epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC

Hearing on

"Identity Theft: A Victim's Bill of Rights"

Before the

United States House Committee on
Oversight and Government Reform,
Information Policy, Census and
National Archives Subcommittee

June 17, 2008
Room 2154, Rayburn House Office Building
Washington, DC

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on "Identity Theft: A Victim's Bill of Rights." My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a non-partisan, public interest research organization, focusing on emerging privacy and civil liberties issues. EPIC has particular interest in the problem of identity theft and we appreciate the interest of this Committee in this very important topic.

The problem of identity theft in the United States is substantial, growing and evolving. According to the Federal Trade Commission, identity theft is the number one concern of American consumers. And it is on the rise. Further, what was once understood as a financial crime is now entering other realms. Medical identity theft is a growing problem. And problems may soon emerge with many of the new web-based government services unless the problem of identity management is not adequately addressed.

Several steps have been taken to assist the victims of identity theft and to prosecute criminals. But in our opinion, none of these efforts get to the root causes of the problem. The Federal Trade Commission assists consumers *after* they believe they have been victims of identity theft. The Federal Bureau of Investigation investigates cases of identity theft *after* the crime has occurred. Even the former President's Identity Theft Task Force focused primarily on expanding prosecutorial authority rather than reducing the likelihood that the crime would occur. While the FTC's "Red Flags Rule" is a step in the right direction, more should be done to prevent Americans from becoming identity theft victims.

In my testimony today, I will outline the elements of a more comprehensive strategy to address the problems of identity theft. The strategy highlights the new forms of identity theft, draws on several proposals already under consideration in Congress, considers how technology could give individuals greater control over their personal credentials, and avoids the tendency to deal with the problem after it has occurred.

In the end, I believe that our goal should be to reduce the number of people who are victims of identity theft. But that will require getting to the source of the problem and reducing the opportunities for the crime to occur.

I. The Problem of Identity Theft

If a person steals cash from your wallet or a camcorder out of the back seat of your car, you are generally aware of the crime, can quickly assess the damages, and are unlikely to suffer any greater harm. The cash is gone. The camcorder is gone. But that is the extent of the loss. That is the end of the story.

If a person obtains your credit card number or obtains the credentials that allow you to open a bank account, to receive medical care, or to access a web site, it is very different story. First, you probably will not know when the theft has occurred. Second, you probably will not know when you are harmed. Third, even if there is an investigation, it is unlikely that you will be able to continue to use the credentials as you have in the past. New accounts will be established, new numbers will be created. But the fraudulent transactions will linger and the ongoing harm to your credit record, your medical records, even your web access remains.

The loss of control over the credentials that make it possible for us to engage in financial transactions, receive medical care, or even communicate online poses a very different problem than the hazards associated with traditional theft. As others have noted, identity theft is both a crime and it facilitates further crime. Public concerns about identity theft are widespread. Identity theft ranks first on the FTC's 2008 survey of consumer complaints.[1] An April 2007 Zogby Interactive Survey "found that ninety-one percent (91%) of adult users on the Internet are concerned that their identities may be stolen (including fifty percent (50%) who are very concerned)."[2] As of June 2005, forty-eight percent (48%) of consumers avoided making purchases on the internet because they feared that their financial information might be stolen.[3] Consumers' concerns are well founded. Identity theft complaints exceeded 300,000 in 2008.[4] The A FTC study estimates that identity theft costs Americans approximately $15.6B annually.[5]

Both businesses and government need to consider how best to provide services while minimizing the risk that personal information will be misused.

II. Medical Identity Theft

The problem of identity theft is not limited to financial fraud. Medical identity theft takes place when a fraud utilizes an individual's personal identity to take advantage of insurance benefits, to gain free medical services, or even to create fake claims for financial assistance using the individual's identity. There have been 19,428 complaints regarding medical identity theft to the Federal Trade

---

[1] Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2008, http://www.ftc.gov/opa/2009/02/2008cmpts.shtm.

[2] *Zogby Poll: Most Americans Worried About Identity Theft*, *available at* www.zogby.com/search/readnews.dbm?ID=1275 *cited by Prepared Statement of the Federal Trade Commission House Committee on the Judiciary on Protecting Consumer Privacy and Combating Identity Theft, Before the Subcommittee on Crime, Terrorism, and Homeland Security* (December 18, 2007).

[3] Cyber Security Industry Alliance, Internet Security Voter Survey (June 2005) at 9 *available at* https://www.csialliance.org/publications/surveys_and_polls/CSIA_Internet_Security_Survey_June_2005.pdf.

[4] Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2008, http://www.ftc.gov/opa/2009/02/2008cmpts.shtm.

[5] Federal Trade Commission, Federal Trade Commission – 2006 Identity Theft Survey Report, *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

Commission since January 1, 1992, the earliest date the FTC began recording such complaints.[6] According to the World Privacy Forum, "medical identity theft victims need an expanded right to correct their medical files in order to recover from this crime, and need more specialized consumer education that is focused on correcting the specific harms of medical identity theft."[7]

It is particularly important to implement safeguards against medical identity theft because the damage arising from the crime is severe, and recent efforts to digitize all medical records exposes increasing numbers of Americans to risk. The American Recovery and Reinvestment Act of 2009 establishes a National Coordinator for Health Information Technology, who is tasked with developing a "nationwide health information technology infrastructure that allows for the electronic use and exchange of information."[8] The law also provides for the expenditure of substantial federal funds to enhance the infrastructure for electronic health records.[9]

Although a transition from a paper system to an electronic system may be inevitable, "the transition must be done correctly and with an acknowledgement of risks such as those medical identity introduces, in mind."[10] Digitized patient records and the National Health Information Network in particular create two significant problems in the context of medical identity theft. The National Health Information Network "may make individuals more vulnerable to medical identity theft by making personally identifiable health information more accessible to criminals who have already learned how to work inside the health care system."[11] Digitized information is much more portable and lends itself to rapid transmission. These attributes are generally viewed as beneficial – they enable patients and health care providers greater access to medical records. However, in the hands of identity thieves, these benefits can become liabilities. Identity thieves can steal and transmit patients' health insurance data with the same ease that pathologists transfer patients' test results to treating physicians.

In the online context, consumers have little understanding of the risk of identity theft. Identity thieves continue to succeed through phishing, pretexting, and spyware and the mere lack of attention by consumers. This lack of attention clearly goes hand in hand with consumers' lack of knowledge regarding the true dangers that may be present. Users are often focused on their primary tasks, and may not notice security indicators or read warning messages.[12] Additionally, lack of attention

---

[6] World Privacy Forum, Medical Identity Theft: The Information Crime that Can Kill You (May 3, 2006) *available at* www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.
[7] *Id*.
[8] The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 § 3001 (2009).
[9] *Id*. at §§ 3011, 3018.
[10] *supra* note 7.
[11] *Id*.
[12] *Id*. at 3.

to the absence of security indicators can be just as threatening. Users can easily overlook indicators for pages not protected by SSL.[13]

III. Recommendations

1) Government Needs to Consider Privacy Protection in the Development of Web 2.0 Services

We strongly support the recommendations of the Government Accountability Office to improve the security of agency databases that contain personal information. As the GAO noted, "The first key step is to develop a privacy impact assessment--an analysis of how personal information is collected, stored, shared, and managed--whenever information technology is used to process personal information." [14] The GAO also recommends that agencies establish robust information security programs as required by the Federal Information Security Management Act (FISMA) of 2002.

The problem is that the federal government is now moving forward with a series of recommendations to expand public access to government information without adequately considering the privacy consequences.[15] While we favor the President's call for increased collaboration, participation, and dissemination of government information, it is equally important to ensure that these programs do not jeopardize important privacy interests.

EPIC has made specific recommendations to the Department of Homeland Security and to the Office of Science and Technology Policy to address some of these challenges.[16] Specifically, we said that the government should:

- Stop the Commercialization of Personal Data Held By Government Agencies
- Don't Track Users on Government Web Sites
- Apply the Privacy Act to All Data Collected by the Government and Government Contractors
- Apply Meaningful Rules for Public Comment Across All Platforms
- Promote Open Government and Protect Privacy

All of those proposals received many favorable comments – the proposal to limit the commercialization of personal data held by federal agencies was particularly

---

[13] *Id*. at 3.
[14] Privacy: Preventing and Responding to Improper Disclosures of Personal Information: Summary, U.S. Government Accountability Office, http://www.gao.gov/products/GAO-06-833T (last visited June 12, 2009).
[15] *See*, *e.g.* President Barack Obama, Memorandum on Transparency and Open Government, January 21, 2009 *available at* http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment; The White House Open Government Initiative, http://www.whitehouse.gov/open/; Public Workshop: Government 2.0: Privacy and Best Practices, 74 Fed. Reg.17876 (April 17, 2009).
[16] http://opengov.ideascale.com/akira/pmd/6537-4049

popular. But there is no indication so far that the OSTP will carry forward these safeguards as it considers the deployment of new web 2.0 tools.

We would ask the Committee to look more closely at privacy safeguards for new web-based government services.

2) Government Needs to Consider Privacy in the Outsourcing of Government Services

A related concern to the web 2.0 developments is the need to ensure that private contractors that obtain personal information from government agencies safeguard all of the information they obtain in accordance with the requirements of the Privacy Act. This is particularly important because individuals are often required to provide information to government agencies to obtain licenses, to purchase property, to pay taxes, to receive benefits, and so on. This could be a serious problem with the increased outsourcing of tax collection, which makes available very sensitive financial information to private firms.

There is no sense in which a "privacy policy" is sufficient to protect the privacy of American citizens in this context. There must be enforceable privacy rights that bind all private contractors that obtain personal information from the federal government and there must be regular audits to determine compliance with legal standards.

There are numerous stories of private contractors misusing access to personal information, including the reports in the 2008 presidential campaign season when State Department contractors improperly accessed the passport files of the Senator Obama, Senator Clinton, and Senator McCain.

We would ask the Committee to consider additional steps that could reduce the risk of identity theft resulting from the transfer of personal information to the private sector.

3) Comprehensive Privacy Legislation is Necessary

The identity theft problem continues to escalate in part because it is too easy for companies to collect personal information and too difficult for individuals to safeguard their information once it is in someone else's possession. Privacy policies do not provide privacy protection. All too often, they simply provide a waiver or disclaimer that allows companies to collect and use personal information as they wish.

To reduce the risk of identity theft in the United States, Congress must adopt privacy legislation that places greater responsibilities on companies that collect and use personal information. Oversight by regulatory agencies, such as the Federal Trade Commission, is helpful, but individuals must also be notified when their data

has been improperly released and they need an opportunity to seek damages when companies fail to safeguard the information they collect.

Comprehensive privacy legislation, including breach notification, will place appropriate burdens on companies that collect personal data. They will need to consider the risks of gathering sensitive data, such as Social Security Numbers, and of storing data longer than is necessary. Such legislation should also create incentives to develop new techniques that make it more difficult to commit identity theft and other crimes involving personal information. And it should not preempt stronger state laws.

4) Cybersecurity Policies Must Focus on the Protection of Personal Information

A related goal to reduce the risk of identity theft is to ensure that the nation's cybersecurity policies reflect a clear commitment to the protection of privacy. It is not simply computing resources that must be protected, but also the personal information about individuals stored on servers and transmitted across networks. Techniques that enable monitoring by third parties, even for lawful purposes, expose data that could be obtained and used for improper purposes. A cybersecurity policy that fails to consider this risk could actually magnify the danger of identity theft.

5) Better Systems for Identity Management Need to be Developed

One of the key goals for the federal government over the next several years should be the development of an identity management system that is scalable, robust, and secure. Where identification is necessary, individuals should have the ability to provide only the relevant credentials that are necessary for the transaction. They should not be asked to provide a unique identifier that links to all of their personal information or that increases the risk of identity theft.

The problem is that for too long the government has relied upon the use of the Social Security Number as the primary means to verify identity. This is a terrible practice for many reasons, not the least of which is the SSN's link to many, many record systems. Social Security Numbers are also frequently used as both a record locator and a password. Not surprisingly, access to another person's SSN is one of the easiest ways to commit identity theft.

These problems with the SSN are also the reason that privacy advocates and technical experts have opposed the establishment of the REAL ID, a more modern form of the SSN that would make it easy to link together databases as well as to commit identity theft once the system was compromised.

IV. Conclusion

In the years ahead, Americans will interact with government in an online world that is more complex and more information intensive than our current world. Even this Committee hearing, which was only recently made available over the Internet for viewing, could soon include blog posts, twitter feeds, and opinion polls that allow individuals to engage government and to express their views. Increased government openness and transparency is a boon for civic participation. But the government should exercise caution when implementing technologies that can expose citizens' personal information to identity thieves and other bad actors. And legislators should enact comprehensive, meaningful privacy safeguards to protect individuals' personal information.

Thank you again for the opportunity to appear before the Committee. I will be pleased to answer your questions.