

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Testimony of

Evan Hendricks, Editor/Publisher
Privacy Times

www.PrivacyTimes.com

www.CreditScoresAndCreditReports.com

Before The House Committee On Energy & Commerce
Subcommittee On Commerce, Trade, and Consumer Protection

June 20, 2006

Mr. Chairman, Ranking Member Schakowsky, thank you for the opportunity to testify before the Subcommittee. My name is Evan Hendricks, Editor & Publisher of Privacy Times, a Washington newsletter since 1981. For the past 28 years, I have studied, reported on and published on a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have served as an expert witness in litigation, and as an expert consultant for government agencies and corporations.

I am the author of the book, "Credit Scores and Credit Reports: How The System Really Works, What You Can Do."

Due to pre-existing travel plans and other commitments, I am not able at this time to provide as detailed a prepared statement as I would prefer. Please allow me to make some fundamental points.

I appreciate the opportunity to appear before the subcommittee and applaud its work on H.R. 4127. While the bill could still be improved, it at least represents an important step forward in consumer privacy protection, and underscores this Committee's desire to move our nation's policy in the right direction. Conversely, H.R. 3997 would have disastrous consequences and should be withdrawn as an

inexcusable effort to weaken consumers' rights at a time that they clearly need to be strengthened.

I also applaud the underlying purpose of this hearing – to fashion a more comprehensive approach to protecting privacy. In my view, a comprehensive approach is long overdue. I am particularly happy to be sharing the panel with my distinguished colleagues from academia and industry. I believe this panel represents a hopeful potential for consensus on this all-important issue.

A Brief History

The first serious effort to establish a national privacy policy came in the early 1970s in the wake of the Watergate scandal. Sen. Sam Ervin, a longtime proponent of privacy, sought to establish a national policy by proposing a comprehensive “Privacy Act,” creating rights of Fair Information Practices (FIPs) for individuals, that would apply to both the governmental and private sector.

Lobbying and politics forced Sen. Ervin to cut a deal. The result was the Privacy Act of 1974, applying only to federal agencies, and the creation of the Privacy Protection Study Commission (PPSC), a blue-ribbon panel that held hearings, studied information-privacy issues relating to most of the private sectors, and made legislative and other recommendations published in its final report.¹ The PPSC agreed that consumers needed legal protection, but recommended a sectoral approach, rather than a comprehensive one. The PPSC supported separate statutes for financial, medical and insurance records. The conclusion favoring a sectoral approach did not seem unreasonable at the time, but in hindsight, it resulted in an importance sense, of privacy being “divided and conquered” by institutional forces at the cost of individual rights. Many of the legislative proposal stemming from the PPSC’s recommendations “died on the vine” in the late 1970s and were forgotten.

The result for the past three decades has been a sort of *ad hoc*, “hit-and-miss” response driven by anecdotes. For example, when Judge Robert Bork was nominated to be a Supreme Court Justice, a local news reporter obtained his video rental records and wrote a story about his movie viewing preferences. Congress

¹ *Personal Privacy In The Information Age: The Report of the Privacy Protection Study Commission*, (July 1977; GPO Stock No. 052-003-00395) Herein referred to as the PPSC Report.

moved quickly to pass the “Video Privacy Protection Act.” The *ad hoc*, sectoral approach is also driven by the Congressional committee jurisdictional issues.

The product of 30 years of *ad hoc* development of our nation’s privacy policy is a growing list of Federal and State laws, some of them effective, and some not. On the federal level we have Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley (GLB), the Cable Television Privacy Act, the Telephone Consumer Protection Act (TCPA), the Children’s Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA).

One downside of the sectoral approach is the plethora of uneven and potentially conflicting standards for the handling of personal data. Another downside is that important types of personal data are left uncovered by law or do not appear to be clearly covered.

Of course, these shortcomings have inspired States to try to fill the gaps and to respond to fast evolving privacy issues in order to protect their citizens.

Fair Information Practices (FIPs)

Prof. Alan F. Westin, of Columbia University, was one of the early, modern-day scholars of privacy. In his 1967 book, Privacy and Freedom, he focused on the emerging issue of “information-privacy” – how the amassing of personal data allowed for new forms of “data surveillance.” In the book, Westin defined privacy in part as “the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.” Harvard Law Professor Charles Fried once referred to privacy as “that aspect of social order by which persons control access to information about themselves.”

Similarly, the U.S. Supreme Court wrote, “To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.”²

The goal of providing individuals with reasonable control over their personal information led to the formulation of Fair Information Practice Principles, an effort

² U.S. Dept. Of Justice v. Reporters Committee, 489 U.S. 749 (1989). This definition of privacy was reaffirmed and expanded upon by the Court in Office of Independent Counsel v. Favish, 541 US 157 (2004)

in which Prof. Westin was integrally involved. In its 1973 report, the [HEW] Secretary's Advisory Committee On Automated Personal Data Systems defined five principles fair information practice:

- (1) there must be no personal data recordkeeping 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 obtained for one purpose from being used or made available for other purposes without his consent;
- (4) there must be a way for an individual to correct or amend a record of identifiable information about him; and
- (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 reasonable precautions to prevent misuse of the data.

One year after the 1973 report, the Watergate scandal raised the nation's privacy consciousness. Prof. Westin's book and the HEW Task Force report became the foundation for enactment of the U.S. Privacy Act of 1974. That Act, in turn in 1975 created the Privacy Protection Study Commission (PPSC), a blue-ribbon panel that held hearings, studied information-privacy issues relating to most of the private sectors, and made legislative and other recommendations published in its final report.³

The report's introduction articulated three objectives⁴ that endorsed Fair Information Act Principles. "These three objectives both subsume and conceptually augment the principles of the Privacy Act of 1974 and the five fair information practices principles set forth in the 1973 report of the [HEW] Secretary's Advisory Committee On Automated Personal Data Systems."

³ *Personal Privacy In The Information Age: The Report of the Privacy Protection Study Commission*, (July 1977; GPO Stock No. 052-003-00395) Herein referred to as the PPSC Report.

⁴ The three general principles were: (1) minimize intrusiveness; (2) open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it (maximize fairness); and (3) create legitimate enforceable expectations of confidentiality

The PPSC report set the foundation for analyzing and evaluating law, policy and organizational practices relating to the collection, use and disclosure of personal data. Its *methodology* was to *identity the principles of Fair Information Practice* and *then apply them* to the issue at hand, whether it be a standard industry practice or the statute governing that industry.

In 1980, the Organization of Economic Cooperation and Development, based in Paris, adopted the following eight principles of fair information practices, still referred to by some experts as the "Gold Standard" of privacy.

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Participation
- Accountability

These principles were endorsed by the Governments of the United States, Japan and most Western European countries. These principles effectively have been recognized by the United Nations in its work on privacy.

These principles are at the core of major U.S. information-privacy laws, like the Fair Credit Reporting Act of 1970, and the U.S. Privacy Act of 1974. They also are at the core of the National Data Protection Laws of European countries, as well as Canada, New Zealand and Australia, and the European Union's Directive On Data Protection.

FIPs: The Goal, and the Measure of Success

The extent to which we will be successful in fashioning the kind of quality law that the American people want and deserve in part will be determined by the extent we are able to incorporate all eight of these principles into the statute. Allow me to briefly explain why.

Openness = Access

The first principle of privacy/FIP is that there should be no record system whose very existence is secret. On an individual basis, Americans must have access to records about them held by major organizations. Americans have this right under the FCRA, Privacy Act and a few other laws. But because they do not have these rights in relation to many other records, there effectively are out of Americans' reach, thereby constituting a form of secret records. I salute the companies at the witness table and others that have endorsed in principle Americans right of access to records about them. It probably is the first step that legislation must tackle. Companies that have not had to implement access requirements worry that it would lead to a tsunami of requests that would overwhelm them. This has never materialized throughout recent history – even throughout 2004 and 2005 when Americans for the first time were entitled to free copies of their credit reports. Some companies also might fret that individual access might expose their proprietary data. But existing statutes are carefully worded to preclude this possibility.

Participation = Correction

A key reason why access is important is so that individuals can discover inaccurate information, dispute it, and have it corrected or removed. This goes to importance of accuracy in Fair Information Practices, ensuring that people are judged on the basis of accurate information.

Purpose Specification/Use Limitation

A fundamental precept of FIPs is that information collected for one purpose should not be collected for other purposes without the consent of the individual. Even under the FCRA and the Privacy Act, there are many allowable data uses without the individual's prior consent. The FCRA permits this by broadly specifying "permissible purposes" – i.e. credit, insurance and "legitimate business purpose." Employment is also a permissible purpose, but deemed so sensitive that it requires prior consent by the job applicant. The Privacy Act allows federal agencies to share data without consent under the "Routine Use" exception. Unfortunately, this has proven too broad a loophole that some Federal agencies are all too willing to take advantage of.

Data Quality

Data quality relates to issues that could make information less useful or unfair. This goes beyond issues of “technical accuracy.” It relates to such issues as completeness and relevance, to borrow two terms from the FCRA. For example, it could be technically accurate that a landlord filed a conviction action in court against the tenant. But that would unfairly portray the tenant if it were proven the landlord’s motion was frivolous and was done to retaliate against the tenant for complaining about unlivable rental conditions – as the latter information would be relevant and give a more complete picture assuring fairness. Maintaining data quality sometimes requires appropriate audits.

Security Safeguards

If information is not adequately protected, then it can be breached and privacy can be compromised. In fact, the Privacy Act requires that agencies:

(10) establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

Moreover, Congress grafted the Privacy Act language into the security safeguards section of the Gramm-Leach-Bliley Act governing financial institutions. The problem is that aside from FTC actions, there is little enforcement of the Privacy Act or GLB security safeguards. That means organizations could calculate it is cheaper not to comply, as the chances of large fines, or other enforcement actions holding organizational heads accountable, were not great. On their face, the Privacy Act and GLB standards seem good. But the recent litany of data breaches underscores that a duty without enforcement is not much of a duty and does not achieve its goals.

Real security requires more than just talking points. It requires leadership, good policies, employee training and awareness, encryption and intrusion detection.

Collection Limitation

This relates to collecting the minimal amount of data needed to accomplish a task. It's also referred to as data minimization, a standard under U.S. wiretap law.

This principle can relate to our discussion in two important ways. First, it relates to limiting the collection and storage of Social Security numbers (SSNs). The SSN is the identity thief's first tool of choice. Many of the publicized security breaches have been potentially traumatic because they involved (unencrypted) SSNs.

Second, it relates to encryption. If personal data, like the above-mentioned SSNs, are robustly encrypted, then even if they are lost and stolen, they are usually unusable. Thus, encryption minimizes the amount of available personal data, enhancing security and privacy.

Accountability = Enforcement

A privacy law without adequate enforcement is a right without a remedy. Unfortunately, many privacy laws suffer from lax enforcement.

It is vital to understand that when you are talking about laws affecting some 200 million people, you need to "democratize" enforcement. You can never build a bureaucracy big enough to enforce such a widely applicable privacy law – nor would you want to.

The best model for enforcement is the FCRA. It's enforcement scheme is

- 1) FTC & Federal Banking Agencies
- 2) State Attorneys General
- 3) Private Right of Action
 - a. Statutory Damages
 - b. Actual Damages
 - c. Punitive Damages
 - d. Attorney's fees

A privacy law cannot fully achieve its goals unless there is an adequate enforcement mechanism and that mechanism cannot be adequate if individuals do not have the ability to enforce their own rights. I'd be happy to provide the subcommittee with numerous examples.

Privacy ‘Infrastructure’

The other necessary aspect of an adequate national policy is Privacy Infrastructure. This relates to having the resources in place to implement and oversee policy. We have slowly begun building this infrastructure. For example, the statute creating the Dept. of Homeland Security created the first statutorily mandated Chief Privacy Officer. The Bush Administration last year directed Federal agencies to appoint a senior officer in charge of privacy policy. Many major corporations began appointing Chief Privacy Officers in the late 1990s.

What is missing in the U.S. is what every other Western nation has: a national office in charge of overseeing privacy policy. In other countries, they are called Office of the Privacy Commissioner or Office of Data Protection Commissioner. In some countries they have regulatory powers; in others, they do not. What is most important is that they are independent offices that typically answer to the legislative branch (the Parliament), not the executive. They typically have jurisdiction over the public and private sectors. These offices typically have limited staff, but pay great dividends in many countries because of their ability to focus attention on everything from questionable practices to emerging technologies. They also serve as a resource for the public, media and legislative and government branches.

Sen. Sam Ervin originally proposed that the United States have such an office, but politics forced him to settle for a study commission. The absence of a national office has greatly retarded the evolution and development of national privacy policy, and resulted in the hodge-podge of laws we have today. In fact, an early job for a U.S. Privacy Commissioner would be to do an accounting of what personal data of Americans actually are protected, and identify gaps and potential conflicts in existing laws.

This subcommittee should include in its legislation the creation of national privacy office. In years past, Sen. Paul Simon proposed creation of such an office. At a minimum, the office should have subpoena power and the ability to conduct audits and handle complaints. I am confident that such an office would pay great dividends for millions of Americans.

Again, thank you for this opportunity. I’d be happy to answer any questions.