Pennsylvania Senate Committee
Communications & Technology Committee
Testimony
Lillie Coney
May 11, 2011

Senate Bills 354, to Exempt Pennsylvania from REAL ID,
Senate Bill 355 regarding Swiping of Drivers' Licenses, and
Senate Bill 356, to Restrict State Government's Use of Biometric Data

Chairman Mike Folmer, thank you for the opportunity to appear before the committee today. My name is Lillie Coney and I am Associate Director of the Electronic Privacy Information Center in Washington, DC. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. EPIC is located in Washington DC and routinely testifies before Congress, Federal agency proceedings and before state legislative committees.

The legislation before the committee today addresses key privacy issues facing policy and decision makers both in the capitol of Pennsylvania and the nation's capitol: protecting the privacy and civil liberties of residents.

Defining Privacy

The right of privacy is defined by the degree to which an individual has control over whom, when, why, and how another may collect, retain, or use their "personal identifiable information" (PII). This relates to one or more data elements that may be used to uniquely identify a person or persons for among a group of people. Typically, PII that would include a name, address, Social Security Number, date of birth, mothers maiden name, home town, high school, birthmarks, tattoos, phone number, e-mail address, biometric, etc. Today, new forms of personally identifiable information would include e-mail addresses, keystroke patterns, biometric information, and IP addresses of digital devices.

The challenge is to create a definition for the term "personally identifiable information" that recognizes the ever-evolving risks to privacy presented by the adoption of new technology. The complexity of the challenge before legislatures is that identity in a cyber-enabled computer communication environment is very different from that of our physical world. A first name, last name, or first initial and last name was often the first piece of information needed to identify an individual in the pre-networked computerized world. Today, a name is not needed to identify a person with extreme accuracy.

In 2006, AOL published a list of 650,000 users' search queries on the Internet. The 20 million search terms included names, addresses, and SSNs, as well as a number of sensitive topics. Queries were listed under individual "user numbers," though users were not identified by name or screen name. Even though AOL later apologized and removed the pages with the information, subsequent copies of the data remain online. A New York Times reporter was able to successfully re-identify a user based on the search histories made available by AOL.[1]

EPIC offers the following observations from our research on the topic of identification and identification systems, which can be found in our publication of "Privacy & Human Rights 2006: An International Survey of Privacy Laws and Developments." The critical point is that many new forms of identification are emerging and effective legislation will need to address these challenges.

Protecting Privacy:

The protection of privacy is hardly a new problem. An 1890 journal article written by American lawyers Samuel Warren and Louis Brandies entitled the "Right to Privacy," captured the attention of law scholars, legislators, and the public. This law journal article has been cited and debated for over a century, and has guided the establishment of laws and international norms that restrain the power of technology and human curiosity to encroach on an individual's "right to be let alone."[2]

Privacy is the foundation upon which other fundamental rights—freedom of religion, association, political beliefs, ownership rights, locational privacy, family privacy, and freely expressed opinions rest.

The "Digital Information Age," ushered in a much-needed expansion of the fundamental human right of privacy. During the 1960s and 1970s, interest in the protection of privacy rights increased with the arrival of the information technology revolution. Congress and many state legislatures in their wisdom acted not in the wake of disaster, but prospectively to address the real threats posed by powerful computer systems. The Federal Privacy Act established the right of citizens to be free from government abuse and misuse of personal information, and the right to be informed of the actions taken by the federal government on their behalf.[3]

In 2006, the state of Pennsylvania became the 22nd state to enact a data breach law that provided guidance to data holders and comfort to residence that their personal

---

[1] Michael Barbara and Tom Zeller Jr., A Face Is Exposed for AOL Searcher No. 4417749, New York Times, page 1, August 9, 2006

[2] Samuel Warren & Louis Brandies, The Right to Privacy, 4 Harvard Law Review 193 (1890)

[3] Cornell University Law School, Legal Information Institute, US Code, available at http://www.law.cornell.edu/uscode/5/usc_sec_05_00000552---a000-.html

information held by others would be protected. [4] Pennsylvania is only one of four states with laws that require transparency in online privacy policies hosted by websites.[5] Because Pennsylvania represents 9% of the nation's population its actions to address the privacy protection of its citizens can have far reaching implications.

REAL ID

The REAL ID Act of 2005[6] creates a de facto national identification card. Ostensibly voluntary, it would become mandatory, as those without the card would face suspicion and increased scrutiny. It is a law imposing federal technological standards and verification procedures on state driver's licenses and identification cards, many of which are beyond the current capacity of the federal government. In fact, REAL ID turns state DMV workers into federal immigration officials, as they must verify the citizenship status of all those who want a REAL ID-approved state driver's license or identification cards. State DMVs would far move away from their core mission -- to license drivers.

REAL ID was appended to a bill providing tsunami relief and military appropriations, and passed with little debate and no hearings. The REAL ID Act repealed provisions in the Intelligence Reform and Terrorism Prevention Act of 2004, which contained "carefully crafted language -- bipartisan language -- to establish standards for States issuing driver's licenses," according to Sen. Richard Durbin. After more than two years, the Department of Homeland Security issued draft regulations for state compliance on March 1, 2007.

The National Conference of State Legislatures estimates that the cost to the states will be more than $11 billion over five years. This is more than 100 times the $100 million cost that Congress initially estimated. For 2006, $40 million was allocated for start-up costs. It is likely that the public will shoulder the cost. The Department of Homeland Security originally estimated that REAL ID would cost $23.1 billion over 10 years. But, when the agency released the final rule in January 2008, it made dubious assumptions and claimed that the national ID system would only cost $9.9 billion.

EPIC and 24 experts in privacy and technology submitted detailed comments in May 2007 on the draft regulations explaining the many privacy and security threats raised by the REAL ID Act. The fundamentally flawed national identification system is unworkable and the REAL ID Act must be repealed. In particular, the group admonishes DHS for its failure to include adequate privacy and security safeguards for this massive national identification database. DHS's own Data Privacy and Integrity Advisory

---

[4] Bruce Johnson, Privacy & Security Law Blog, January 6, 2006, available at http://www.privsecblog.com/2006/01/articles/state-legislation/pennsylvania-becomes-22nd-state-to-enact-a-data-breach-disclosure-law/

[5] National Conference of State Legislatures, March 17, 2011, available at http://www.ncsl.org/default.aspx?tabid=13463

[6] REAL ID Act, available at http://epic.org/privacy/id_cards/real_id_act.pdf

Committee has refused to endorse the agency's plan.[7] "The Committee feels it is important that the following comments do not constitute an endorsement of REAL ID or the regulations as workable or appropriate."

In a detailed analysis of the final rule, EPIC explained that the Department of Homeland Security's REAL ID system includes few protections for individual privacy and security in its massive national identification database. It harms national security by creating yet another "trusted" credential for criminals to exploit. The Department of Homeland Security has faced so many obstacles with the REAL ID system that the agency now plans an implementation deadline of 2017 -- nine years later than the 2008 statutory deadline. It is an unfunded mandate that would cost billions, with the burden ultimately being placed on the individual taxpayer.

Technical experts familiar with the challenges of privacy protection and identification presented the Department of Homeland Security with a variety of recommendations that would have minimized the risks of the REAL ID system. The DHS made some modifications, but left the essential system in place. As REAL ID currently stands, the costs are many and the benefits are few.

Recommendations: Pennsylvania Senate Bill 354

The State of Pennsylvania would be well advised to protect its citizens from the REAL ID Act. It is unenforceable, would lend itself to further attempts to erode the rights of citizens who were unable to meet the requirements imposed by the Department of Homeland Security. Further the benefits of REAL ID are uncertain, while the costs to states for collecting and retaining supplemental identification documents and the further burden of protecting those records would be nearly unbounded.

Drivers License Electronic Data Collection

The presenting of a driver's license so that a merchant could review the date of birth information has become accepted and routine in commercial settings where alcohol and later tobacco are sold. After decades of debate among local, state, and federal decision makers, health advocates, citizens and policy makers it was determined by many to be necessary to protect health, safety and welfare.

Today, more commercial establishments are routinely requesting drivers licenses and swiping them to access the personal information about the license holder stored on the card.[8] This action is not equivalent to asking a customer under a required statue to

---

[7] Data
Privacy and Integrity Advisory Committee, REAL ID Comments, available at http://epic.org/privacy/id_cards/dpiac_comm_050707.pdf

[8] Michael Finney, More retailers requiring driver's license swipes, ABC 7-KGO-TV San Francisco, May 13, 2010, available at http://abclocal.go.com/kgo/story?section=news/7_on_your_side&id=7441118

present a drivers license of state issued identification card to verify the age of a customer prior to completing a sale of alcohol or tobacco. One swipe of a drivers' license will allow within seconds the collection of a set of PII that can be added to a database. The purpose of this data collection is its value in the digital marketplace.

Points of sale in a commercial setting are not just about collecting payment for merchandise, but opportunities to collect personal information. Many of you have been asked at the check counter for your phone number, which you may have provided willingly, without a thought of why it was being collected. This PII in the form of a phone number does not change overtime. You have provided on written and e-forms online and it is a cell-phone it is even more valuable. Phone numbers can be used to track individuals over databases and over time.

The digital information economy runs on personally identifiable information—unfortunately, the more personal, and the more accurate information is the more value it has in the marketplace. Further trouble arises when the value of information is not diminished when it is inaccurate, which can have dire consequence for consumers. The temptation to collect and retain the personal information of customers even when they have not need to do so can lead to harm to consumers. Recently, millions of customers for some of the most reputable companies in the nation received e-mail notices regarding a data breach by a company named Epsilon. Walgreens, JP Morgan Chase, Ritz-Carlton Rewards, Marriott Rewards, and many other retailers and customer loyalty programs were impacted.[9]

I am sure that many of you and your staff, family members, and colleagues received notices regarding the Epsilon breach. A trusted retailer collected the data, but they used it not solely for the purpose you may have intended upon providing the information. In security, circles its called a "honey pot" a data set so valuable that it would be attractive to thieves. Privacy experts know what the consequence may be for consumers—such as more accurate pharming and phishing attacks, where are based on guessing the right bank or retailer to trick consumers into giving up valuable information. If you use e-mail you have seen pharming and phishing attempts—they are e-mail promising riches if you will take receipt of a large amount of money, or saying that they are from a financial institution. Most consumers have learned to delete these messages with no hesitation. Now imagine thieves with the right banks and e-mail addresses of their customers under the same circumstances. Thieves are patient, and when they send messages that look like they came from your bank or retailer with a request to log into your account they may be more successful than any previous attempt at this form of theft in the past.

Targeting customers with means will be easier; creating messages that will be successful will the most difficult thing. If you are wise, you block messages from any

[9] Fahmida Y Rashid, Epsilon Data Breach Hit Banks, Retail Giants, E-Week, April 4, 2011, available at http://www.eweek.com/c/a/Security/Epsilon-Data-Breach-Hits-Banks-Retail-Giants-154971/

retailer who breached your e-mail privacy; if you are fortunate, you change your e-mail address and alert people whom you want to continue to receive communications from. But, it is EPIC's position that consumers should not have to worry about any of this if data collector were required to follow a set of fair information practices that would place controls on how PII could be used and create transparency for data subjects on how their information is being used.

Finally, private sector data warehouses far out strip any data collection by state or federal agency. Few states, and only a handful of federal laws protect this information. When the data is outside of the direct collection by the federal government the Federal Privacy has not been determined to apply. Federally funded local and state "Fusion Centers" have targeted integrating private data sources for use by these data collection, analysis and reporting facilities. Fusion centers are a means of bringing together information from distributed sources for the purpose of collection, retention, analysis, and dissemination. The list of Fusion Center entities includes every type of business, utility, public service agency, and education institution imaginable.[10]

Recommendations Senate Bill 355

There may be reasons to use the verification and authentication features of state issued drivers licenses, but this should be expressly constrained by state law. Law for example that mandate verification of age for the purchase of alcohol or tobacco set the purpose for the collection and the use of the information. However, a remote electronic verification process should be based upon an allowed or not allowed report from the DMV in the case of alcohol or tobacco purchases.

Computers do not understand natural language; they operate on a very basic communication scheme that can only recognize two states, which are expressed in human terms as a "one" or a "zero." This is also easily translated to be either true and false or in the case of a sale of alcohol or tobacco—yes or no. The swipe of a drivers licenses to authenticate someone as being approved to purchase alcohol or tobacco should only elicit an approved or not approved response. Any more would provoke data over collection or data over reporting. There is no need to know the persons birth date or age, place of employment, home address, phone number, blood type, or any range of data points that may be on a drivers license machine readable zone.

The bill could provide for notice to vendors or retailers regarding the implications for collecting drivers' license information, retaining that information for purposes not associated a state law.[11]

---

[10] Fusion Center Guidelines available at http://epic.org/fusion_center-appendix_c.pdf; more on Fusion Centers see: http://epic.org/privacy/fusion/

[11] EPIC, Federal Drivers License Privacy Protection Act, available at http://epic.org/privacy/drivers/

I would ask that the committee consider that the digital economy is monetizing personal lives of Pennsylvania residents. The overwhelming majority of consumers have no knowledge of the vast network of databases that house information about them to what extent that information is used to determine benefits or foregone opportunities for employment, loans, insurance, etc.

Any entity that collects personally identifiable information must disclose that information to consumers, the purpose of the collection, the intended use of the information, a consumers right to know how their information has been used, and to correct incorrect information, that the information must be secured against abuse or misuse by insiders or external threats. Finally, consumers must have the right to see redress of harms based on the abuse or misuse of information.

Finally, federal and many states protect the data on the drivers' license record. In 1989, a stalker killed a young woman who was just beginning a career. He was able to gain access to her home address because the DMV record was considered public information.[12]

Biometric Identification Systems

Universal identifiers, such as biometrics, will not solve the fundamental problem of how much damage an identity thief can do once a victim's identifiers are compromised.[13] Biometric authentication involves comparing the previously captured physical characteristics of a consumer with newly provided samples of that same characteristic.[14] This one fact alone means that there must be a registry of the biometric identifier to compare a sample with, such as is the case with the FBI fingerprint laboratory.

Biometrics collection of fingerprints is related to arrests of suspects, application for certain state licenses, and a requirement for certain jobs such as bank teller, or police officer. Over the years the numbers of fingerprints in the FBI's database has grown significantly. Today, the first of several steps in attempting to identify an individual based on fingerprints begins with computers selecting possible matches, then trained

---

[12] ID Investigation Discover, Rebecca Schaeffer, available at http://investigation.discovery.com/investigation/hollywood-crimes/schaeffer/rebecca-schaeffer.html

[13] Universal identifiers have also generated significant criticism on grounds of human rights. See, e.g. Richard Sobel, The Degradation of Political Identity Under a National Identification System, 8 B.U.J. SCI. & TECH. L. 37, 48 (2002). See also Nat'l Research Council, IDS – Not That Easy: Questions About Nationwide Identity Systems (Stephen Kent & Lynette Millett eds. 2002), available at http://www.nap.edu/catalog/10346.html?opi_newdoc041102 (last visited May 6, 2011).

[14] EPIC & Privacy International Privacy & Human Rights: An International Survey of Privacy Laws and Developments 49 (EPIC ed., 2006).

technicians making decisions regarding the final signatures comparison. For decades it was assumed that this process could be conducted without error, until an incident in 2004, when the agency identified the wrong person and for days refused to believe it had made a mistake. Brandon Mayfield an attorney living in Oregon for his bar requirement had provided fingerprints to the state, which were collected and retained by the FBI. Following the Madrid booming, crime labs around the world analyzed a fingerprint from a bag found at the scene of the terrorist attack. The FBI "called it 'absolutely incontrovertible' and a 'bingo match'," [15] in reports to the media.

Advances in technology now make it easier to collect fingerprints in remote locations. U.S. troops have been using mobile scanners to take fingerprints; eye scans, and input other personal data from Iraqis (and more recently, Afghans) at checkpoints, workplaces, the sites of attacks, and door-to-door canvasses. This information is being used to build an unprecedented identification database of Iraqis that is administered by the U.S. military. However, there is as yet no indication of any privacy safeguards protecting against the risk that this information will be used to fuel the ethnic cleansing. In 2007, the Los Angeles Police Department through a Department of Homeland Security Grant acquired mobile fingerprint collection devices.[16]

The results will be even larger data warehouses of fingerprint information, which will have to be completely reliant upon automated computer matching to determine the accuracy of a match. This is further complicated by the lack of common knowledge among the population on fingerprint identification. Software errors, hardware or firmware malfunctions all can led to breakdowns in a fully automated identification system.

Today, some retailers are now using fingerprint collection to facilitate point of sell transactions both in the US and abroad.[17] This trend will continue, which will make the ability to reliably say that a fingerprint is matched to a particular individual more difficult. The more places this type of data is collected the more likely it will be abused or misused by thieves. This is the road the SSN took when it began to be widely collected and used to track people over databases and overtime.

Recommendations Senate Bill 356

The steps outlined in this bill are forward thinking and acknowledge the many new forms of personally identifiable information that are unique biometrics. It is

---

[15] Jennifer L. Mnookin, "The Achilles' Heel of Fingerprints" Washington Post, May 29, 2004, Page A27, available at http://www.washingtonpost.com/wp-dyn/articles/A64711-2004May28.html

[16] http://urgentcomm.com/mag/radio_lapd_procures_mobile/

[17] Tom Young, Angelica Mari, Retailers fingerprint plans prompt privacy concerns, May 22, 2008, available at http://www.computing.co.uk/ctg/news/1826631/retailers-fingerprint-plans-prompt-privacy-concerns

important to create a mechanism for adding to this list of characteristics as new ones are identified.

It would be helpful if a report could be complied on the current use of biometric identification for the benefit of the committee's further work in this area. This would also inform citizens, researchers, decision makers, and your colleagues in other states on the state of this privacy issue. Too little is understood about how biometric information is being collected, retained and used.

Conclusion

The bills the committee is considering are important and worthy of the efforts of the authors and cosponsors to address the rising tide of data collection on Pennsylvania citizens. EPIC applauds your efforts and finds that states are better suited to act quickly to address privacy and consume problems much more effectively than federal efforts unless guided by the experience of the states.

We offer one caution; Congress over the past several decades has adopted a routine policy of pre-empting state privacy and consumer laws in favor of weaker federal statues. This practice is harmful to privacy and consumer rights. To the degree states can address this issue the better they will be able to react to new threats to privacy and consumer protection.

Thank you,

Lillie Coney
Associate Director
Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
http://epic.org/