

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Testimony of

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

Before The House Committee On Financial Services
Subcommittee On Oversight & Investigations

July 21, 2005

Madame Chairwoman, 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 25 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 this time to provide as detailed a prepared statement as normal. Please allow me to make some fundamental points.

The breach of the credit card data of 40 million consumers underscores several important weaknesses in our national privacy policy.

- 1) Our traditional approach to privacy problems, reacting to anecdotal problems with narrowly tailored legislation has left major gaps in what information is protected, and to what extent it is protected. Credit card processors argue that they are not

covered by the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, or other laws to protect financial privacy.

- 2) If institutions have discretion not to notify consumers of a breach, some institutions won't notify consumers.
- 3) Individuals seeking to learn if they're information was compromised cannot always get straight answers from customer services representatives.
- 4) Breaches impose real costs and damages on consumers, including loss of time, energy and opportunity, and stress
- 5) Individuals are often left without direct recourse or a remedy, despite the damaging nature of some breaches.
- 6) For many organizations handling sensitive consumer data, security remains an afterthought.

Loss of Consumer Confidence

Given the nature of recent breaches potentially affecting 50 million Americans, it should be no surprise that consumer confidence in the security of credit card data and other sensitive information is falling. This could have enormous, negative implications for the economy. The conventional response is to fret more about the effect that increased privacy protections will have on the prerogatives of large organizations. This case should show that we've reached a tipping point, where the risk to consumers individually, and the economy as a whole, is too great to put off an aggressive legislative platform for protecting consumer data. Just reflect upon the fall in small investor confidence following the burst of the "dot-com bubble," and more troubling, the accounting scandals of Enron and WorldCom. The current breaches indicate that our financial data systems are heading for a fall in consumer confidence.

FACTA Was Progress, More Is Needed

Thanks in large part to the work of this Committee, the FACT Act represented important progress in expanding more comprehensive protections for consumer privacy. Unfortunately, the recent breaches underscore that more needs to be done.

Starter List For More Progress

Leading lawmakers are working hard on more comprehensive solutions. Many of the efforts are bipartisan. Reps. Frank, Hooley, Barton and others are all working on the issue. Sens. Specter and Leahy are working together at Senate Judiciary Committee. At the Commerce Committee Sens. Gordon Smith and Bill Nelson are working with Sens. Daniel Inouye, John McCain, Mark Pryor and Stevens. One of the more comprehensive measures is the one introduced earlier this year by Sens. Nelson and Schumer.

The challenge is to be able to advance federal legislation that does not preempt State law. Because of recent progress in the states in the areas of breach-notification laws and credit report “freeze” laws, it would be very counterproductive to preempt State laws in these areas.

Here are some of the areas that need to be addressed to restore consumer confidence in the security of their data:

- 1) Extend to all data brokers and information aggregators the rights of Fair Information Practices (FIPs), including (1) access to and (2) correction of records, (3) purpose specification, (4) collection limitation;
- 2) Create a private right of action so people have a remedy when they are unreasonably damaged by breaches
- 3) Restrict the uses of Social Security numbers
- 4) Create a national standard for breach notification, but only if it improves upon the California law
 - a) Require companies responsible for breaches to offer victims free credit monitoring services
 - b) Create a federal seal for the outside of the envelope to notify people that there is a notice of a data-security breach inside
- 5) Extend security safeguards to non-financial institutions
- 6) Create a national standard for freezing credit reports, but only if it doesn't preempt State law
- 7) Require more matching of identifiers before a credit report can be disclosed (see California statute)
- 8) Create a U.S. Privacy Commission to oversee privacy policy, investigate complaints, and advise Congress

I'd be happy to answer any questions. I've attached a related article that I published in the March 6, 2005 *Washington Post*.

When Your Identity Is Their Commodity

By Evan Hendricks

Sunday, March 6, 2005; Page B01

So you think it's your personal information? That's not the viewpoint of the mega-companies compiling and selling data about you. As they see it, if they collect the information, they own it. Sure, it's about you, but it's theirs. You might think "privacy," but they see a commodity -- and a valuable one at that.

And for now, they're right. Never mind that there's a fundamental conflict built into this arrangement. The same companies entrusted with safekeeping our essential information make money only if they sell that information, and they do so in bulk. What's more, the current system places the burden on you to put a stop to any practices you don't like -- provided you discover them. You have to obtain your credit file, dispute errors, "opt-out," call, write -- and hope for the best.

Those are a few of the lessons emerging from a pair of privacy debacles last month that left millions of Americans asking how they can protect themselves and their data in an age when identity theft is the crime of choice. The first of these fiascos involved a company called ChoicePoint Inc., which admitted that it had been tricked into providing information on 145,000 people to a group of bogus companies, and the second stemmed from Bank of America's loss of credit data on 1.2 million federal employees. The incidents suggest that our sensitive personal information has been treated as just another commodity, deserving no more respect (and maybe less protection) than soybeans or pork bellies.

The scandals have re-stoked congressional interest. The day after Sens. Arlen Specter (R-Pa.) and Patrick Leahy (D-Vt.) announced Judiciary Committee hearings on the ChoicePoint scam, Leahy learned that his credit card data was on the Bank of America backup tape that disappeared without a trace. Like the growing number of Americans victimized by such "leakages," he didn't sound too happy.

Perhaps these events will prove to be the tipping point for policymakers and will educate consumers as to their stake and role in what has been aptly termed the "Data Revolution."

Did we say we wanted this revolution?

In fact, we did -- or at least we didn't complain about its benefits. Without the data revolution, there would be no information age. Personal information is vital to this new epoch. The collection and sharing of that information has powered the economy by increasing the availability of consumer credit, while at the same time lowering the cost of granting it. It also facilitates screening of employees, tenants, nannies and others who are entrusted with access to

offices and homes. It makes it more convenient for our highly mobile population to buy houses, rent apartments and get instant store credit.

But there's a dark side: The current system invites identity theft, a fast-growing and distressing crime.

Ultimately, privacy has a very good chance of prevailing over the forces chipping away at it. Not only do Americans overwhelmingly view privacy as a fundamental right that must be preserved, but the economics of the electronic age also dictate the need for innovations that will protect that personal information while continuing to enable the information age.

Brace yourself, however: it's going to get worse before it gets better.

As the Supreme Court has recognized, the key to protecting privacy in the modern world is ensuring that individuals maintain reasonable control over their personal data. Reaching that goal requires a mix of strong national policy, good use of technology and consumer awareness.

ChoicePoint's recent lapse shows how far we have to go. A still at-large fraud ring became "customers" of ChoicePoint by posing as 50 fake businesses, including debt collectors and check-cashing firms. The thieves used ChoicePoint as a portal for accessing at least one major credit bureau, enabling them to filch Social Security numbers, other identifiers such as addresses, and sensitive credit report data. Although the full extent of the damage is not yet known, it's clearly one of the worst cases ever: ChoicePoint sent letters to 145,000 consumers warning that their data were compromised; 750 individuals were confirmed victims of identity theft.

The perpetrators picked quite a target. ChoicePoint is a symbol of the "commodification" of our personal data, having compiled 19 billion records covering virtually every American adult. A spinoff of Equifax, the giant credit bureau, ChoicePoint taps a wide range of taxpayer-subsidized sources, including local property records; driver records; boating, pilot and professional licenses; and court records showing bankruptcies, liens, judgments and divorce. Its sales to corporations and governments last year topped \$900 million. (Other database companies are Acxiom, LexisNexis, Westlaw and Seisint.) While some of ChoicePoint's mammoth databases are filled with public records, these records are no longer "public" once ChoicePoint houses them. The company will give you access to some of the files it keeps on you, as required by the Fair Credit Reporting Act (FCRA). But it recently argued to the Electronic Privacy Information Center (EPIC), a public interest research center here in Washington, that other data are not subject to the FCRA.

That means you cannot see your data or correct errors -- even though other companies and government agencies could buy the same data and use them for making decisions about you.

With the Byzantine nature of the laws governing personal information and of the electronic systems that house such information, you need a scorecard to know when your information is protected by federal statute: credit reports (yes), video rental records (yes), federal agency records (yes), medical records (generally no), bank and credit card records (kind of), non-credit database company records (who knows?).

Our system evolved this way because Congress has declined to take a comprehensive approach that would establish a baseline of protection for all personal information. Instead, it has focused on some sectors, or responded to problems as they have arisen.

Congressional action became imperative after the Supreme Court ruled in 1976 that the Constitution did not protect personal data held by banks and other private firms. In essence, the court held that by becoming a bank customer, you surrender your information to the flow of commerce, and thereby surrender your privacy. The information might be about you, but if financial institutions collect and keep it, they own it.

So yes, your information is a commodity; and no, you don't get a cut.

The credit report is at the epicenter of identity theft. First it enables the crime and later it becomes the main source of damage to the victim.

There are three major credit reporting agencies (CRAs) -- Equifax, TransUnion and Experian (formerly TRW). Each maintains electronic credit reports on 200 million American adults. The industry proudly proclaims the system as the best in the world, and claims it has boosted the economy by reducing the cost of credit while increasing convenience for businesses and highly mobile consumers.

Throughout the 1990s, however, complaints about glaring inaccuracies and the CRAs' inability, or unwillingness, to correct them prompted Congress to act. In 1996, it strengthened the first privacy law, the Fair Credit Reporting Act of 1970. Burgeoning identity theft led to more FCRA amendments in 2003.

We know why Willie Sutton robbed banks. Identity thieves also know where the money is. Once they steal identities, thieves can get credit in the victim's name and go on a shopping spree.

When a thief applies for credit using your name and Social Security number (SSN), the CRAs disclose your credit report. Typically, their algorithms will tolerate conspicuous discrepancies in name and address, even in city and state, as long as the fraudster puts your exact SSN on the credit application. It turns out to be a relatively low-risk, high-reward crime.

A Federal Trade Commission survey estimated that nearly 10 million Americans were victims of some form of identity theft in 2003, triple the number in 2001. Yet, in a little-noticed report that year, the TowerGroup, a Massachusetts-based consulting firm, said the incidence of identity theft was such a small fraction of transactions that most financial service companies could not justify the extra expense of preventing it.

That's not much comfort to the victims who describe such crimes as a form of "data rape" that leaves them deeply scarred. It takes a maddening amount of time and effort to persuade credit bureaus to remove fraudulent accounts from credit reports, or to convince creditors to stop reporting them. In the meantime, unpaid debts and collections can ruin a victim's credit score, often leading to denials of mortgages or other credit. The aggravation and frustration tend to

compound. The burden is on the victim to write certified letters, keep records and follow up until the problem is solved.

How can you protect yourself? It's ironic, but the best method of protection is regularly checking your own credit report for early signs of identity theft. The report shows which companies have pulled it and why. So if you live in Virginia and a car dealer in Texas pulled your report -- that's a red flag. Another sign is an unpaid debt that isn't yours. Starting Sept. 1, East Coast residents can get all three of their credit reports once a year for free -- thanks to Congress's 2003 overhaul of the FCRA. Marylanders already are entitled under state law.

To its credit, ChoicePoint is offering free credit reports and a free report-monitoring service to the 145,000 recipients of its warning letter. Monitoring services offer a glimmer of hope, as they give you regular access to your credit report and alert you to new entries. Such alerts could enable you to nip identity theft in the bud. The main problem is that each credit bureau charges about \$100 a year for the service. It's a bit like a protection racket. They will charge you so you can make sure that they did not improperly divulge data to help an identity thief. That's good work if you can get it.

Since the FCRA already requires "maximum possible accuracy," and directs bureaus to curb identity theft, why aren't such services "standard features," rather than "extras"? Price aside, these services prove a vital point: Database technology has finally allowed us to plug into our own personal information, a privilege thus far reserved for the CRAs and ChoicePoints of the world -- and the thousands of companies they sell to. This will enable individuals to ensure the accuracy and proper use of their data, and to promptly rap the knuckles of those who cross the line.

The information age, understandably viewed as detrimental to privacy, can be turned to privacy's advantage. In the future, all individuals will routinely monitor their personal data, and not just their credit reports. The companies that now seem to be the crux of the problem have incentives to make us all part of the solution. Government agencies and major corporations can save billions of dollars by converting personal data transactions from paper to electronics, but public resistance will continue until there's a strong privacy regime in place. The ChoicePoints of the world could even profit by helping, but they'll have to view us as more than just "data subjects." It's ironic that large firms, which have been careless about privacy, might discover they have financial incentives to become genuine privacy advocates, and figure out ways to live up to the task. Of course, that realization is probably a ways off. Meanwhile, go check your credit report.

Author's e-mail: evan@privacytimes.com

Evan Hendricks is editor and publisher of Privacy Times and author of "Credit Scores & Credit Reports: How the System Really Works, What You Can Do" (Privacy Times).