Second Annual National Institute
Cyber Law: Expanding the Horizon

Lillie Coney
Associate Director, EPIC

Hearing on

"e-Data Breaches and Privacy Protection Statues: States v. Federal"

June 18-20, 2008

The old saying that "what you don't know won't hurt you" has rarely held true, and when it relates to data breaches, it is never true. According to the Federal Trade Commission, for the seventh year in a row identity theft is the number one concern of American consumers.[1] We also know that 216 million Americans have been impacted by data breaches.[2]

However, what is unknown is to what extent the lack of transparency on the part of industries, businesses, and data brokers about the full scope of data breaches frustrates the ability of the Federal government to make policy, enforce laws, and protect privacy rights of citizens. This is a far-reaching problem that impact Americans all across the country.

The foundation of privacy protection is the notion that individuals should have the ability to control when and under what circumstance personal information may be accessed and used.

History of Privacy Protection

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."[3]

In 1948, the right of privacy found a place in international law through its adoption into the Universal Declaration of Human Rights.[4] Article 12, states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The "Digital Information Age," ushered in a much-needed expansion of the fundamental human right of privacy. During the 1960s and 1970s the interest in the protection of privacy rights increased with the arrival of the information technology revolution. Congress in its wisdom acted not in the wake of disaster, but prospectively to address the real threats posed by powerful computer systems. The Federal Privacy Act

---

[1] Federal Trade Commission, Consumer Fraud and Identity Theft Complaint Data, January-December 2006, available at <http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf>.
[2] Privacy Rights Clearinghouse, A Chronology of Breaches, available at <http://www.privacyrights.org/ar/ChronDataBreaches.htm#3>, December 14, 2007.
[3] Samuel Warren & Louis Brandies, The Right to Privacy, 4 Harvard Law Review 193 (1890).
[4] Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A(III) on December 10, 1948, available at <http://www.un.org/Overview/rights.html>.

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.

The Privacy Act of 1974 was passed in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. However, its scope was limited to federal government agencies. It safeguards privacy of federal government-held records through the creation of four procedural and substantive rights in personal data. First, the Privacy Act requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it allows individuals to sue the government for violating the provisions of the Act.

There are, however, several exceptions to the Privacy Act. For example, government agencies that are engaged in law enforcement can excuse themselves from the Act's rules. Agencies have also circumvented information sharing rules by exploiting a "routine use" exemption. In addition, the Act applies only to certain federal government agencies (except for Section 7's limits on the Social Security Number (SSN) that applies to federal, state, and local governments). Aside from Section 7, the Privacy Act does not cover state and local governments, though individual states may have their own laws regarding record keeping on individuals.

Data Breaches a New Consumer Privacy Threat

On July 1, 2003, California became the first state to enact a law that required that entities report the losses of personal information directly to consumers. Data breaches for the purpose of this paper involve the loss of personal information as first codified under California Civil Statue 1798.29. The statue defines personal information to mean "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social security number, Driver's license number or ID number, account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."[5] In January 2008 the California breach notification law was expanded to include medical information, and health insurance information.[6]

The California breach notification law drew little notice when it first when into effect. However, that changes in February 2005, when it became known that ChoicePoint a large data broker had inadvertently sold identity thieves personal information on over

[5] California Civil Codes Section 1789.25-.39, available at http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=15005815040+0+0+0&WAISaction=retrieve

[6] Deborah Gage, California data-breach law now covers medical information, San Francisco Gate, January 4, 2008, available at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/04/BUR6U9000.DTL

145,000 individuals.[7] The company sought to comply with the law by informing all California residents of the data breach incident. The notice was reported in the press and it became apparent that the breach had impacted individuals who lived in other states, the District of Columbia, and three territories. ChoicePoint voluntarily expanded the breach notification to include all individuals harmed by the sell of data to bogus companies established by identity thieves.

Between July 2003 and February 2005, California was the only state with a data breach notification law enacted. On March 31, 2005, Arkansas became the second state with a data breach notification law enacted. That year 35 states considered breach notification laws, and twenty were successful in becoming law: "Arkansas, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana (applies to state agencies only), Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas and Washington."[8]

As of May 1, 2008, there are 42 states with data breach notification laws enacted.[9]

There are no reliable figures on the total number of data breaches, which have occurred. However, we can pinpoint the event that made the serious consideration of data breaches noteworthy.[10]

The Privacy and One Federal Legislative Effort: Cybercrime Enforcement Act of 2007

The Privacy and Cybercrime Enforcement Act of 2007 would strengthen penalties for identity theft, require notices for security breaches, and establish privacy impact assessments for federal rulemakings.[11] To a great degree, the lack of transparency on data breaches, computer system breaches, anomalies, and software failures inhibits the ability of the government to proactively address computer network vulnerabilities and enforce privacy laws.[12]

The failings of private actors to manage the personally identifiable information entrusted to their care justify the passage of H.R. 4175. Further, a recent report from the Samuelson Clinic confirms that the private sector is willing and able to act in putting in place security measures to protect computer networks that house personally identifiable

---

[7] Privacy Rights Clearinghouse, A Chronology of Data Breaches, available at http://www.privacyrights.org/ar/ChronDataBreaches.htm

[8] National Conference of State Legislatures, 2005 Breach Notification Laws, available at http://www.ncsl.org/programs/lis/cip/priv/breach05.htm

[9] National Conference of State Legislatures, Breach Notification Laws, available at http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

[10] Privacy Rights Clearinghouse, Chronology of Data Breaches, available at http://www.privacyrights.org/ar/ChronDataBreaches.htm

[11] Conyers, Smith, Scott, Forbes, Sanchez, Davis, and Jackson-Lee, H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007, November 14, 2007.

[12] Peter G. Neumann, Testimony, U.S. Senate Permanent Subcommittee on Investigations of the Senate Committee on Government Affairs, June 25, 1996.

information when there are state statutes that require notice to consumers should a data breach occur.[13]

Section 102. Failure to Provide Notice of Security Breaches involving Sensitive Personally Identifiable Information

This bill will do what the Privacy Act should have done—include private data networks under the requirements to protect personally identifiable information. This is a key component for the privacy protections afforded by "fair information practices" that are outlined in the Privacy Act. This effort will do what the Congress should have done upon completion of the 1974 law-- include private data holders, that manage records containing personally identifiable information under the requirements to protect that information, and to disclose failures to do so.

In 2006, the largest data breach in US history was revealed when TJX Companies Inc., acknowledged that at least 45.7 million credit and debit cards were stolen by hackers who managed to penetrate its network. Another 455,000 customers who returned merchandise without receipts were robbed of their drivers' license numbers and other personal information. Also in 2006 the Department of Veterans affairs reported that the names, SSN, and dates of birth of 26.5 million U.S. veterans were on a lap top computer that was stolen from a Virginia employee's home—the computer was later recovered.[14]

The provisions of the bill do not preempt state law, but rather create an important federal baseline. As we have learned, the states can respond more quickly than the federal government to emerging privacy challenges and it is very important that the federal government not limit the important work of the states in this area. As of August 2007, according to Consumers Union, 39 states had enacted laws requiring notice regarding data security breaches involving personal information.[15]

Defining "Sensitive Personally Identifiable Information"

The bill addresses the difficult issue of defining "personally identifiable information," which is a key step in addressing the security of personally identifiable information. The names, addresses, and phone numbers of individuals are clearly personally identifiable information and should be protected. The bill also correctly covers other types of identifiers, such as a Social Security Number (SSN), biometric identifier or drivers license number that raise particular privacy risks when linked to a person's name. In fact, many of these identifiers alone could be considered "sensitive personally identifiable information" and should be separately protected.

---

[13] Samuelson Law, Technology & Public Policy Clinic, Security Breach Notification Laws: Views from Chief Security Offices, University of California-Berkeley School of Law, available at <http://www.law.berkeley.edu/clinics/samuelson/cso_study.pdf>, December 2007.
[14] EPIC & Privacy International, Privacy and Human Rights 2006, pages 23-36 (2007).
[15] Consumers Union, Notice of Security Breach State Laws, available at <http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf>, August 21, 2007.

The bill also allows the use of the last four digits of the SSN as a means of identification. This is a reasonable safeguard that EPIC has long advocated, but it may not fully address the privacy concerns associated with the use of the SSN. The SSN is a classic example of "mission creep," where a government-designed program instituted for a specific, limited purpose has become something completely different, sometimes with disastrous results.[16]

The SSN was created in 1936 to facilitate the administration of Social Security laws, a well-intended and proven benefit to our nation. Over time, however, legislation allowed the SSN to be used for purposes unrelated to the administration of the Social Security. For example, in 1961 Congress authorized its use by the Internal Revenue Service as a taxpayer identification number.

Congress in its deliberation on the 1974 Privacy Act recognized the threats posed by abuse of the SSN and made it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her SSN.[17] Unfortunately, due to the abuse of the SSN by the private sector for commercial purposes, consumers are routinely threatened with denial of benefits or services should they refuse to disclose the number to non-federal government actors.[18]

In 2006, the President's ID Theft Task Force was established to "track down criminals who traffic in stolen identities and protect American families from this devastating crime."[19] EPIC participated in the Task Force proceedings and provided extensive comments.[20] The Task Force recommended the reduction of reliance on SSNs at all levels of government, and pointed the misuse of the SSN by businesses.

Pattern recognition is the Achilles Heel of any security system. The SSN has been exploited to the point that for the benefit of all - today's consumers as well as the generations yet to come - the entire number should be protected, its use strictly limited by force of law.

The challenge is to create a definition for the term "personally identifiable information" that recognizes the ever-evolving risks to privacy. As written in the bill, the definition of personally identifiable information is too narrow. 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

---

[16] Marc Rotenberg, Executive Director, EPIC, Testimony, Protecting the Privacy of the SSN from Identity Theft, available at <http://www.epic.org/privacy/ssn/idtheft_test_062107.pdf>, June 21, 2007.
[17] Privacy Act of 1974, 5 U.S.C. § 552 (a) (2006).
[18] GAO Report, Social Security Numbers: Subcommittee Questions Concerning the Use of the Number for Purposes Not Related to Social Security, <http://epic.org/privacy/ssn/gao-00-253.pdf>, July 2000
[19] Press Release, Office of the Press Secretary, Fact Sheet: The President's Identity Task Force, available at <http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html>, May 10, 2006.
[20] EPIC, Comments to the Federal Identity Theft Task Force, P065410, available at <http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf>, January 19, 2007.

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.[21]

The bill makes a good start on this challenge, but more will need to done in order to adequately protect the privacy of individuals. 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.

New Forms of Identification and New Privacy Risks

In recent years, technology has evolved rapidly to enable electronic record creation and the construction of large commercial and state databases. The trend in technology is that computers and networked systems that contain personally identifiable information are on the rise.[22] The forms of information used to identify and track persons online can be static, such as screen names or computer-assigned Internet Protocol addresses; or dynamic, such as in the case of service-assigned Internet Protocol addresses, which can change. Dynamic Internet Protocol addresses are small software files stored on users' personal computers, with or without the users' knowledge, by web sites, web site advertisers, electronic communications, or search engine services as a means of tracking and recording online activity.[23]

The privacy and consumer rights advocacy communities are becoming increasingly aware of the threats posed by a whole host of activities based on what has been termed "micro-targeting." The amounts and types of personally identifiable information that may eventually rest in the hands of businesses because of the pervasiveness of this type of surveillance are tremendous.

---

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

[22] EPIC and Privacy International, Privacy and Human Rights 2006, pages 23-36 (2007).

[23] EPIC, Privacy? Proposed Google/DoubleClick Deal, available at <http://www.epic.org/privacy/ftc/google/>, see also Center for Digital Democracy <http://www.democraticmedia.org/> and US Public Interest Research Group <http://www.uspirg.org/> 2007.

EPIC has also noted a rapidly expanding use of biometrics, from the physical capture of digitized signatures of consumers at the point of sale at retail establishments to the collection of fingerprint scans or fingerprint geometry. The latter practice is being deployed in a broad spectrum of contexts, from retail customers to elementary schools.

Emerging technologies for identification of individuals include face recognition systems, hand geometry (palm prints), voice recognition systems, gait recognition (how a person moves), and DNA databases.

In addition to these areas of identification, the definition should also reflect that identity could be derived from with whom we associate in our day-to-day on-line and off-line lives. Freedom of association is fundamental to our democratic experience. Social justice, environmental, religious, and political movements have their foundation in the freedom of persons who share like beliefs to associate with one another.

The deployment of Fusion Centers absent the oversight of federal government regulation or statutes to control and direct the application of surveillance is a threat to privacy and civil liberties.[24] Fusion Centers marks the emergence of an inter-networked communication infrastructure that could facilitate the creation of a modern surveillance society. The name given to the criminal justice/national security components of this endeavor are "information fusion centers." Fusion Centers are an amalgamation of commercial and public sector resources for the purpose of optimizing the collection, analysis, and sharing of information on individuals. To achieve this objective, underlying communication infrastructure must support access to identity data networks that are managed by federal and state agencies of every description as well as private sector data warehouses.[25]

Another consideration for defining privacy should include the especially sensitive area for victims of domestic violence who have minor children or dependents.[26] The bill considers the issue of a mother's maiden name, but EPIC would strongly encourage that in the interest of privacy and security that other relationships be considered in the scope of the definition of "personally identifiable information."

For the reasons outlined above, data breach protection should ensure routine review of the definition of personally identifiable information so that the law will remain abreast of changes as custom, technology, and the law forge new relationships that define our identity in cyberspace.

The Entire Data Record Must be Protected

[24] EPIC, Fusion Centers and Privacy, available at <http://www.epic.org/privacy/fusion/>.
[25] Lillie Coney, Testimony, DHS Privacy Advisory Committee, available at <http://www.epic.org/privacy/fusion/fusion-dhs.pdf>, September 26, 2007.
[26] EPIC, Domestic Violence and Privacy, available at <http://www.epic.org/privacy/dv/>.

EPIC endorses the bill language that requires "technology protection measures that renders the data element indecipherable."

EPIC offers the following observations and recommendations for the committee's consideration. This provision of the law should apply to the protection of all personally identifiable information in digital form. It will not matter to the victim of a data breach if the information was lost through accident, poor security practices, or mischief. We note that significant data breaches have occurred because of poor security practices or circumvention of security measures, such as removal of large quantities of data records from office locations on personal portable computer devices that were subsequently lost or stolen. Data can also be lost or stolen by insiders who abuse or misuse legitimate access to data networks or computers.[27] The miniaturization of computer storage devices is making the specter of insider abuse of information networks more pressing.[28] Computer storage devices literally the size of an adult's thumb can potentially hold thousands of records. For these reasons, EPIC recommends that the bill include language that requires the application of proven and sufficient cryptographic measures to protect and control access to personally identifiable information.

EPIC supports the language in the bill that focuses on actions of "covered obligation," because of the harm caused to consumers by data breaches. We are also in strong favor of the definition of "security breach" as defined by the bill, which encompasses "the security, confidentiality, or integrity of computerized data that there is a reason to believe has resulted in a improper access…" Further, we concur with the findings of the Samuelson Clinic's report that companies are reacting to address the problem of data breach only in the presence of state statutes that require breach notification to consumers. Finally, we recommend that the entire data record be protected with cryptographic and data access protocols that create oversight and accountability for the protection of personally identifiable information. The required reporting of data breaches to federal government agencies, coupled with the publication of breaches in the federal register are powerful tools to help consumers and the federal government define the scope of the problem. Secrecy has never been a good rule for increasing security—disclosure makes the process of addressing computer security vulnerabilities viable.[29]

Ownership of Personally Identifiable Information

We are our data—a cyber-based economy will mean that our lives are judged by the sum total of personal information that is collected, stored, maintained, and shared among commercial data holders. The bill's "Obligations to Report" identifies the "person who owns or possesses data" as the responsible party. EPIC recommends that

[27] Peter G. Neumann, Computer Related RISKS, Chapter 8, A Human-Oriented Perspective, Addison-Wesley Publishing Company, 1995.
[28] Bruce Schneier, Big Risks Come in Small Packages, Wired News, available at < http://www.wired.com/politics/security/commentary/securitymatters/2006/01/70044>, January 26, 2006
[29] RISKS Digest, Dodger, The, Visibilities viable. Cyber-terrorists blackmail banks and financial institutions, available at <http://catless.ncl.ac.uk/Risks/18.17.html#subj6.1>, June 2, 2006

the focus should not be limited to ownership, but should extend applicability of the statute to anyone who "has custody" of personally identifiable information. This approach will leave in play state statutes or federal protections that exist to aid consumers or states, where data breaches protection laws are enacted.[30]

Today there are product offerings that provide data storage options that move repositories for business, and personal information from the business or home computer to host computer sites that provide storage and processing services.[31] In addition, social networking sites are proving to be attractive to individuals as a means of communicating with others, but it is also creating a wealth of information on the private lives of users.[32] Social networking web sites, such as MySpace, Facebook, and Friendster have become established forums for keeping in contact with old acquaintances and for meeting new ones. Users can create their own web page and post details about themselves: where they went to school, their favorite movie titles, and their relationship status. They can link to friends on the same site, whose photos, names, and perhaps a brief description, will also appear on the webpage. While these websites are useful tools for exchanging information, there has been growing concern over breaches in privacy caused by these social networking services.

E-mail services, such as Google's Gmail, provide what is described as "free" email and large storage capacity in exchange for the ability to enable auto-text reading of customers and incoming and outgoing e-mail communications and serving ads based on the content of messages. The privacy of Gmail subscribers is definitely an issue, and for e-mail senders to Gmail subscribers the reading of e-communication should be prohibited. The communications involved can be private personal matters, business or organization plans, or deliberations on a sensitive business or policy discussion. How this e-mail system might be used is open for discussion, but what should be very clear is that the communication content of these messages includes personally identifiable information.

Federal Statues and Breach Notification:

Title II – Non-Criminal Privacy Enforcement and Privacy Impact Statements

EPIC is very pleased with the bill's language found in Section 202, that describes coordination of state and federal efforts, except in cases where the state attorney general determines that it is not feasible to provide notice to the US Attorney General when filing of an action. The bill does allow for the US Attorney General to stay any non-Federal action under section 201 pending the resolution of a pending federal case under section 201 of this title.

---

[30] Consumer Reports, Notice of Security Breach State Laws, August 21, 2007.
[31] Computer Storage Services, available at <http://www.computerstorageservices.com/>, December 2007.
[32] EPIC, Social Networking Web Sites, available at <http://www.epic.org/privacy/socialnet/default.html>.

It is the experience of privacy and consumer advocates that the States play a vital role in identifying and addressing threats to consumer right, often more quickly than the federal government. As a rule, the federal government should establish a floor in the areas of privacy and consumer protection, which act as a complement in facilitating the States' vital function in these areas of law.

Section 203. Requirement that Agency Rulemaking take into Consideration Impacts on Individual Privacy

EPIC is very supportive of the bill language regarding Privacy Impact Assessments and rulemaking. The stress on greater and statutorily defined obligations to provide transparency on the rulemaking process related to Privacy Impact Assessment requirements is important for the following reasons:

First, the language of the bill is explicit: "Whenever an agency is required by Section 553 of this title, or any other law, to publish a general notice of proposed rulemaking for a proposed rule, or publishes a notice of proposed rulemaking for an interpretative rule involving the internal revenue laws of the Untied States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information for 10 or more individuals, other than agencies, instrumentalities, or employees of the federal government, the agency shall prepare and make available for public comment an initial privacy impact assessment that describes the impact of the proposed rule on the privacy of individuals."

Second, transparency is a key component of a functioning healthy democracy. It can be translated into public policy decisions that allow citizens, policymakers, and the media to assure themselves that a local, state or federal government agency is functioning as intended.[33] This title of the bill will serve the purposes of checking the authority exercised by federal government agencies as it relates to privacy rights. The section also creates a necessary bridge between the enforcement of several Federal statutes with complementary purposes—the Privacy Act, Freedom of Information Act, the E-government Act.

Finally, the language will remove ambiguity that may currently exist in the minds of agency administrators regarding their obligations to make public information related to privacy impact assessments. EPIC filed a court challenge to an attempt by the Transportation Security Administration to withhold a Privacy Impact Assessment from the public, which was in violation of federal law.[34] EPIC requested the Privacy Impact Assessments from the TSA under the Freedom of Information Act, and received heavily

[33] EPIC, Litigation Under the Federal Open Government Laws (FOIA) 2006, web page, available at <http://www.epic.org/bookstore/foia2006/>.
[34] EPIC v. US Transportation Security Administration, Civil Action No. 03-1846 (CKK), available at <http://www.epic.org/privacy/airtravel/pia_order.pdf>, August 2, 2004.

redacted documents from the agency in its reply.[35] EPIC sued the agency for full disclosure of the documents as required by the E-Government Act. The TSA argued that the Federal Privacy Act and the E-Government Act, which requires publication of Privacy Impact Assessments, were segregated.

EPIC is pleased to see the language of Section 553 (2) (A) because it is the heart of our nation's Federal Privacy Act. The bill embodies the much-awaited linking of the protections of the fair information practices provisions outlined in the Federal Privacy Act to the E-Government Act. Privacy rights and privacy impact assessments are made whole by creating a level playing field regarding the collection and use of personally identifiable information. The requirements that privacy impact assessments measure and report on whether an individual is informed by a federal government agency at the time of collection of personally identifiable information that it is occurring, allowing persons access to such information, preventing the use of the information collected for one purpose to be used for another, requiring securing of the information, and in the event of compromise notice to consumers with 14 days of the date of compromise, will be the most important accomplishment of this statute should it become law.

EPIC strongly endorses section 553a guidance on the agency ruling making process as it relates to public notice of work related to Privacy Impact Assessments.[36] The requirement for a senior agency official to sign the final document will improve accountability and transparency on the agencies privacy impact assessment process.

Notice of proposed rulemaking is the key to the public's fuller understanding of what the privacy consequences might be for agency actions that impact personally identifiable information. The language found in Section 553a better serves the public comment process on matters related to privacy.

Regarding the "Final Privacy Impact Assessment," it is important to consider that electronic records are very elusive things—it may be very difficult to enforce the intent of the provisions of this law without taking steps to ensure that there is transparency in the publication of e-documents that are only available via the Internet or its equivalent. For example, EPIC recently discovered in the midst of our involvement in an agency proceeding before the Federal Trade Commission regarding the proposed merger of Google and DoubleClick that the Chair of the FTC's spouse's law firm Jones Day had one of the parties to the merger as a client.[37] The relationship was discovered because of a document posted on the Jones Day web site. The Jones Day web page referenced the European Parliaments and the US Federal Trade Commission proceedings on the merger request by Google and DoubleClick. Needless to say, we were surprised to discover this

[35] EPIC, Alert e-Newsletter, Volume 11.18, available at <http://legalminds.lp.findlaw.com/list/epic-news/msg00164.html>, September 24, 2004.
[36] Conyers, Smith, Scott, Forbes, Sanchez, Davis, Jackson-Lee, H.R. 4175, Section 203, November 14, 2007.
[37] EPIC, Privacy? Proposed Google-DoubleClick Deal, available at <http://www.epic.org/privacy/ftc/google/>, 2007.

relationship last Monday, December 10, 2007, and upon our review and analysis determined that it had not been disclosed during the agencies proceedings on the matter.

Upon our making a complaint requesting the recusal of the Chair from participation in the Commission's decision making role on the merger request—the e-document disappeared from the Jones Day web site. EPIC has the original e-document through no help of the Federal Trade Commission or Jones Day.[38] This is a serious matter and one that we hope that Congressional Oversight and Judiciary Committees will take under consideration. The two issues are fairness and transparency in agency proceedings where the stakes are high and the interest in the billions of dollars. Agency rulemaking, like the rule of law under court proceedings, must be without blemish.

This phenomenon of the disappearing e-document is not limited to non-government Internet publications; it has also been observed by EPIC in the actions taken by federal government agencies when publishing documents online. For example, the Election Assistance Commission, after voting on December 13, 2005 in a public proceeding to adopt new voting systems standards, posted the final document online. However, by March 2006 the document initially posted by the agency had been replaced by another version. The new version of the final guidance on voluntary voting systems standards had substantial changes to key areas of the final reported document. EPIC's voting project identified the document switch, and raised questions regarding the lack of transparency on the agency's part in not reflecting on the record the withdrawal of the version passed in December 2005 and its replacement with another document.[39] The highly controversial issue of electronic voting security coupled with public scrutiny of the process of standards development is an important indication that the oversight authority of the Congress should strictly enforce agency rule promulgation in electronic online formats.

EPIC is very supportive of the language in the promulgation of agency analysis, as it is very helpful to the cause of openness in federal government actions related to privacy rights.

In addition to the measures outlined in section 553 of the bill, EPIC recommends that the entire Privacy Impact Assessment announcements of public comment periods, final documents, agency analysis, and changes to documents be published in the federal register. We further recommend that version control measures be enforced on any electronic publication of these documents.

---

[38] EPIC, Recusal of Chair of the Federal Trade Commission in the Merger review for Google-DoubleClick Merger Request, see original motion available at <http://www.epic.org/privacy/ftc/google/recusal_121207.pdf> and the new filing available at <http://www.epic.org/privacy/ftc/google/recusal2_121307.pdf>.

[39] EPIC's Project the National Committee for Voting Integrity, documents, Security section Dec. 13, 2005 version, available at <http://votingintegrity.org/pdf/security-121305.pdf> and the Security section published on line sometime is early 2006, available at <http://votingintegrity.org/pdf/security-011206.pdf>.

Version control is a process developed by software engineers to keep track of multiple versions of documents in electronic form. Often, subsequent iterations of a document may appear to be very much the same, but in fact have minor or major differences. The adoption of version numbers, date and time stamps, and making available past versions (linked from the current e-version of the document), a change document (reflecting all changes made in the new version), and requiring that any update, or upgrades to web pages ensure that old link addresses for documents once made public remain in working order should go a long way in protecting the integrity and efficacy of laws to ensure transparency in rulemaking related to privacy impact assessments.

EPIC would caution that Section 553 (c) Waivers might offer opportunities for avoidance of compliance with the law. We note agencies' designation of broad "routine use" provisions that frustrate the intent of the Federal Privacy Act. If there is a pressing need for an agency to act without first conducting a privacy impact assessment due to some unforeseen or emergency situation, or if the rule is considered classified and only reported to oversight committees, thus requiring a reassessment under Section 553 (e), the period of reconsideration should be every 3 years until the provisions of 553 (a) are enforced.

Further, the collection of public comments is at least as important as the agency's internal decision making processes. EPIC and a coalition of organizations under the umbrella of the Privacy Coalition led a public comment campaign during the Department of Homeland Security's REAL ID rulemaking process.[40] Typically, the Federal agency comment process is so cumbersome and convoluted that if non-government groups had not invested so much time and resources on the issue of stopping REAL ID, promoting a grassroots public comment campaign would have been out of the question. Electronic access to the comment process should be easy for the average person to engage. The irony was that despite the difficulty of engaging the public comment process on REAL ID, the demand for access to the public comment process exceeded the agency's ability to manage the volume. In the last hours of the comment period on REAL ID the Department of Homeland Security's fax reception of comments was overtaxed, necessitating the addition of an e-mail option for comments to be sent. At the close of the effort over 10,000 persons successfully overcame the obstacles during the REAL ID public comment period.[41]

EPIC recommends that the bill stress access and usability features of the public comment process to enhance the effectiveness of the effort for gaining a true sense of the public sentiments regarding the privacy implications of Federal agency proposed actions. E-mail, faxes, webpage comment based systems should not be too complicated or require specialized knowledge to use. Several Privacy Coalition partners in the REAL ID Public Comment Campaign worked to make the process simple and accessible with great

[40] Bruce Schneier, Schneier on Security Blog, REAL ID Action Required Now, available at <http://www.schneier.com/blog/archives/2007/05/real_id_action.html>.
[41] Privacy Coalition, REAL ID Public Comment Campaign, available at <http://www.privacycoalition.org/stoprealid/#action> May 2007.

success.[42] EPIC also believes that all comments submitted during agency rulemaking public comment periods should be made available and accessible online, and should be available to the public at no cost.

Private Right of Action

Finally the private right of action afforded to those who object to the final rule promulgated by the action is very important for judicial oversight of an agency's decision making authority. The rules for the right of judicial review make it very important that the public notice provisions of the law rises to the level of "effective public notice." There should be great care taken to be sure that interested parties will have every opportunity to be made aware of the agency actions related to privacy impact assessments. For this reason, EPIC recommends that publication of the final rule should be in the physically published federal register in addition to any other electronic means available to the agency.

EPIC recommends that as an added incentive to agencies not to amend or change election documents on the final rules for privacy impact assessments that the date of a one-year limit can be adjusted accordingly should the agency's online version of the rule be altered, changed, become unavailable (that the time on the period to seek judicial remedy be extended by the exact amount of time that the e-version of document is not available to the public).

Conclusion

Security breaches and identity theft are serious problems in the United States. I fully recognize the benefits of new technology, more must be done to address the problems when technology breaks down or creates new risk to persona privacy.

Federal efforts to address problems with data breaches should focus on adopting best practices that are developed by states, while at the same time not preempting the ability of state to legislate in this area.

Thank you.

[42] Privacy Coalition, REAL ID Public Comment Campaign, available at <http://www.privacycoalition.org/stoprealid/#action> May 2007.

BIOGRAPHY – LILLIE CONEY

Lillie Coney is Associate Director with the Electronic Privacy Information Center (EPIC) in Washington, DC. She works at the nexus of technology, privacy and civil rights issues focusing on emerging policy and business practices that affect consumer rights. Her policy specialty is privacy and public elections. She is the Public Policy Coordinator for the National Committee for Voting Integrity (NCVI), and has testified before the Election Assistance Commission. She served on the Brennan Center Taskforces on the Security and Usability of Voting Systems. She also served as a member of the ACM Committee on Guidelines for Implementation of Voter Registration Databases. She has authored peer reviewed law journal articles and scientific publications, hosted policy discussions both in the United States and Canada, been cited in numerous research and policy reports on voting technology issues.

Ms. Coney also serves as the Coordinator for the Privacy Coalition. The Privacy Coalition has over 40 organizations and affiliates who share a commitment of freedom and privacy rights. She coordinated the coalition's REAL ID public comment campaign for the Department of Homeland Security's agency rule making process. She has testified before the Department of Homeland Security's Data Privacy and Integrity Advisory Committee in 2006 and 2007 on the deployment of CCTV Surveillance and "Fusion Centers."