Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, EPIC

Hearing on

"Identity Theft and Data Broker Services"

Before the

Committee on Commerce, Science and Transportation,
United States Senate

May 10, 2005
253 Senate Russell Office Building
Washington, DC

Mr. Chairman, and members of the Committee, thank you for the opportunity to appear before you today. My name is Marc Rotenberg and I am Executive Director and President 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. We are very pleased that you have convened this hearing today on Identity Theft and Data Broker Services.

The main point of my testimony today is to make clear the extraordinary urgency of addressing the unregulated sale of personal information in the United States and how the data broker industry is contributing to the growing risk of identity theft in the United States. There is every indication that this problem is getting worse.

Whatever your views may be on the best general approach to privacy protection, I urge you to take aggressive steps to regulate the information broker industry and to protect the privacy and security of Americans.

The Significance of the Choicepoint Matter

With all the news reporting of the last few months, it has often been difficult to tell exactly how a criminal ring engaged in identity theft obtained the records of at least 145,000 Americans. According to some reports, there was a computer "break-in." Others described it as "theft."[1] In fact, Choicepoint simply sold the information.[2] This is Choicepoint's business and it is the business of other companies that are based primarily on the collection and sale of detailed information on American consumers. In this most recent case, the consequences of the sale were severe.

According to California police, at least 750 people have already suffered financial harm.[3] Investigators believe data on least 400,000 individuals may have been compromised.[4] Significantly, this was not an isolated incident. Although Choicepoint CEO Derek Smith said that the recent sale was the first of its kind, subsequent reports revealed that Choicepoint also sold similar information on 7,000 people to identity thieves in 2002 with losses over $1 million.[5] And no doubt, there may have been many disclosures before the California notification law went into effect as well as more recent disclosures of which we are not yet aware.

---

[1] Associated Press, "ChoicePoint hacking attack may have affected 400,000," Feb. 17, 2005, *available at* http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10920220.htm.
[2] Robert O'Harrow Jr., "ID Theft Scam Hits D.C. Area Residents," Washington Post, Feb. 21, 2005, at A01.
[3] Bob Sullivan, "Data theft affects 145,000 nationwide," MSNBC, Feb. 18, 2005, *available at* http://www.msnbc.msn.com/id/6979897/.
[4] Associated Press, "ChoicePoint hacking attack may have affected 400,000," Feb. 17, 2005, *available at* http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10920220.htm.
[5] David Colker and Joseph Menn, "ChoicePoint CEO Had Denied Any Previous Breach of Database," Los Angeles Times, March 3, 2005, at A01.

The consumer harm that results from the wrongful disclosure of personal information is very clear. According to the Federal Trade Commission, last year 10 million Americans were affected by identity theft. Identity theft is the number one crime in the country. For the fifth year in a row, identity theft topped the list of complaints, accounting for 39 percent of the 635,173 consumer fraud complaints filed with the agency last year.[6] And there is every indication that the level of this crime is increasing.

Choicepoint is not the only company that has improperly disclosed personal information on Americans. Bank of America misplaced back-up tapes containing detailed financial information on 1.2 million employees in the federal government, including many members of Congress.[7] Lexis-Nexis originally reported that it made available records from its Seisint division on 32,000 Americans to a criminal ring that exploited passwords of legitimate account holders.[8] That number was later revised to 310,000.[9] DSW, a shoe company, announced that 103 of its 175 stores had customers' credit and debit card information improperly accessed.[10] Last week, Time Warner revolved that it lost track of detailed data concerning 600,000 current and previous employees.

Legislation in this area is long overdue. Regrettably, Choicepoint and other information brokers have spent a great deal of time and money trying to block effective privacy legislation in Congress. According to disclosure forms filed with the U.S. House and Senate, obtained by the Wall Street Journal, Choicepoint and six of the country's other largest sellers of private consumer data spent at least $2.4 million last year to lobby members of Congress and a variety of federal agencies. The Journal reports that, "Choicepoint was the biggest spender, with $970,000 either paid to outside lobbyists or spent directly by the company."[11]

But the real cost for these activities is born by Americans, all across the country. This improper disclosure and use of personal information is contributing to identity theft, which is today the number one crime in the United States. According to a 2003 survey by the Federal Trade Commission, over a one-year period nearly 5% of the adult populations were victims of some form of identity theft.[12]

---

[6] Federal Trade Commission, "FTC Releases Top 10 Consumer Complaint Categories for 2004," (Feb. 1, 2005), *available at* http://www.ftc.gov/opa/2005/02/top102005.htm.

[7] Robert Lemos, "Bank of America loses a million customer records," CNet News.com, Feb. 25, 2005, *available at* http://earthlink.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html?tag=st.rc.targ_mb.

[8] Jonathan Krim and Robert O'Harrow, Jr., "LexisNexis Reports Theft of Personal Data," Washingtonpost.com, March 9, 2005, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A19982-2005Mar9?language=printer.

[9] LexisNexis Data on 310, 000 People Feared Stolen , New York Times, Apr. 12, 2005, available at http://www.nytimes.com/reuters/technology/tech-media-lexisnexis.html?.

[10] Associated Press, "Credit Information Stolen From DSW Stores," March 9, 2005, *available at* http://abcnews.go.com/Business/wireStory?id=563932&CMP=OTC-RSSFeeds0312.

[11] Evan Perez and Rick Brooks, "Data Providers Lobby to Block More Oversight," *Wall Street Journal*, March 4, 2005, at B1.

[12] Federal Trade Commission, "Identity Theft Survey Report" (Sept. 2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

Growing Dependence on the Information Broker Industry

Mr. Chairman, the representatives of the information broker industry will testify this morning that the American economy and even our national security are becoming increasingly dependent on this industry. In many respects, this is true. These companies have become the true invisible hand of the information economy. Their ability to determine the opportunities for American workers, consumers, and voters is without parallel. If a Choicepoint record says you were late on a rent payment, whether or not that's true, you may lose a chance for a new apartment or a job. If one of these companies wrongfully removes registered voters from the voting roles, those people are denied their Constitutional right to vote.

The stakes becomes even higher with homeland security. Axciom, for example, may play a central role in the identity verification procedures for Secure Flight, the new airline passenger prescreening system. According to the Wall Street Journal, a Virginia company named Eagle Force has tested sample passenger information against commercial databases supplied by Arkansas-based Acxiom Corp.[13] Acxiom is the same company that stirred controversy after it shared information about JetBlue Airways' passengers, without their knowledge, with a defense contractor in 2002.[14]

Even as we become more reliant on these firms, the reports of problems in the industry and the skyrocketing problem of identity theft have made clear that Congress must step in. There are simply no market mechanisms that protect privacy, ensure accuracy, or limit security breaches where there is no direct obligation to the person whose personal information is at risk.

EPIC's Efforts to Bring Public Attention to the Problems with Choicepoint

Well before the recent news of the Choicepoint debacle became public, EPIC had been pursuing the company and had written to the FTC to express deep concern about its business practices and its ability to flout the law. On December 16, 2004, EPIC urged the Federal Trade Commission to investigate Choicepoint and other data brokers for compliance with the Fair Credit Reporting Act (FCRA), the federal privacy law that helps insure that personal financial information is not used improperly. [15] The EPIC letter said that Choicepoint and its clients had performed an end-run around the FCRA and was

[13] "US To Require Airline Passengers' Full Names, Birth Dates," Wall Street Journal, May 4, 2005, *available at* http://online.wsj.com/article/0,BT_CO_20050504_012176,00.html

[14] EPIC pursued a complaint against JetBlue and Axcio at the Federal Trade Commission, arguing that "JetBlue Airways Corporation and Acxiom Corporation have engaged in deceptive trade practices affecting commerce by disclosing consumer personal information to Torch Concepts Inc., an information mining company with its principal place of business in Huntsville, Alabama, in violation of 15 U.S.C. § 45(a)(1)." Although the FTC chose not to take action in response to the complaint, it continues to be our position that when a company represents that it will not disclose the personal information of its customers to a third party and subsequently does so, it has engaged in an unfair and deceptive trade practice.

[15] Letter from Chris Jay Hoofnagle, Associate Director, EPIC, and Daniel J. Solove, Associate Professor, George Washington University Law School, to Federal Trade Commission, Dec. 16, 2004, *available at* http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html.

selling personal information to law enforcement agencies, private investigators, and businesses without adequate privacy protection.

Choicepoint wrote back to us to say, in effect, that there was no problem. The company claimed to comply fully with FCRA and that the question of whether FCRA, or other federal privacy laws, should apply to all of its products as simply a policy judgment. It made this claim at the same time it was spending several million dollars over the last few years to block the further expansion of the FCRA.

Mr. Chairman, hindsight may be 20-20, but it is remarkable to us that Choicepoint had the audacity to write such a letter when it already knew that state investigators had uncovered the fact that the company had sold information on American consumers to an identity theft ring. They were accusing us of inaccuracy at the same time that state and federal prosecutors knew that Choicepoint, a company that offered services for business credentialing, had exposed more than a hundred thousand Americans to a heightened risk of identity theft because it sold data to crooks.

But the problems with Choicepoint long preceded this recent episode. Thanks to Freedom of Information Act requests relentlessly pursued by EPIC's Senior Counsel Chris Hoofnagle, we have obtained over the last several yeas extraordinary documentation of Choicepoint's growing ties to federal agencies and the increasing concerns about the accuracy and legality of these products.[16] So far, EPIC has obtained FOIA documents from nine different agencies concerning Choicepoint. One document from the Department of Justice, dated December 13, 2002, discusses a "Report of Investigation and Misconduct Allegations . . . Concerning Unauthorized Disclosure of Information."[17] There are documents from the IRS that describe how the agency would mirror huge amounts of personal information on IRS computers so that Choicepoint could perform investigations.[18] Several documents describe Choicepoint's sole source contracts with such agencies as the United States Marshals Service and the FBI.[19]

Among the most significant documents obtained by EPIC were those from the Department of State, which revealed the growing conflicts between the United States and foreign governments that resulted from the efforts of Choicepoint to buy data on citizens across Latin America for use by the US federal law enforcement agencies.[20] One document lists news articles that were collected by the agency to track outrage in Mexico and other countries over the sale of personal information by Choicepoint.[21] A second document contains a cable from the American Embassy in Mexico to several different government agencies warning that a "potential firestorm may be brewing as a result of the sale of personal information by Choicepoint.[22] A third set of documents describes public

[16] *EPIC v. Dep't of Justice et al.*, No. 1:02cv0063 (D.D.C. 2002).
[17] *Available at* http://www.epic.org/privacy/choicepoint/default.html.
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*

relations strategies for the American Embassy to counter public anger surrounding the release of personal information of Latin Americans to Choicepoint.[23]

Lessons of Choicepoint

The Choicepoint incident proves many important lessons for the Congress as it considers how best to safeguard consumer privacy in the information age.

First, it should be clear now that privacy harms have real financial consequences. In considering privacy legislation in the past, Congress has often been reluctant to recognize the actual economic harm that consumers suffer when their personal information is misused, when inaccurate information leads to the loss of a loan, a job, or insurance. Consumers suffer harms both from information that is used for fraud and inaccurate information that leads to lost opportunities through no fault of the individual.

A clear example of how the company has contributed to the growing problem of identity theft may be found in Choicepoint's subscriber agreement for access to AutoTrackXP, a detailed dossier of individuals' personal information. A sample AutoTrackXP report on the ChoicePoint web site shows that it contains Social Security Numbers; driver license numbers; address history; phone numbers; property ownership and transfer records; vehicle, boat, and plane registrations; UCC filings; financial information such as bankruptcies, liens, and judgments; professional licenses; business affiliations; "other people who have used the same address of the subject," "possible licensed drivers at the subject's address," and information about the data subject's relatives and neighbors.[24] This sensitive information is available to a wide array of companies that do not need to articulate a specific need for personal information each time a report is purchased. Choicepoint's subscriber agreement shows that the company allows access to the following businesses: attorneys, law offices, investigations, banking, financial, retail, wholesale, insurance, human resources, security companies, process servers, news media, bail bonds, and if that isn't enough, Choicepoint also includes "other."

Second, it should be clear that market-based solutions fail utterly when there is no direct relationship between the consumer and the company that proposed to collect and sell information on the consumer. While we continue to believe that privacy legislation is also appropriate for routine business transactions, it should be obvious to even those that favor market-based solutions that this approach simply does not work where the consumer exercises no market control over the collection and use of their personal information. As computer security expert Bruce Schneier has noted, "ChoicePoint doesn't bear the costs of identity theft, so ChoicePoint doesn't take those costs into account when figuring out how much money to spend on data security."[25] This argues strongly for regulation of the information broker industry.

---

[23] *Id.*

[24] ChoicePoint, AutoTrackXP Report, http://www.choicepoint.com/sample_rpts/AutoTrackXP.pdf.

[25] "Schneier on Security: Choicepoint" *available at* http://www.schneier.com/blog/archives/2005/02/choicepoint.html.

Third, there are clearly problems with both the adequacy of protection under current federal law and the fact that many information products escape any kind privacy rules. Choicepoint has done a remarkable job of creating detailed profiles on American consumers that they believe are not subject to federal law. Products such as AutoTrackXP are as detailed as credit reports and have as much impact on opportunities in the marketplace for consumers as credit reports, yet Choicepoint has argued that they should not be subject to FCRA. Even their recent proposal to withdraw the sale of this information is not reassuring. They have left a significant loophole that will allow them to sell the data if they believe there is a consumer benefit. [26]

But even where legal coverage exists, there is insufficient enforcement, consumers find it difficult to exercise their rights, and the auditing is non-existent. According to EPIC's research, while Choicepoint claims to monitor their subscribers for wrongdoing, there is no public evidence that the company has referred a subscriber to authorities for violating individuals' privacy. In other words, in the case where a legitimate company obtains personal information, there is no publicly available evidence that Choicepoint has any interest in whether that information is subsequently used for illegitimate purposes.

Law enforcement, which has developed increasingly close ties to information brokers such as Choicepoint, seems to fall entirely outside of any auditing procedures. This is particularly troubling since even those reports that recommend greater law enforcement use of private sector databases for public safety recognize the importance of auditing to prevent abuse.[27]

And of course there are ongoing concerns about the broad permissible purposes under the FCRA, the use of credit header information to build detailed profiles, and the difficulty that consumers continue to face in trying to obtain free credit reports that they are entitled to under the FACTA.

Fourth, we believe this episode also demonstrates the failure of the FTC to aggressively pursue privacy protection. We have repeatedly urged the FTC to look into these matters. On some occasions, the FTC has acted. [28] But too often the Commission has ignored privacy problems that are impacting consumer privacy and producing a loss of trust and confidence in the electronic marketplace. In the late 1990s, the FTC promoted self-regulation for the information broker industry and allowed a weak set of principles promulgated as the Individual References Service Group to take the place of effective legislation. It may well be that the Choicepoint fiasco could have been avoided

---

[26] Aleksandra Todorova, "ChoicePoint to Restrict Sale of Personal Data," Smartmoney.com, March 4, 2005, *available at* http://www.smartmoney.com/bn/index.cfm?story=20050304015004.

[27] *See* Chris J. Hoofnagle, "Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," *University of North Carolina Journal of International Law & Commercial Regulation* (Summer 2004), *available at* http://ssrn.com/abstract=582302.

[28] *See* FTC's investigation into Microsoft's Passport program. Documentation *available at* http://www.epic.org/privacy/consumer/microsoft/passport.html.

if the Commission chose a different path when it considered the practices of the information broker industry.

The FTC has also failed to pursue claims that it could under section 5 of the FTC Act, which prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumer nor offset by countervailing benefits to consumers and competition.[29] It may be that the unfairness doctrine could be applied in cases where there is no direct relationship between the consumer and the company, but to date the FTC has failed to do this. [30]

Fifth, we believe the Choicepoint episode makes clear the importance of state-based approaches to privacy protection. Congress simply should not pass laws that tie the hands of state legislators and prevent the development of innovative solutions that respond to emerging privacy concerns. Many states are today seeking to establish strong notification procedures to ensure that their residents are entitled to at least the same level of protection as was provided by California.[31]

In this particular case, the California notification statute helped ensure that consumers would at least be notified that they are at risk of heightened identity theft. This idea makes so much sense that 38 attorney generals wrote to Choicepoint to say that their residents should also be notified if their personal information was wrongly disclosed. [32] Choicepoint could not object. It was an obvious solution.

Recommendations

Clearly, there is a need for Congress to act. Although Choicepoint has taken some steps to address public concerns, it continues to take the position that it is free to sell personal information on American consumers to whomever it wishes where Choicepoint, and not the consumer, believes there is a "consumer-driven benefit or transaction."[33] Moreover, the industry remains free to change its policies at some point in the future, and

---

[29] 15 U.S.C. § 45(n); Letter from Michael Pertschuk, FTC Chairman, and Paul Rand Dixon, FTC Commissioner, to Wendell H. Ford, Chairman, House Commerce Subcommittee on Commerce, Science, and Transportation (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[30] In *FTC v. Rapp*, the "Touch Tone" case, the FTC pursued private investigators engaged in "pretexting," a practice where an individual requests personal information about others under false pretenses. No. 99-WM-783 (D. Colo. 2000), 2000 U.S. Dist. LEXIS 20627. In a typical scheme, the investigator will call a bank with another's Social Security Number, claim that he has forgotten his bank balances, and requests that the information be given over the phone. The FTC alleged that this practice of the defendants, was deceptive and unfair. It was deceptive because the defendants deceived the bank in providing the personal information of another. The practice was unfair in that it occurs without the knowledge or consent of the individual, and it is unreasonably difficult to avoid being victimized by the practice.

[31] "Choicepoint Incident Prompts State Lawmakers to Offer Data Notification Bills," 10 *BNA Electronic Commerce & Law Report* 217-18 (March 9, 2005).

[32] Associated Press, "38 AGs send open letter to ChoicePoint," Feb. 18. 2005, *available at* http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-02-19-ag-letter-to-choicepoint_x.htm.

[33] "Choicepoint Halts Sale of Sensitive Information, as Agencies Launch Probes," 10 *BNA Electronic Commerce and Law Report* 219 (March 9, 2005).

the steps taken to date do not address the larger concerns across the information broker industry.

Modest proposals such as the extension of the Gramm-Leach-Bliley Act's Security Safeguards Rule are unlikely to prevent future debacles. The Safeguards Rule merely requires that financial institutions have reasonable policies and procedures to ensure the security and confidentiality of customer information. Recall that the disclosure by Choicepoint did not result from a "hack" or a "theft" but from a routine sale. Moreover, the Security Safeguards Rule will do nothing to give consumers greater control over the transfer of their personal information to third parties or to promote record accuracy.

Extending notification statutes such as the California bill would be a sensible step, but this is only a partial answer. Notification only addresses the problem once the disclosure has occurred. The goal should be to minimize the likelihood of future disclosures. It is also important to ensure that any federal notification bill is as least as good as the California state bill and leaves the states the freedom to develop stronger and more effective measures. What happens for example, when at some point in the future, we must contend with the extraordinary privacy problems that will result from the disclosure of personal information contained in a database built on biometric identifiers?

There are several proposals pending in the Senate to address the growing problem of identity theft. In particular, the Notification of Risk to Personal Data Act, S. 751, and the Comprehensive Identity Theft Prevention Act, S. 768, provide strong complimentary safeguards. The Committee should act quickly to ensure their passage.

Notification of Risk to Personal Data Act, S. 751

One of the lessons of the recent disclosures about the information broker industry is that we could not understand the scope of the problem without information about actual security breaches. Imagine trying to legislate airline safety or the reliability of medical products without even basic information about the extent of the problem or the number of people affected. That is where the information security problem was before the passage of the California notification law. That critical state law ensured, for the first time, that those whose personal information had been wrongfully disclosed would be notified of the breach and given the opportunity to take additional measures. Not surprisingly, once the problem became known, other states urged Choicepoint to provide notification to their residents. Thirty-eight state attorneys general wrote to the head of Choicepoint. Many state legislatures are now considering bills that would establish similar notification obligations.

Given this experience, Senator Feinstein's bill, the Notification of Risk to Personal Data Act, is an obvious first step in the effort to help ensure that Americans can protect themselves when security breaches occur. The bill would require federal agencies and private sector businesses that engage in interstate commerce to provide notification when personal information is acquired by unauthorized persons. The bill recognizes that

there may be delayed notification where this is necessary to aid a law enforcement investigation. The bill also provides certain exceptions for national security and law enforcement, though sensibly does not allow these exceptions to be used to hide violations of law or to protect poor administration. There are a number of alternatives for notification that recognize that there may be more efficient and less costly ways to notify individuals in certain circumstances.

While this is a good measure, we are concerned that the bill will preempt stronger state laws that may be developed to address the problem of notification where risks to personal data arise. We understand the interest in a single national standard, but this is an area where the states should retain the freedom to innovate and explore new solutions to this far-reaching problem. We urge the committee to remove Section 5 of the Act, which would preempt state law.

We also caution against any effort to limit the circumstances under which notification might occur. As a matter of fairness, it should be the individual's right to know when his or her personal information has been improperly obtained. And it should be equally obvious that given the choice businesses will choose not to provide notice unless they are required to do so.

Comprehensive Identity Theft Prevention Act, S. 768

Improved notification will play an important role in assisting consumers where security breaches occur, but clearly the long-term goal must be to reduce the risk of these disclosures and to minimize harm when these breaches occur. This is not a new problem. Congress has worked for more than thirty years to provide privacy safeguards and to protect against the risks associated with the automation of personal information. A good privacy bill works for both consumers and businesses. The Fair Credit Reporting Act, for example, was a benefit to both consumers and the credit reporting industry because it established privacy safeguards and helped ensure greater accuracy in the information that was made available to credit grantors.

The problem today is that information brokers are operating outside of any comprehensive regulatory scheme. Moreover, they have no direct relationship with the individuals whose personal information they routinely sell to others. So, there are inadequate incentives to protect privacy or to ensure accuracy. There is a clear need to establish comprehensive protections for the information broker industry.

The Comprehensive Identity Theft Prevention Act, S. 768, provides an excellent framework for privacy protection in the information broker industry. Building on the general approach of the FCRA and other privacy statutes, the bill aims to ensure that when personal information is collected, it will be used for appropriate purposes, and that when problems arise there will be meaningful remedies.

The Act requires the Federal Trade Commission to establish rules for information brokers and for the protection of personal information. The rules cover data accuracy,

confidentiality, user authentication, and detection of unauthorized use. Significantly, the Act also gives individuals the opportunity to review the information about them held by data brokers. This helps ensure accuracy and accountability and is similar to provisions currently found in the Fair Credit Reporting Act.

The Information Protection and Security Act also provides meaningful enforcement by ensuring that the states are able to pursue investigations and prosecution, after appropriate notice to the FTC and the Attorneys General. The Act also gives individuals, who of course are the ones that suffer the actual harm, to pursue a private right of action.

Additional Safeguards

Furthermore, to the extent that information brokers, such as Choicepoint, routinely sell data to law enforcement and other federal agencies, they should be subject to the federal Privacy Act. A "privatized intelligence service," as Washington Post reporter Robert O'Harrow has aptly described the company, Choicepoint should not be permitted to flout the legal rules that help ensure accuracy, accountability, and due process in the use of personal information by federal agencies. [34] It would be appropriate to consider legislation that would establish safeguard for the use of commercial information by government agencies.[35]

Also, Professor Daniel Solove and EPIC's Chris Hoofnagle have put a very good framework forward. [36] This approach is similar to other frameworks that attempt to articulate Fair Information Practices in the collection and use of personal information. But Solove and Hoofnagle make a further point that is particularly important in the context of this hearing today on Choicepoint. Increasingly, the personal information made available through public records to enable oversight of government records has been transformed into a privatized commodity that does little to further government oversight but does much to undermine the freedom of Americans. While EPIC continues to favor strong open government laws, it is clearly the case that open government interests are not served when the government compels the production of personal information, sells the information to private data vendors, who then make detailed profiles available to strangers. This is a perversion of the purpose of public records.

Looking ahead, there is a very real risk that the consequences of improper data use and data disclosure are likely to accelerate in the years ahead. One has only to look at the sharp increase in identity theft documented by the Federal Trade Commission, the extraordinary rate of data aggregation in new digital environments, and the enormous efforts of the federal government to build ever more elaborate databases to realize that the

---

[34] Robert O'Harrow, *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (Free Press 2005).

[35] *See, e.g.,* Center for American Progress, "Protecting Privacy in the Digital Age," May 4, 2005, *available at* http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=651807.

[36] Daniel Solove and Chris Jay Hoofnagle, "A Model Regime of Privacy Protection," March 8, 2005, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902.

risk to personal privacy is increasing rapidly. Congress can continue to deal with these challenges in piecemeal fashion, but it seems that the time has come to establish a formal government commission charged with the development of long-terms solutions to the threats associated with the loss of privacy. Such a commission should be established with the clear goal of making specific proposals. It should include a wide range of experts and advocates. And it should not merely be tasked with trying to develop privacy safeguards to counter many of the government new surveillance proposals. Instead, it should focus squarely on the problem of safeguarding privacy.

Congress needs to establish a comprehensive framework to ensure the right of privacy in the twenty-first century. With identity theft already the number one crime, and the recent spate of disclosures, any further delay could come at enormous cost to American consumers and the American economy.

The REAL ID Act

Finally, Mr. Chairman, I would like to say a few words about the REAL ID Act, a sweeping proposal for a new federal identification system, that may be taken up tonight as part of the supplemental appropriation for the troops in Iraq.

As you know, this bill, which was rejected in the last Congress, has gone forward in this Congress without even a hearing. It would require state agencies to collect sensitive personal information on every American citizen who drives a car. It would put the state DMVs in the position of enforcing the country's immigration laws. It would give the federal government broad authority to regulate a traditional state function. Whatever one's views may be about the merits of the legislation, it should concern all sides that this proposal could pass in the Senate without a hearing or even debate.

I make this point today in this hearing on identity theft because the state DMV record systems have actually become the target of identity thieves. In recent months, three state DMVs have been attacked by identity thieves. In March, burglars rammed a vehicle through a back wall at a DMV near Las Vegas and drove off with files, including Social Security numbers, on about 9,000 people. Recently, Florida police arrested 52 people, including 3 DMV examiners, in a scheme that sold more than 2,000 fake driver's licenses. Two weeks ago, Maryland police arrested three people, including a DMV worker, in a plot to sell about 150 fake licenses.

It is obviously the case that the establishment of new identification requirements in the United States, the dramatic expansion of the authority of the Department of Homeland Security, and the requirement that we all now deposit with state agencies the very documents that establish our proof of identity will have a profound impact on the issues under consideration today.[37]

[37] *See* EPIC, "National ID Cards and REAL ID Act," *available at* http://epic.org/privacy/id_cards/

Under any reasonable policy process, there would be an opportunity to examine these issues in more detail and to assess the risks that will surely result from the implementation of this legislation. Before there is a vote on this proposal, there should be a hearing in this Congress on this bill.[38] That power still remains with the Senate. I urge you to exercise it.

Conclusion

For many years, privacy laws came up either because of the efforts of a forward-looking Congress or the tragic experience of a few individuals. Now we are entering a new era. Privacy is no longer theoretical. It is no longer about the video records of a federal judge or the driver registry information of a young actress. Today privacy violations affect hundreds of thousands of Americans all across the country. The harm is real and the consequences are devastating.

Whatever one's view may be of the best general approach to privacy protection, there is no meaningful way that market-based solutions can protect the privacy of American consumers when consumers have no direct dealings with the companies that collect and sell their personal information. There is too much secrecy, too little accountability, and too much risk of far-reaching economic damage.

There are two important bills now before the Committee. The Notification of Risk to Personal Data Act, S. 751, would provide meaningful notice to individuals when their personal information is wrongfully disclosed. The Comprehensive Identity Theft Prevention Act, S. 768, would help reduce the likelihood of future breaches. I hope the Committee will be able to act quickly on these proposals.

I appreciate the opportunity to be here today. I will be pleased to answer your questions.

References

EPIC Choicepoint Page, available at http://www.epic.org/privacy/choicepoint/

[38] See letter from Senators Sam Brownback, R-Kan., Joe Lieberman, D-Conn., and 10 other Senators to Senate Majority Leader Bill Frist, Apr. 11, 2005 ("Because of its magnitude, this legislation should be referred to the Senate Judiciary Committee on a schedule that provides adequate time for full and careful consideration. Legislating in such a complex area without the benefit of hearings and expert testimony is a dubious exercise and one that subverts the Senate's deliberative process."), available at http://www.senate.gov/%7Egov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=953&Month=4&Year=2005