries. In order to help consumers resolve complaints and to penalize unethical companies, they should have the power to take action when irresponsible companies breach privacy principles established in law.

ADDITIONAL ISSUES

State Preemption

All three bills propose state preemption, though S. 2606 will allow for common law tort and certain other claims to go forward. Limiting the ability of states to develop additional safeguards to protect the privacy interests of their citizens is a dangerous precedent and has only occurred in a few statutes. By and large federal privacy laws operate as a floor and allow states, "the laboratories of democracy," to develop new and innovate safeguards as required.¹⁶ We believe this approach should be followed with Internet privacy.

Additional Safeguards

In addition to the other substantive provisions to protect privacy on the Internet. S. 2606 also proposes important amendments that would update current privacy laws. The Video Privacy Protection Act would be extended to include all video recordings, recorded music, and book purchases. The Cable Communications Policy Act would be extended to satellite TV subscriptions. These are sensible recommendations that build on current laws.

Anonymity

Finally, although the bills do not directly address the issue of online anonymity, I would like to underscore that this issue remains one of the central challenges of Internet privacy. While anonymity does create some risk, the loss of anonymity in the online world could significantly undermine any legislative effort to safeguard privacy. We have noticed a disturbing trend in the last year with more and more web sites requiring registration and making use of new tracking techniques to profile Internet users. Legislative safeguards will help limit the worst of the abuses, but formal recognition of a right to be anonymous in the online world may be the most robust form of privacy protection in the years ahead.

CONCLUSION

We commend the Committee for the important efforts to address online privacy. We believe that S. 2606 provides the most robust framework to protect privacy on the Internet, that it is consistent with other privacy laws, and that it is in the interests of consumers and business to ensure a high standard for privacy protection in the world of e-commerce. We urge the Committee not to place too much value on privacy notices

¹⁶ See, e.g., Video Privacy Protection Act (1988) 18 U.S.C. § 2710(f), Cable Communications Policy Act (1984) 47 U.S.C. § 551(g).

without other substantive safeguards. Privacy law is based on Fair Information Practices, a collection of rights and responsibilities that help safeguard the interests on consumers in the world of rapidly changing technology.

REFERENCES

Articles, Reports and Web Sites

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 *Stanford Law Review* 1193 (1998).

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]

Joel R. Reidenberg, "Restoring Americans' Privacy in Electronic Commerce," 14 *Berkeley Technology Law Journal* 771 (1999).

Testimony of Marc Rotenberg before the Subcommittee on Communications, Senate Commerce Committee on the Online Privacy Protection Act of 1999, July 27, 1999.

Paul Schwartz, "Privacy and Democracy in Cyberspace," 52 *Vanderbilt Law Review* 1609-1702 (November 1999).

Gregory Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards," 25 *Yale Journal of International Law* 1-88 (Winter 2000)

Books

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

Colin Bennet, *Regulating Privacy* (Cornell Press 1992)

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 2000: United States Law, International Law, and Recent Developments* (EPIC 2000).

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