Testimony of
Evan Hendricks, Editor/Publisher
Privacy Times
www.privacytimes.com

Before The Senate Committee On The Judiciary
Subcommittee On Terrorism, Technology & Homeland Security
November 4, 2003
Hearing: "Database Security: Finding Out When Your Information Has Been Compromised"

Mr. Chairman, Ranking Member Senator Feinstein, thank you for the opportunity to testify before the Subcommittees. My name is Evan Hendricks, Editor & Publisher of Privacy Times, a Washington newsletter since 1981. For the past 26 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 want to commend the Chairman for holding this hearing, and commend Senator Feinstein for her leadership in introducing S 1350, "Notification of Risk To Personal Data Act." In an April 3 House Banking Subcommittee hearing that focused on three troubling examples of massive database security breaches, I recommended that Congress use the California State Law on notification as the starting point for enacting a national standard for all Americans. S 1350 is an important step toward achieving this worthy goal.

Defining Privacy: "Fair Information Practices"

When it comes to the collection, use and disclosure of personal information, privacy in our modern age is defined by principles known as Fair Information Practices (FIPs). This definition is recognized and accepted by nearly all Western Governments, including the U.S. Government, by academic and legal experts, and by such international bodies as the Organization of Economic Cooperation and Development (OECD), the European Union and the United Nations.

The principles are the foundation for the Fair Credit Reporting Act, the Privacy Act and several other information-privacy laws. As articulated by the OECD in 1980, they cover such issues as access and correction, transparency, data security, specifying and limiting the purposes for which data can be used, data minimization, and enforcement. In the mid-1990s, when the Federal Trade Commission took the lead for establishing the U.S. Government's privacy policy on electronic commerce, it distilled the FIPs into five principles: (1) Notice; (2) Choice/Consent; (3) Access; (4) Security and (5) Enforcement.

A fundamental premise of FIPs is that they create rights for individual and duties for organizations that collect and maintain personal data.

S 1350 is an excellent starting point because it recognizes two important principles. First, that transparency – more "sunshine" on organizational data practices – is imperative if personal privacy is to be protected. Second, that data security is vital to safeguarding privacy and that if security is breached, the individual has a right to know.

The legislation is the latest in a 30-year trend to convince companies to be more proactive about data security. The U.S. Privacy Act of 1974 requires Federal Agencies to "establish appropriate administrative, technical and physical safeguards to insure" security and confidentiality and "protect against anticipated threats . . . which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual."

Under several federal court rulings regarding the FCRA, companies are vicariously liable for employees who pull credit reports for unauthorized purposes.
As the U.S. Court of Appeals for the Sixth Circuit pointed out in its 1998 opinion in Jones v. Federal Fin. Reserve Corp. (144 3d 961), "Protecting consumers from the improper use of credit reports in an underlying policy of the FCRA. An apparent authority theory is in keeping with FCRA's underlying deterrent purpose because employers are in a better position to protect consumers by use of internal safeguards." In Kodrick v. Ferguson (54 F.Supp.2d 788), U.S. District Judge Moran wrote that sloppy security practices "almost invite violations" of credit report privacy.

The Gramm-Leach Bliley Act imposes data security duties on financial institutions. Moreover, a Federal Trade Commission enforcement action made it clear that companies are subject to Section 5 "Unfair and Deceptive Practices" investigations if they claim to observe security as part of their privacy policies but then allow data leakages through sloppy practices. New York Attorney General Eliot Spitzer applied the State's unfair practices law in a recent enforcement action against Victoria's Secret for data leakages at its Web site.

Stronger requirements are needed because the threat to data security will continue to escalate for at least a few reasons.

First, identity theft continues as one of the fastest growing crimes in the United States. In past months, new studies by the FTC, General Accounting Office, Gartner Group, Privacy & American Business and the Identity Theft Resource Center all found that the prevalence of identity theft, and the damage it causes, is far worse than previously believed. Increasingly, identity thieves are targeting organizational record systems in order to harvest the personal data necessary to engage in this form of fraud. In other words, our personal data has value and in the wrong hands, can be converted into near-instant credit. Moreover, the biggest threat to data security traditionally is posed by authorized insiders who decide to use personal information for unauthorized purposes. Fraud rings are known to bribe insiders in order to obtain personal data. This means that a person's privacy can be seriously jeopardized, but never learn about it, or learn well after even more damage has been done.

Second, there is a community of hackers constantly probing and testing data security. We still do not know the percentage of hackers that are hacking for malicious purposes. However, we do know that there is a community of "Carders," that is, hackers who specialize in

obtaining and trafficking in credit card numbers. Hackers recently snared an unknown number of e-mail addresses from the Orbitz Web site, and then sent spam to those e-mail addresses. The FBI is investigating. It's not clear if Orbitz has notified all affected customers.

Third, despite the trend towards stronger legal duties cited above, there is not a strong organizational culture of data security throughout many organizations, even though they maintain or have access to the personal data of millions of Americans. This is due in part to the relative "newness" of the electronic data age, but in my opinion, more attributable to the absence of long-standing and well-known law and policy that would require organizations to take seriously the issues of data security and privacy.

New York AG Spitzer's investigation of Victoria's Secret was a case in point. Despite a succession of highly publicized data leakages causing harm to consumers and embarrassment and costs to companies, the company's Web site allowed anyone to access hundreds of customer names, addresses and orders through simple manipulation of the online customer identification number. The customer, Jason Sudowski, talked to a Victoria's Secret representative, but was told, "Well, there's no credit card numbers being displayed, so what's the big deal?" It was only after Sudowski called the media that the retailer fixed the glitch. And, it was only because of Spitzer's investigation that New York customers were notified and offered a remedy.

Another concern is the trend towards outsourcing data processing chores to overseas firms in lower-wage countries, including The Philippines, India, Pakistan and Jamaica. Equifax, the giant credit reporting agency (CRA), outsources some dispute handling to Jamaica. *Privacy Times* reported in September that the other two CRAs, Experian and Trans Union, were ready to begin outsourcing to The Philippines and India. A story in the Oct. 22 *San Francisco Chronicle* underscored one reason why this will increase security risks: A Pakistani employee of a subcontractor doing medical transcription for the Univ. of San Francisco Hospital, complained that the subcontractor had not paid for her work and threatened to post patient records on the Internet unless she was paid. The article noted that there are no enforceable privacy laws in Pakistan or the other low-wage countries to which personal data chores are being outsourced. It was this kind of scenario – the prospect of a citizen's data being exported to a country with inadequate law – that prompted the European Union to include trans border data flow restrictions in its directive on data protection.

S 1350

Due to the relative suddenness of this hearing, I have not had the opportunity to fully analyze and contemplate all aspects of S 1350. As I said, it is an excellent starting point. Here are some initial ways that the proposal could be improved:

Provide A Right Of Access. In order to be able to assess potential threats to their privacy, individuals need to know what information is being kept about them. The problem today is that in too many instances, Americans do not know what data are being kept on them – and don't even have a right to find out. A right of access will promote better security because organizations will need to authenticate individuals seeking access to their records. Individuals will be able to discover what information is being kept on them and, in

some cases, opt out from systems, thereby removing their personal data and the threat altogether. Another benefit of access is the ability to correct inaccurate data, thereby promoting data integrity throughout the system. As Americans, we enjoy a right of access to our credit reports under FCRA, our federal records under the Privacy Act and Freedom of Information Act, our State records under State FOIA/PA laws, our medical records under HIPAA, our Cable TV records under the 1984 Cable TV law, and to a lesser extent, insurance and employment records under various State laws. We need to extend access rights by law to personal data held by all major organizations. Further, in the electronic environment the cost and burden of providing access is decreasing.

Because notification of consumers should only be required when a breach or leakage has the potential for harm, there will be cases in which a more routine breach will not result in notification. In such cases, it is imperative that individuals have the right to learn 1) if the organization maintains data on them; and 2) what procedures the organization has to protect data and provide notice in significant cases. Again, this fits squarely into the category of "Sunshine being the best disinfectant."

Adopt The Privacy Act's Security Standard. As mentioned above, Section (e)(10) of the Privacy Act requires Federal agencies to "establish appropriate administrative, technical and physical safeguards to insure" security and confidentiality and "protect against anticipated threats . . . which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual." Federal agencies have lived under this standard without much problem. In fact, a similar standard is likely to evolve for financial institutions due to regulations proposed by banking agencies under GLB. This standard should be extended to all major organizations that handle sensitive personal data.

Create A Private Right of Action. S 1350 logically delegates enforcement to the FTC and State AGs, the entities that have been most active in enforcing privacy and consumer protection laws. However, the bill also needs a private right of action so that individuals can go to court to enforce their own rights. Remember we are talking about mammoth databases maintaining records on anywhere between a few million to 210 million Americans. Given this scope, you will never be able – nor would you want—to build a bureaucracy large enough to carry out adequate enforcement. The private right of action needs to include minimum statutory damages, attorney's fees and injunctive relief. This right would only apply to serious cases where the company's conduct was determined to be "gross negligence" or a "reckless disregard for the rights of consumers."

Curtail The Use of SSNs as a personal identifier. The SSN is the first tool of choice of identity thieves. Restricting the circulation of SSNs by restricting their use outside of government, employment and banking, will reduce risks. Sen. Feinstein, Sen. Bunning, Rep. Clay Shaw, and others have introduced legislative proposals to this effect.

Create An Independent Privacy Office. Most people don't realize that Sen. Sam Ervin originally proposed such an office along with the Privacy Act. Now, every advanced nation has one except the United States.

Thank you for this opportunity to testify. I would be happy to answer any questions.