PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Testimony of

Evan Hendricks, Editor/Publisher
Privacy Times
www.privacytimes.com
Author
"Credit Scores & Credit Reports:
How The System Really Works, What You Can Do"
www.CreditScoresandCreditReports.com

Before The Senate Banking Committee
March 15, 2005

Mr. Chairman, Ranking Senator Sarbanes, distinguished Members, thank you for the opportunity to testify before the Committee. My name is Evan Hendricks, Editor & Publisher of *Privacy Times*, a Washington newsletter since 1981. For the past 27 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 a book about credit scoring and credit reporting, as well as books about general privacy matters and the Freedom of Information Act. I have served as an expert witness in Fair Credit Reporting Act and identity theft litigation, and as an expert consultant for government agencies and corporations.

I was closely involved in the multi-year process that resulted in the 1996 Amendments and 2003 Amendments to the Fair Credit Reporting Act. Working with your highly competent staffs, I was proud of our many accomplishments in 2003.

The recent ChoicePoint and Bank of America incidents underscore that we have much more work to do in order to ensure Americans' rights to information-privacy.

I think that there is broad agreement that an important lesson to be drawn from our FCRA work is that the best way to improve our national credit reporting system is to strengthen protections for consumers. The more power that consumers have to maintain reasonable control over their credit reports, the better the chances for improving their accuracy and ensuring they

will be used fairly and only for permissible purposes. What's true for credit reporting is true for the other non-credit systems filled with personal information.

What's starkly clear from the ChoicePoint episode is the lack of transparency regarding the personal data collected, stored and sold by ChoicePoint and its "cousins," which include Acxiom, LexisNexis/Seisent, and Westlaw– to name a few. Most people do not know about these companies, even though they maintain personal data on over 100 million people.

Moreover, these companies often do not allow individuals to access their data or correct errors -- even though other companies and government agencies could buy the same information data and use it for making decisions about those individuals.

In essence, these are "secret files." In being the first federal body to articulate Fair Information Principles, the first principle set forth by the 1973 HEW Secretary's Advisory Committee On Automated Personal Data Systems was: "There must be no personal data recordkeeping systems whose very existence is secret." This is because history has shown us that secret files are a recipe for inaccuracy, abuse of privacy and poor security.

In my opinion, the non-credit database companies generally operate in violation of principles 2-5 as well, at least in regard to information not already covered by the FCRA. Those principles are: (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.

Possible Solutions

There are no quick or easy solutions to protecting privacy. Like many privacy and consumer experts and advocates, I heartily endorse the concepts underlying legislation introduced by Sen. Bill Nelson and Rep. Edward Markey to extent the protections of the FCRA to non-credit database companies. Similarly, I conceptually favor Sen. Dianne Feinstein's efforts to make notification of security breaches the law of the land. Were it not for the pioneering Californian State law, we might not even know about the ChoicePoint debacle. On the other hand, it would probably be counter-productive for Congress to pass a law that was not at least as strong as the California law. I also agree with the general thrust of measures to curb trafficking in Social Security numbers by Rep. Clay Shaw and others. Details are always important, but since this is not a strictly legislative hearing, we do not need to get into them now.

I also want to bring to the committee's attention the fine work of some of my colleagues, including Consumer Union's endorsement of the efforts of Sen. Nelson/Rep. Markey;[1] the newly drafted "Model Regime For Privacy Protection," by George Washington Univ. Law Prof. Daniel

[1] http://www.consumersunion.org/pub/core_financial_services/002028.html; asking for strong federal standards for security, customer screening, and consumer access and correction

J. Solove & Chris Jay Hoofnagle, head of the San Francisco office of the Electronic Privacy Information Center (EPIC);[2] U.S. PIRG's emphasis that any legislation 1) should be based on FIPs, (2) should have a private right of action, (3) should not preempt states.[3] In addition, Linda Foley of The Identity Theft Resource Center pointed out that when there are security breaches, consumers should not only be notified, but should also be advised as to what information fields were stolen or acquired illegally. And, the Center for Democracy and Technology reminds us not to forget about the oft-overlooked problem of government access to private sector data.[4]

Because there is so much that we do not know about the ChoicePoint and Bank of America incidents, it is premature at this point to identify all of the appropriate responses. That is why my recommendations include a call for a thorough investigation of each incident and a public airing of the results. At the end of the day, I favor Congress taking as comprehensive approach as is politically possible.

Current Gaps In Law, Policy & Information Systems

The recent incidents underscore gaps in current law, policy and information systems. In its recent exchange with EPIC, ChoicePoint acknowledged that its insurance, employment background and tenant screening "products" were covered by the FCRA. But it argued that the rest of the data, including those sold to law enforcement, were not covered by FCRA. This is particularly troubling given that, as noted in Robert O'Harrow's book, "No Place To Hide" (Free Press 2005), ChoicePoint effectively bills itself as a private intelligence service.

I probably disagree with ChoicePoint's view that so many of its information products fall outside of the FCRA. The Act's definition is intentionally very broad, and includes "character, general reputation, personal characteristics, or mode of living …" However, the fact that ChoicePoint takes this position means that consumers cannot be assured that they can see and ensure the accuracy of data about them.

Even where ChoicePoint agrees that its products are covered by the FCRA, there are troubling loopholes.

For examples, ChoicePoint says it has three "products" that are free under the FACT Act: the C.L.U.E. (auto and homeowners insurance); "WorkPlace Solutions" (employment background screening) and "Tenant History" (apartment rentals).

ChoicePoint said there would be no C.L.U.E report on you if you have not filed an auto or home insurance during the last five years.

However, it also said it would not have an employment history or tenant history report "if you have not applied for employment with a customer that we serve," or "have not submitted a residential lease application with a customer that we serve."[5]

---

[2] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902
[3] www.pirg.org/consumer/pdfs/pirgendorsesnelsonmarkey.pdf
[4] www.cdt.org
[5] www.choicepoint.com/factact.html, visited March 13, 2005

How could it not have a "report" on you, but then sell one to an employer or landlord when they asked for it? Under ChoicePoint's interpretation, you apparently could not check the accuracy of a report *before* it was sold to a landlord or employer. But the FCRA requires that *every* CRA shall, upon request, disclose to the consumer "*all information in the consumer's file*." And, even if no insurance claims were filed, ChoicePoint regularly buys data from State Departments of Motor Vehicles, which presumably means it maintain records on most American drivers in one or more of its databases.

Absent Congressional action, this fundamental question of access might have to be decided by the courts. But that could take years, which is one more reason that Congress should require by law that database companies comply with Fair Information Principles, and give individuals the ability to enforce their rights.

The Gramm-Leach-Bliley Act includes safeguards for the security of credit data, including credit header data (identifying information from credit reports). But if ChoicePoint files are based on identifying information from public records or other non-credit files, then ChoicePoint presumably would argue that it is not subject to GLB's security safeguards.

Under this reasoning, the coverage may be even scantier for other database companies, including Acxiom, LexisNexis/Seisint, and Westlaw.

One of the many ironies is the secrecy shrouding these and other database companies that traffic in consumer data. Accordingly, to adequately protect privacy we need to have greater disclosure about all aspects of their operations and practices. This should not be surprising. After all, the same Supreme Court Justice, Louis Brandeis, called privacy, "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." Brandeis also said "the Sunshine is the best disinfectant."

Privacy Protection Requires 'Sunshine'

The truth is that we do not know:

- Precisely what information these companies collect
- Where they collect it from
- The manner in which they organize and/or maintain it
- The mechanisms they have to ensure security, or to facilitate both consumer access to their data and correction of errors (if any)
- Whether they audit their systems to ensure accuracy or take other steps to do so
- The mechanisms (if any) for notifying consumers if data are leaked

In the ChoicePoint matter, we do not know precisely how the fraud ring exploited weaknesses in the company's systems. It appears that the thieves used ChoicePoint as a "portal" for accessing credit report data. Equifax told the *Atlanta Business Journal* that as many as 8,000 of its credit reports may have been obtained fraudulently through ChoicePoint.

- Is the 8,000 number accurate?
- Why then did ChoicePoint send notices to 145,000 people? How did ChoicePoint calculate that number and why the discrepancy with the Equifax number?
- Did the fraud ring engage in some sort of two-step process, using ChoicePoint to first try and identify a universe of good candidates for identity theft, and then zero in on the best candidates and pull their full credit reports?
- How long had this been going on?
- Why didn't ChoicePoint or Equifax notice what might have been an unusual pattern?

Needed: A Complete Accounting of The ChoicePoint Case & The Overall Landscape

The unanswered questions cited above underscore the need for a full accounting, not only of the specifics of the ChoicePoint case, but of the overall landscape. Because of the need to maintain the integrity of the ongoing investigations, the various law enforcement authorities are not likely to fully inform the public of what they learn. Therefore, it is imperative that Congress ensure that we have a full accounting of the affair.

More broadly, the time has come for a full accounting of the large database companies and the personal information they collect, maintain and disclose.

ChoicePoint, Acxiom, LexisNexis/Seisint, Westlaw and the like should move promptly to disclose publicly the following inventories:

- The government agencies – federal, state and local – that provide them with personal data and under what terms
- The kinds of personal data they collect
- The manner in which personal data are housed. To what extent is information from different sources co-mingled? Are there separate "silos?"
- Warranty card information – which database companies collect this, what are their sources, how is it stored and used?
- 800 Toll-free profiling data – consumers can give up personal information about themselves simply by calling well-equipped 800 phone numbers. The information that is captured by a Caller-ID type technology known as Automatic Number Identification (ANI) is stored and sold by some database companies.

State Agencies Should Suspend Sale of Some Personal Data Until Truth Be Known

Considering there remain many "unknowns" concerning the ChoicePoint episode in particular, and the database industry in general, it would seem prudent for some governmental agencies to suspend their release of at least some personal data to ChoicePoint until there is a full accounting.

There simply is no way of assessing the risk to consumers' privacy until we know the answers to the questions listed above. Therefore, it would be imprudent for agencies like State

Depts. Of Motor Vehicles to continue to permit the possibly under-supervised sharing of drivers' data with ChoicePoint until confidence is restored. Curbing the release of such data would help reduce the risk of breaches in the near-future, and could also expedite industry cooperation in establishing more robust consumer protections.

'Self-Regulation Already Failed'

Several database companies attempted to show that consumers did not need legal rights by "self-regulating." With much fanfare in 1997, some of them joined with the FTC to announce the "IRSG Principles" (Individual Reference Services Group).[6] While it seemed to offer some promise at the time, in hindsight the effort turned out to be little more than a public relations exercise designed to stave off Congressional action. Many of the FTC's privacy-related recommendations were not followed by industry.

ChoicePoint Wants Benefits, But Not Responsibility

ChoicePoint has been involved in various episodes relating to either improper collection of information or providing inaccurate information that unfairly disadvantaged individuals.

Prior to the 2000 George Bush-Al Gore presidential battle, Florida-based DBT Online Inc. signed a $4 million contract with the state of Florida to "cleanse" voter rolls of convicted felons. DBT, later acquired by ChoicePoint, had misidentified 8,000 Floridians as felons, temporarily barring them from voting. In July 2002, ChoicePoint settled out of court with the NAACP, which had sued on behalf of the voters. The company recently disputed charges by the Electronic Privacy Information Center that it was responsible for the incident.

"Simply put, ChoicePoint played no role in the Florida election in 2000. Database Technologies (DBT) performed the legally-mandated review of Florida's voter rolls prior to our acquisition in 2000. The process, a part of which included DBT, was created by the Florida legislature and implemented by State election officials. DBT was hired to create an overly inclusive list of potential voter exceptions based on criteria established by the Secretary of State, which DBT told the State might create false positives. County election supervisors – not DBT – were solely responsible for verifying the eligibility to vote of any voter identified by DBT on the exceptions list. In particular, county election supervisors – not DBT – were solely responsible for the decision to remove any voter from the rolls," wrote CEO Derek Smith in a statement posted to the company Web site.

Here are some other incidents:

- In 2000, ChoicePoint was accused of breaking its contract with the Pennsylvania Department of Transportation for posting drivers' records on the Internet. The State fined ChoicePoint $1.3 million and made the company agree to provide driver information only to insurance companies for insurance-related purposes. The State also barred the ChoicePoint employees involved in the posting from having any association with Pennsylvania records. (see Privacy Times, Vol. 20 No. 2, 1/19/00)

[6] http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm

- A pending lawsuit accuses the company of violating the Federal Drivers Privacy Protection Act by selling DMV data without drivers' consent (see Privacy Times, Vol. 23 No. 13, 7/1/03). ChoicePoint said in SEC filings that an unfavorable outcome in such a case "could have a material adverse effect on the company's financial position or results of operations."

- Also in 2003, ChoicePoint announced it would end its practice of obtaining and selling personal data on Mexican citizens for purposes of verifying identity and citizenship once the person was in the U.S. The information - name, address, date of birth and citizen ID number - was purchased by the Georgia-based company under a contract that required the vendor to certify the information was legally obtained and was available to be used for identity. ChoicePoint's Chuck Jones told the media that the company agreed to stop the practice because the results of a government inquiry determined the information was confidential under Mexican law. He said the data would be returned to government representatives and purged from the company's system. In April 2003, the AP reported that the U.S. government had bought access from ChoicePoint to data on hundreds of millions of residents of 10 Latin American countries - apparently without their consent or knowledge. The information allowed a myriad of federal agencies to track foreigners entering and living in the U.S. (see PT, Vol. 23 No. 13, 7/1/03).

  The same year, a federal judge in Kentucky ordered ChoicePoint to pay single mom Mary L. Boris $447,000 in punitive and actual damages for violating the Fair Credit Reporting Act by failing to corrected inaccurate insurance claims data after it was disputed. "ChoicePoint's witnesses made particularly negative impressions upon the jury," Judge John Heyburn II wrote. "They repeatedly denied making any mistakes and instead seemed to blame all defective data on others. Furthermore, ChoicePoint employees appeared slow to recognize problems even once they were put on notice and disclaimed all responsibility ... Most notable, they seemed annoyed at even having to appear at trial… ChoicePoint never really explained the computer glitches which apparently caused this problem. To this day, the court is still unclear what procedures, if any, ChoicePoint uses to (e)nsure the accuracy of its mass-circulated reports."

- In two separate cases in 2003, ChoicePoint settled out of court with Louisianans Deborah Esteen and Dorothy Moten Johnson for allegedly selling false information about them to potential employers, according to the *Atlanta Business Journal* and MSNBC. Johnson's background check supposedly revealed she was convicted of public payroll fraud. According to her suit, she had never been arrested or convicted of anything in her life.

Anyone can make mistakes. But what's most troubling about some of these incidents is what appears to be ChoicePoint's consistent unwillingness to take responsibility for them.

Moreover, a new article by Bob Sullivan at MSNBC found that two privacy activists who were able to review their ChoicePoint "general" file found many inaccuracies. For Deborah Pierce, one notation suggested a "possible Texas criminal history" and then recommended a manual search of Texas court records. Pierce had only been in Texas twice and never had a problem with police. There were also numerous inaccuracies in her past addresses and other routine data. The report also listed three automobiles she never owned and three companies listed that she never owned or worked for.

Richard Smith's dossier had the same kind of errors as Pierce's. His file also suggested a manual search of Texas court records was required, and listed him as connected to 30 businesses which he knew nothing about.

It also said that he and his wife had a child three years before they were married, that he had been married previously to another woman, and most absurd, that he had died in 1976. "Pretty obviously the data quality is low," Smith said. He equated a ChoicePoint report to the results of a Google search on a person -- solid information is mixed in with dozens of unrelated items. The more common a name, the more extraneous information is produced.

These descriptions raise troubling doubts about ChoicePoint's methods for collecting data and ensuring accuracy.

Comprehensive Approach is Needed

As U.S. PIRG pointed out, Congress needs to fashion legislation that is based upon principles of "Fair Information Practices" (FIPs). Earlier, I mentioned the five principles developed by the 1973 HEW Task Force.

The Committee should also be guided by the 1980 FIPs developed by the Organization of Economic Cooperation and Development (OECD), with the endorsement of the U.S. Government, Japan and Western European governments. These eight principles are often referred to as the "Gold Standard" of privacy.

(1) Collection Limitation
(2) Data Quality
(3) Purpose Specification
(4) Use Limitation
(5) Security Safeguards
(6) Openness
(7) Participation
(8) Accountability

As mentioned before, the newly drafted "Model Regime For Privacy Protection," by Prof. Daniel J. Solove & Chris Jay Hoofnagle offers even more specific guidance for the issues before the Committee. They are:

Notice, Consent, Control, and Access

1. Universal Notice.
2. Meaningful Informed Consent
3. One-Step Exercise of Rights.
4. Individual Credit Management
5. Access to, and Accuracy of Personal Information.
Security of Personal Information.
6. Secure Identification.
7. Disclosure of Security Breaches.

Business Access to and Use of Personal Information

8. Social Security Number Use Limitation.
9. Access and Use Restrictions for Public Records.
10. Curbing Excessive Uses of Background Checks.
11. Private Investigators.

Government Access to and Use of Personal Data

12. Limiting Government Access to Business and Financial Records.
13. Government Data Mining.
14. Control of Government Maintenance of Personal Information.

Privacy Innovation and Enforcement.

Effective Enforcement of Privacy Rights.

Mr. Chairman, thank you again for this opportunity. I would be happy to answer any questions and look forward to working with this Committee and others to fashion a solution to the problems raised by these recent data leakages.