March 17, 2005

Deborah Platt Majoras
Chairman
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580

Re: Testimony on Choicepoint and Commercial Data Brokers

Dear Chairman Majoras,

We are writing on behalf of the nation's leading consumer, privacy and civil liberties organizations to express our concern that your testimony before the House Energy and Commerce Committee on commercial data broker Choicepoint was not well informed, and did not adequately reflect the concerns of American consumers about the sale of their sensitive personal information.

As the Chair of the Federal Trade Commission you have a unique responsibility to protect the interests of American consumers, not the narrow political interests of companies such as Choicepoint that are already in the midst of multiple federal and state investigations. Your ability to ensure fairness in the marketplace helps promote consumer confidence and discourages harmful business practices. Your apparent alignment with the businesses that are now the target of Congressional investigation is deeply distressing.

We noted that your position on what should be done was very much in line with the views of the companies testifying before Congress, which had leaked or sold data to criminals, but was very far from the views expressed by consumer and privacy groups.

We urge you to consider the following:

* The Federal Trade Commission may itself be responsible for growing problem of identity theft and the failure to establish adequate regulations of data brokers such as Choicepoint. In the late 1990s, Choicepoint and others formed a weak self-regulatory system, known as the Individual Reference Services Group (IRSG) Principles, that the FTC approved. That system allowed companies such as Choicepoint to sell Social Security Numbers and other information to whomever they deemed "qualified."

In retrospect, we now know that the category of "qualified" was so broad as to include criminals. The self-regulatory principles were weak in other ways. They contained no effective right to opt-out, no right to free access, no right of enforcement, and no right to correction. The IRSG dissolved shortly after the FTC endorsed the proposal.

Also in the 1990s, the FTC defined "credit report" in such a way as to create the "credit header loophole." This loophole allowed many businesses to openly traffic in Social Security Numbers with no restriction at all.

The FTC should correct these extraordinary policy blunders and urge the application and enforcement of Fair Information Practices (FIPs) to the commercial data broker industry consistent with the Fair Credit Reporting Act. These include the right of access and correction, purpose limitation, robust security, and citizen enforcement rights. This is the primary goal and must be reflected in the overall national policy and the FTC's positions.

* Your House testimony stated that "Extending the Federal Trade Commission's safeguards rule to sensitive personal information collected by data brokers is one sensible step that could be taken." While this is a necessary condition, it is not a sufficient one. The Safeguards rule applies generally to many types of companies that use information in their businesses. Companies such as information brokers, however, that primarily buy and sell personal information as their business model, should be subject to a more comprehensive and robust scheme based on Fair Information Practices. For example, Committee member Edward J. Markey has proposed the Information Security and Protection Act, HR 1080, which would require the FTC to establish regulations subjecting information brokers to requirements similar to those of the Fair Credit Reporting Act.

* In your testimony, you said, "With respect to opt in or opt out, I think it's important that we learn from the Gramm-Leach-Bliley scheme. What we have found is that, in fact, consumers have received millions, collectively, of notices of their right to opt out of a financial institution sharing their personal information and they have not exercised that right. They have not wanted to bother with that. We believe, again, they really just want to make sure that banks and merchants and others are responsibly handling their information and safeguarding it."

We believe that the exact opposite conclusion should be drawn from the problems with the Gramm-Leach-Bliley Act privacy provisions. The obvious fact is that it is difficult and time consuming for consumers to opt out under GLBA. In comparison, the Do-Not-Call list, which is easy to use and well publicized, has already secured 80 million opt outs. The previous FTC rightly pointed to the success of the Do-Not-Call Registry as a workable solution to a significant privacy concern.

Now is an excellent time to remedy the problem with GLBA by taking the initiative, as the previous FTC Chairman did, to be an advocate of consumers and create a single, easy to use opt out system akin to the Do-Not-Call Registry. In addition, of course, many consumers may choose not to opt out because after reading the notices they are frustrated with GLBA's limited privacy protections, which generally allow information sharing regardless of whether the consumer opts out or not. Our groups would also urge the FTC to support strengthening GLBA to provide for greater privacy protections than its weak notice and limited opt-out right.

* Your testimony also reflected that the FTC views the Choicepoint matter primarily as a security problem, rather than as a privacy problem. Even if Choicepoint's sale of personal information were done securely, that would not solve the problem. Choicepoint and other data brokers act as consumer reporting agencies but sell personal information to law enforcement and a variety of other businesses outside the protections of the FCRA. Choicepoint's standard subscriber agreement enumerates the types of businesses eligible for the company's reports.

They include 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."

This demonstrates that the primary issue is privacy, not security. Choicepoint allows dissemination of sensitive personal information to a broad array of businesses based on their status, not on their need for the personal information. Under the FCRA, a credit report can be pulled for a number of enumerated purposes. But under Choicepoint's regime, there is no purpose specification. Access is conditioned on one's status as an employee of a business, rather than on whether a specific purpose is articulated for obtaining the information. We think that it is this distinction that has contributed to personal information being sold to criminals. If users of Choicepoint were required to articulate a specific justification for each acquisition of personal information, auditing would be more effective, and there would be less opportunity to obtain information for illegitimate reasons.

* In your testimony, you endorsed a national notification system for security breaches that is substantially weaker than existing California law. The standard you proposed, one where individuals will only be granted notice where a "significant risk of harm" is present, is unworkable and has been rejected by all those of have worked seriously on the matter. There is no objective way to measure a "significant risk of harm," and companies that sell personal information to criminals will deny that any harm occurred, thus evading the notice requirement. This relevant information--notice that a company is irresponsible with consumer data, regardless whether harm results--is relevant to consumer decisionmaking. It is one of the only ways that consumers can tell whether their data is really protected. The California law has shed light on serious, systemic security problems in the information industry. How many of those problems would have come to light if a company could avoid notice by claiming that "no significant risk" to consumers existed?

The FTC has a long way to come on these issues to adequately represent the public interest in this matter. Although there will often be disagreements between the Commission and the consumer community, at least previous FTC Chairs have made an effort to meet frequently with consumer groups and to respond aggressively when problems have been brought to their attention.

We have attached testimony and other information on Choicepoint for your review. We again request that we meet as soon as possible to discuss Choicepoint and the FTC's consumer approach to the serious threats to privacy that this industry has caused.

Sincerely,

Marc Rotenberg
Executive Director
EPIC

Beth Givens
Director
Privacy Rights Clearinghouse

Chris Jay Hoofnagle
Director
EPIC West Coast Office

Pam Dixon
Executive Director
World Privacy Forum

Evan Hendricks
Editor
Privacy Times

Edmund Mierzwinski
Consumer Program Director
U.S. Public Interest Research Group

CC: House Commerce Committee Chairman Barton
House Commerce Committee Ranking Member Dingell
House Commerce CTCP Subcommittee Chairman Stearns
House Commerce CTCP Subcommittee Ranking Member Schakowsky
Senate Commerce Committee Chairman Stevens
Senate Commerce Committee Ranking Member Inouye
Congressional Privacy Caucus Co-Chairs Markey, Dodd, and Shelby

Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, EPIC

Hearing on

"Protecting Consumer's Data: Policy Issues Raised by Choicepoint"

Before the

Subcommittee on Commerce, Trade and Consumer Protection,
Committee on Energy and Commerce,
U.S. House of Representatives

March 15, 2005
2123 Rayburn House 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 protecting consumer's data and the policy issues raised by Choicepoint.

In my statement today, I will summarize the significance of the Choicepoint matter, discuss EPIC's efforts to bring public attention to the problem before the incident was known, suggest several lessons that can be drawn from this matter, and then make several specific recommendations.[1]

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. Whatever your views may be on the best general approach to privacy protection, Choicepoint has made clear the need to regulate the information broker industry.

The Significance of the Choicepoint Matter

With all the news reporting of the last several weeks, 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."[2] In fact, Choicepoint simply sold the information.[3] 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.[4] Investigators believe data on least 400,000 individuals may have been compromised.[5] 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

[1] Many other organizations have also played a critical role in drawing attention to the growing problem of identity theft. These include Consumers Union, the Identity Theft Resource Center, Privacy International, the Privacy Rights Clearinghouse, the Privacy Times, the US Public Interest Research Group, and the World Privacy Forum.
[2] 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.
[3] Robert O'Harrow Jr., "ID Theft Scam Hits D.C. Area Residents," Washington Post, Feb. 21, 2005, at A01.
[4] Bob Sullivan, "Data theft affects 145,000 nationwide," MSNBC, Feb. 18, 2005, *available at* http://www.msnbc.msn.com/id/6979897/.
[5] 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.

revealed that Choicepoint also sold similar information on 7,000 people to identity thieves in 2002 with losses over $1 million.[6] 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 that we are not yet aware.

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.[7] 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.[8] Lexis-Nexis made available records from its Seisint division on 32,000 Americans to a criminal ring that exploited passwords of legitimate account holders.[9] DSW, a shoe company, announced that 103 of its 175 stores had customers' credit and debit card information improperly accessed.[10]

But there are factors that set Choicepoint apart and make clear the need for legislation for the information broker industry. First, Choicepoint is the largest information broker in the United Stares. The company has amassed more than 19 billion records and has acquired a large number of smaller companies that obtain everything from criminal history records and insurance claims to DNA databases. The private sector and increasingly government rely on the data provided by Choicepoint to determine whether Americans get home loans, are hired for jobs, obtain insurance, pass background checks, and qualify for government contracts.

Choicepoint has become the true invisible hand of the information economy. Its ability to determine the opportunities for American workers, consumers, and voters is without parallel.

Second, the Choicepoint databases are notoriously inaccurate. A recent article in MSNBC, "Choicepoint files found riddled with errors," recounts the extraordinary errors

---

[6] David Colker and Joseph Menn, "ChoicePoint CEO Had Denied Any Previous Breach of Database," Los Angeles Times, March 3, 2005, at A01.

[7] 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.

[8] 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.

[9] 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.

[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.

in just one Choicepoint report that was provided to a privacy expert. [11] Among the statements in the 20-page National Comprehensive Report was an inaccurate entry that described "possible Texas criminal history" and a recommendation for a follow-up search. The report listed an ex-boyfriend's address, even though she had never lived with the fellow. As MSNBC reporter Bob Sullivan writes, "The report also listed three automobiles she never owned and three companies listed that she never owned or worked for."

The report on the document provided to Deborah Pierce is very similar to an earlier report described by another privacy expert Richard Smith, "who paid a $20 fee and received a similar report from Choicepoint several years ago. The company offers a wide variety of reports on individuals; Smith purchased a commercial version that's sold to curious consumers. Smith's dossier had the same kind of errors that Pierce reported. His file also suggested a manual search of Texas court records was required, and listed him as connected to 30 businesses that he knew nothing about."

Third, 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."[12]

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.[13]

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

[11] Bob Sullivan, "ChoicePoint files found riddled with errors Data broker offers no easy way to fix mistakes, either, " MSNBC, March 8, 2005, *available at* http://www.msnbc.msn.com/id/7118767/.

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

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

insure that personal financial information is not used improperly. [14] The EPIC letter said that Choicepoint and its clients had performed an end-run around the FCRA and was 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 fully comply 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 consumer 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.[15] So far, EPIC has obtained FOIA documents from nine different agencies concerning Choicepoint. Much of the material is available on our web site at http:www.epic.org/privacy/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." [16] 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. [17] Several documents describe Choicepoint's sole source contracts with such agencies as the United States Marshals Service and the FBI. [18]

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. [19] One document lists news articles that were collected by the agency to track outrage in Mexico

[14] 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.
[15] EPIC v. Dep't of Justice et al., No. 1:02cv0063 (CKK)(D.D.C.).
[16] *Available at* http://www.epic.org/privacy/choicepoint/default.html.
[17] *Id*.
[18] *Id*.
[19] *Available at* http://www.epic.org/privacy/choicepoint/default.html.

and other countries over the sale of personal information by Choicepoint.[20] 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.[21] A third set of documents describes public relations strategies for the American Embassy to counter public anger surrounding the release of personal information of Latin Americans to Choicepoint.[22]

Choicepoint's activities have fueled opposition to the United States overseas and raised the alarming prospect that our country condones the violation of privacy laws of other government.[23] As USA Today reported on September 1, 2003:

> After the Mexican government complained that its federal voter rolls were the source, and were likely obtained illegally by a Mexican company that sold them to Choicepoint, the suburban Atlanta company cut off access to that information.
>
> In June, ChoicePoint wiped its hard drives of Mexicans' home addresses, passport numbers and even unlisted phone numbers. The company also backed out of Costa Rica and Argentina.
>
> ChoicePoint had been collecting personal information on residents of 10 Latin American countries — apparently without their consent or knowledge — allowing three dozen U.S. agencies to use it to track and arrest suspects inside and outside the United States.[24]
>
> The revelations helped kindle privacy movements in at least six countries where the company operates. Government officials have ordered — or threatened — inquiries into the data sales, saying ChoicePoint and the U.S. government violated national sovereignty.

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

---

[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] EPIC and Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* 123-24, 182, 493 (2004) (Public Records, Argentina country report, Mexico country report)
[24] Associated Press, "Vendor sells Latin American citizen data to U.S.," Sept. 1, 2003, *available at* http://www.usatoday.com/tech/news/techpolicy/2003-09-01-choicepoint_x.htm.

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.[25] 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."[26] This argues strongly for regulation of the information broker industry.

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. [27]

---

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

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

[27] 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.

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, there is no indication that commercial data brokers audit their users and refer wrongdoers for prosecution. 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.[28]

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. While on some occasions, the FTC has acted. [29] 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 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 that 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.[30] 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. [31]

---

[28] 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.

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

[30] 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), at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[31] 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-

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.[32]

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. [33] Choicepoint could not object. It was an obvious solution.

Finally, there is still a lot we do not know about the Choicepoint company. This firm has expanded so rapidly and acquired so many companies in the last few years, it is very difficult to assess how much information it actually has on Americans. As a starting point for further work by the Committee, I would urge you and Committee Staff to obtain your own Choicepoint records in the AutoTrackXP service as well as the National Comprehensive Report. This is the information about you that Choicepoint sells to strangers. If you want to understand the serious problem of record accuracy, this is one good place to start.

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 fee to sell personal information on American consumers to whomever it wishes where Choicepoint, and not the consumer, believes there "consumer-driven benefit or transaction."[34] Moreover, the company remains free to change its policies at some point in the future, and the steps taken to date do not address the larger concerns across the information broker industry.

---

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.

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

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

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

Modest proposals such as the extension of the Gramm-Leach-Bliley Act's Security Safeguards Rule are unlikely to prevent future Choicepoint 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 disclosure. 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?

At this time, legislation such as the Information Protection and Security Act, H.R. 1080, provides a good starting point to safeguard consumer privacy and reduce the growing threat of identity theft. It would allow the FTC to develop fair information practices for data brokers; violators would be subject to civil penalties. Enforcement authority would be given to the FTC and state attorneys general. Consumers would be able to pursue a private right of action, albeit a modest one. And states would be free to develop stronger measures if they chose.

But a stronger measure would establish by statute these same authorities and impose stricter reporting requirements on the information broker industry. It would include a liquidated damages provision that sets a floor, not a limit, on damages when a violation occurs, as is found in other privacy laws. It is even conceivable that Congress could mandate that information brokers provide to consumers the same information that they propose to sell to a third party prior to the sale. This would make consent meaningful. It would promote record accuracy. And it would allow the consumer to determine for himself or herself whether in fact the transaction will provide a "consumer-driven benefit." Proposals for credit report "freeze" legislation that allow consumers to determine when it is in their benefit to release personal credit information provides a good parallel for strong legislation in the data broker field.

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. [35]

Also, a very good framework has been put forward by Professor Daniel Solove and EPIC's Chris Hoofnagle. [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, consider the extraordinary rate of data aggregation in new digital environments, as well as the enormous efforts of the federal government to build ever more elaborate databases to realize that the 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 safeguard privacy.

Congress needs to establish a comprehensive framework to safeguard 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.

Finally, Mr. Chairman, there are several practical questions left open by the Choicepoint matter. First, as we said to the FTC in December, Choicepoint has done a poor job tracking he use of personal information on American consumers that it routinely sells to strangers. Now is the time for Choicepoint to go back to its audit logs and determine what the legal basis was for selling the information that was provided to the identity theft ring. In fact, we believe that Choicepoint should be required to review all of

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

its audit logs for the past year and report to this committee on whether it has uncovered any other instance of breaches within the company. Just as heads of financial companies are now required to vouch for the accuracy of their financial statements, the heads of the information broker companies should be required to make an annual representation tot he public that they have reviewed the audit logs of their companies and are assured that the information they have disclosed has only been used for lawful purposes.

Second, there is the question of what Choicepoint intends to do with the money that it received from the sale of personal information to an identity theft ring. How can Choicepoint possibly keep the funds from those transactions? In a letter that EPIC sent to Choicepoint COO Douglas Curling, we urged the company to "disgorge the funds that you obtained from the sale of the data and make these funds available to the individuals who will suffer from identity theft as a result of this disclosure." Since Mr. Smith, the company's President is at the hearing today, perhaps he can explain what Choicepoint will do with the funds.

Third Choicepoint has still not provided to the victims of the negligent sale the same information that it disclosed to the identity thieves. At the very least, we think the company should give people the same records it sold to the crooks.

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 American 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. The Choicepoint debacle has made this clear.

The Committee may not be able to solve every privacy problem, but I urge you today to focus on the information broker industry and to pass legislation such as the Information Protection and Security Act. The information broker industry has been flying under the radar for too long.

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/

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Testimony of

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

Before The Senate Banking Committee
March 15, 2005

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

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

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

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

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

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

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

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

In my opinion, the non-credit database companies generally operate in violation of principles 2-5 as well, at least in regard to information not already covered by the FCRA. Those principles are: (2) there must be a way for an individual to find out what information about him is in a record and how it is used; (3) there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent; (4) there must be a way for an individual to correct or amend a record of identifiable information about him; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Possible Solutions

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

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

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

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

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

Current Gaps In Law, Policy & Information Systems

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

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

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

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

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

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

---

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

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

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

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

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

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

Privacy Protection Requires 'Sunshine'

The truth is that we do not know:

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

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

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

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

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

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

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

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

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

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

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

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

'Self-Regulation Already Failed'

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

ChoicePoint Wants Benefits, But Not Responsibility

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

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

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

Here are some other incidents:

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

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

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

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

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

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

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

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

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

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

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

Comprehensive Approach is Needed

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

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

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

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

Notice, Consent, Control, and Access

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

Business Access to and Use of Personal Information

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

Government Access to and Use of Personal Data

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

Privacy Innovation and Enforcement.

Effective Enforcement of Privacy Rights.

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

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony of Chris Jay Hoofnagle
Director, Electronic Privacy Information Center West Coast Office

After the Breach:
How secure and accurate is consumer information held by
ChoicePoint and other data aggregators?

Before the
California Senate Banking, Finance and Insurance Committee
Room 3191, State Capitol

Wednesday, March 16, 2005

Introduction

Chairman Speier, Vice-Chairman Cox, and Members of the Committee, thank you for extending the opportunity to testify on information aggregators. My name is Chris Hoofnagle and I am director of the Electronic Privacy Information Center's (EPIC) West Coast office. Founded in 1994, EPIC has closely tracked the development of entities we call "commercial data brokers," companies like Choicepoint, Lexis, and Acxiom that buy and sell personal information for a variety of purposes.

In June 2001, EPIC filed a series of requests under the Freedom of Information Act (FOIA) seeking access to government records regarding Choicepoint and its competitors. Four years and a lawsuit later, we have some idea about how this company operates, and how commercial data brokers pose a severe threat to privacy.

In December 2004, EPIC filed a complaint with the Federal Trade Commission, urging the agency to engage in a serious inquiry on the status of data brokers' products. EPIC believes that some of these products may be "consumer reports" for purposes of the Fair Credit Reporting Act, thus subjecting both the seller and the buyer to regulation under the Act.

Since that December filing, there have been a series of serious security breaches involving sensitive personal information in the news. Some commercial data brokers have sold personal information directly to criminals. This news has rekindled interest in creating rules for commercial data brokers to protect personal information.

In my statement today, I will begin by discussing Choicepoint and its recent data acquisitions. I will then shift to the fuel for Choicepoint's data—public records. Public records were intended to provide citizens with a window onto government, but increasingly they serve as a microscope for businesses and government to profile citizens. Next I will discuss commercial data brokers' self-regulatory rules. I will conclude with a framework of suggestions for reform of the commercial data broker industry.

The Known Extent of Choicepoint's Data Acquisition

Choicepoint became independent from Equifax, a leading U.S. credit rating agency, in 1997. ChoicePoint obtains 40,000 new public records daily to insert into its database of more than 19 billion records. Its business and government services division offers through its "AutoTrackXP" product identity verification, property records, bankruptcy records, licenses, liens, judgments, and other records to local, state and federal law enforcement,[1] including the Drug Enforcement Administration and the Federal Bureau of Investigation.[2] It also advertises the AutoTrackXP product as a solution for financial services anti-fraud and anti-money laundering compliance.[3]

Since its spinoff from Equifax, ChoicePoint has acquired a number of information collection and processing companies. These include:

- National Data Retrieval, Inc., a provider of public records information;
- List Source, Inc., d/b/a Kramer Lead Marketing Group, a marketing company in the life and health insurance and financial services markets;
- Mortgage Asset Research Institute, Inc., a mortgage fraud monitoring company; Identico Systems, LLC, a customer identity verification company;
- Templar Corporation; insuranceDecisions, Inc., an insurance industry claims administration company;
- Bridger Systems, Inc., a USA PATRIOT Act compliance company;
- CITI NETWORK, Inc. d/b/a Applicant Screening and Processing, a tenant screening company;
- TML Information Services, Inc., a provider of motor vehicle reports.
- Drug Free, Inc., a drug testing company;
- National Drug Testing, Inc., a drug testing company;
- Application Profiles, Inc., a background check company;
- Informus Corporation; a company enabling ChoicePoint to offer products online;
- Tyler-McLennon, Inc., a background screening company;
- ChoicePoint Direct Inc., formerly known as Customer Development Corporation, a database marketing company;
- EquiSearch Services, Inc.;
- DATEQ Information Network, Inc., an insurance underwriting services company;
- Washington Document Service, Inc., a court record retrieval service;
- DataTracks Technology, Inc., a public record information company;
- DataMart, Inc., a database software company; Statewide Data Services, Inc;
- NSA Resources, Inc., a drug testing company;
- DBT Online, Inc., a public record services provider;

---

[1] CHOICEPOINT, AUTOTRACKXP AND CHOICEPOINT ONLINE, http://www.choicepoint.com/industry/government/public_le_1.html (accessed Oct. 25, 2004).

[2] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595 (Summer 2004) (attached as Appendix I).

[3] CHOICEPOINT, ALL FINANCIAL SOLUTIONS, http://www.choicepoint.com/business/financial/allfinan.html (accessed Oct. 25, 2004).

- RRS Police Records Management, Inc., a provider of police reports and related services;
- VIS'N Service Corporation; Cat Data Group, LLC;
- Drug Free Consortium, a drug testing company;
- BTi Employee Screening Services, Inc., an employee pre-screening services company;
- ABI Consulting Inc., a drug screening company;
- Insurity Solutions, Inc., an insurance rating company;
- National Medical Review Offices, Inc.;
- Bode Technology Group, Inc., a DNA identification company;
- Marketing Information & Technology, Inc., a direct marketing company;
- Pinkerton's, Inc., a preemployment screening company;
- Total eData Corporation, an e-mail database company;
- L&S Report Service, Inc., a provider of police records;
- Resident Data, Inc., a residential screening services provider;
- Vital Chek Network, Inc., a provider of vital records;
- Accident Report Services, Inc., a provider of police records;
- Programming Resources Company, insurance software company;
- Professional Test Administrators, Inc., a drug testing company;
- CDB Infotek, a seller of public records;
- Medical Information Network, LLC, an online physician verification service; and
- Rapsheets.com, an online provider of criminal records data.

As you can see, it is difficult to generalize about Choicepoint. The company has personal information in many fields, and the public does not fully understand how this information is gathered, used, and sold. I would like to focus today's discussion on two aspects of Choicepoint's activities: the company's "AutoTrackXP" product, and the "VitalChek" subsidiary.

AutoTrackXP

On its website, ChoicePoint markets "AutoTrackXP", which is described as:

> AutoTrackXP and ChoicePoint Online provide Internet access to more than 17 billion current and historical records on individuals and businesses, and allow users to browse through those records instantly. With as little information as a name or Social Security number, both products cross-reference public and proprietary records including identity verification information, relatives and associates, corporate information, real property records and deed transfers. In addition, access is available to a staff of field researches who perform county, state and federal courthouse searches.[4]

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

[4] ChoicePoint, AutoTrackXP and ChoicePoint Online, http://www.choicepoint.com/industry/retail/public_cbi_1.html.

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.[5]

The AutoTrackXP report is very similar in content to a standard credit report issued by one of the "big three" credit reporting agencies. However, AutoTrackXP is not governed by the Fair Credit Reporting Act. This means that anyone with a Choicepoint account can buy an AutoTrackXP report.

AutoTrackXP is Made Available to Law Enforcement With Little Privacy Process

Federal law enforcement agencies have multi-million dollar contracts with Choicepoint to have Internet access to AutoTrackXP. This raises serious due process issues. When law enforcement requests a credit report, it has to comply with procedures designed to protect individuals. For instance, full credit report normally cannot be obtained without a court order, grand jury subpoena, or child support request. But law enforcement can obtain much of the same information from AutoTrackXP reports without engaging in any process.

The Privacy Act of 1974 was enacted, in part, because of the specter of a federal data clearinghouse, one central place where all personal information could be stored for government access. When the law was passed in 1974, Congress envisioned that only the government could have the incentive and precious computing resources to build such a data clearinghouse. Congress was wrong—the private sector has created the feared federal data clearinghouse. Our law should not allow an end-run around the protections of the FCRA and Privacy Act where the private sector can escrow troves of personal information custom-tailored for the government.

AutoTrackXP is Available to a Wide Variety of Businesses Based on Their Status, Not Need

I have attached as Appendix II the standard subscriber agreement that Choicepoint uses for its services. Notice that page one enumerates the types of businesses that are eligible for the company's services. They include 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."

This illustrates a subtle but important reason why EPIC believes AutoTrackXP should be subject to Fair Credit Reporting Act regulation. Choicepoint allows dissemination of sensitive personal information to a broad array of businesses based on the business' status, not on their need for the personal information. That is, under the FCRA, a credit report can be pulled for a number of enumerated purposes. But under Choicepoint's regime, there is no purpose specification. Access is conditioned on one's status as an employee of a business, rather than on whether a specific purpose is articulated for obtaining the information. We think that it is this distinction that has contributed to personal information being sold to criminals. If users of Choicepoint were required to articulate a specific justification for each acquisition of personal information, auditing would be more effective, and there would be less opportunity to obtain information for illegitimate reasons.

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

Choicepoint isn't the only company that makes available sensitive personal information to those who may have no legitimate need or purpose for the data. U.S. Senator Charles Schumer noted last week that Westlaw made available Social Security Numbers to Congressional staff persons who had accounts on the service. Westlaw addressed the problem by blocking staff access to the database. It is unclear how many other Westlaw subscribers have access to the same information.

Lexis-Nexis too offers personal information databases to subscribers who have no legitimate need for the data through its "person locator" databases. A law student recently e-mailed EPIC to say that SSNs were available to those who have student accounts with Lexis-Nexis. The company "protects" against SSN misuse with the following click-through warning, and no requirement that the user articulate a need for the data:

> The use of information obtained from this file is limited to use in the ordinary course and scope of the user's business or profession. The user represents and warrants that such use is for a lawful and appropriate purpose.
>
> The Fair Credit Reporting Act (15 U.S.C. sec 1681) prohibits use of information from this file to determine a consumer's eligibility for credit or insurance for personal, family or household purposes, employment or a government license or benefit.

The sources of information in this database include:

- California Secretary of State Filings
- California Secretary of State, Corporation Filings
- California Secretary of State, LTP & LLC Filings
- Orange Co., CA DBA Filings
- San Bernardino Co., CA DBA Filings
- San Diego Co., CA DBA Filings
- Santa Clara Co., CA DBA Filings
- Ventura Co., CA DBA Filings
- California Professional Licenses
- California Real Estate Licenses
- California State License Board Information

Commercial Data Brokers' Auditing Raises Serious Questions

The data leaks exposed in recent years have involved tens of thousands,[6] hundreds of thousands, or even millions[7] of records. How is it that so many records can be stolen before wrongdoing is detected?

[6] Individuals were easily able to exploit the relationship between Ford Motor Credit and Experian to obtain 30,000 credit reports. Benjamin Weiser, *Identity Ring Said to Victimize 30,000*, N.Y. TIMES, Nov. 26, 2002, p A1.
[7] Twenty million SSNs were stolen from commercial data broker Acxiom in 2003. While Acxiom claimed that its security system was extraordinary, hackers were able to download password files for all accounts on the system.

In its subscriber agreement, Choicepoint writes that the company: "will conduct periodic reviews of Subscriber activity…violations discovered in any review by [Choicepoint] will be subject to immediate action, including…referral to federal or state regulatory agencies."

Has the company ever referred subscribers to authorities? Has the company terminated accounts of subscribers suspected of wrongdoing? Just how many unauthorized accesses can occur before Choicepoint's self-policing mechanism catches wrongdoing? 10? 10,000?

Has Choicepoint ever notified individuals, before implementation of the California Security Breach Notice Law, of unauthorized access to personal information? The answer may be no. In a recent Securities and Exchange Commission filing, Choicepoint wrote that in context of the most recent breach, the company only searched its records back to July 1, 2003:

> "These numbers were determined by conducting searches of our databases that matched searches conducted by customers who we believe may have had unauthorized access to our information products on or after July 1, 2003, the effective date of the California notification law…"[8]

If Choicepoint really cares about privacy and security, why did the company only search back to the effective data of California's security breach notification law?

The public does not know the answer to any of these questions.

Choicepoint's New Stance Is Insufficient to Protect Privacy

Two weeks ago, Choicepoint announced that the company will no longer sell "sensitive consumer data" except where "there is a specific consumer-driven transaction or benefit, or where the products support federal, state or local government and criminal justice purposes."[9] We think that this concession does not fully address the risks to privacy posed by AutoTrackXP. First, Choicepoint is one of many commercial data brokers; its decision does not bind others. Second, it has articulated a subjective standard—"specific consumer driven transaction or benefit"—for sale of personal information. Under this standard, Choicepoint can decided what a consumer benefit is. In the past, Choicepoint has declared that selling personal information benefits consumers in the aggregate, and thus individuals should have no right to opt-out of Choicepoint's databases.[10] Simply put, Choicepoint's idea of what benefits consumers differs

---

DOJ, Milford Man Pleads Guilty to Hacking Intrusion and Theft of Data Cost Company $5.8 Million, Dec. 18, 2003, available at http://www.usdoj.gov/criminal/cybercrime/baasPlea.htm.

[8] Choicepoint form 8-K, Mar. 4, 2005, available at http://phx.corporate-ir.net/phoenix.zhtml?c=95293&p=irol-SECText&TEXT=aHR0cDovL2NjYm4uMTBrd2l6YXJkLmNvbS94bWwvZmlsaW5nLnhtbD9yZXBvPXRlbmsmaXBhZ2U9MzMxMzE3MiZkb2M9MCZhdHRhY2g9b24=

[9] ChoicePoint to Exit Non-FCRA, Consumer-Sensitive Data Markets; Shift Business Focus to Areas Directly Benefiting Society and Consumers, Choicepoint Press Release, Mar. 4, 2005, available at http://www.choicepoint.com/choicepoint/news.nsf/IDNumber/TXK2005-5381565?OpenDocument.

[10] The privacy statement mailed to individuals who request their AutoTrackXP report read in part: "We feel that removing information from these products would render them less useful for important business purposes, many of which ultimately benefit consumers. ChoicePoint DOES NOT DISTRIBUTE NON-PUBLIC INFORMATION (as

from what consumers and consumers advocates think benefits them. Third, Choicepoint can always change its policy to the detriment of privacy. The last decade has seen a number of companies change their privacy policies to the detriment of consumers without any objection by the Federal Trade Commission.

VitalChek

VitalChek performs "expedited delivery of over 25,000 certified vital record documents on a weekly basis…VitalChek now provides service in all 50 states as well as British Columbia, Canada." VitalChek is now owned by Choicepoint.

Serious questions are raised by this relationship. Why should this company have access to vital records in all fifty states? When one orders a vital record, does Choicepoint get a copy too? Should vital records, which contain the same information that credit card companies use to authenticate new accounts, be so easily alienated on vitalchek.com?

And while Choicepoint emphasizes how responsible the company is with personal data, on its Vitalchek site, anyone can click on "Ultimate People Finder," and buy personal information on another for $6.95.

Perverting the Purpose of Public Records

Much of the personal information in AutoTrackXP originates from public records. In a variety of contexts, the government compels individuals to reveal their personal information, and then pours it into the public record for anyone to use for any purpose. The private sector has collected the information, repackaged it, and brought it back to the government and businesses full circle.

Privacy expert Robert Ellis Smith published a list of personal information that appears in court records systems in various states.[11] The list includes medical records, Social Security numbers, victim's names, credit card and account numbers, psychiatric evaluation reports, juror's names, tax returns, payroll information, vehicle identification and driver's license numbers, and family profiles.

It is unfair to have this information systematically poured into the public record and used for any purpose by the private sector.[12]

---

defined in the Principles) TO THE GENERAL PUBLIC PURSUANT TO SECTION V(C) OF THE PRINCIPLES. The general public therefore has NO direct access to or use of NON-PUBLIC INFORMATION (as defined in the Principles) from ChoicePoint whatsoever. Letter from Gina Moore, ChoicePoint, to Chris Hoofnagle, Electronic Privacy Information Center (Feb. 21, 2003) (emphasis in original), available at http://epic.org/privacy/choicepoint/cp_nooptout.pdf.

[11] Robert Ellis Smith, Here's Why People Are Mad, Vol. 29, No. 3 Privacy J. 7, 7 (Jan. 2003) (citing Stephen Grimes, administrator of the Judicial Records Center in Rhode Island).

[12] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1084 (2002); see Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137, 1152-54 (2002) (explaining how the digitization of records has made personal information documents more accessible and less secure)

Public record policy in America was designed to protect people from government power; to provide a window into the operations of officials and thus a check on arbitrary or abusive exercise of authority. To a large extent, access to public records has served this purpose. But with electronic access and the power of aggregation, these policies have increasingly shifted to benefit the government and businesses. We need to realign these policies so that less personal information appears in the public record, while maintaining access to documents that allows for investigation and oversight of government.

Correction Rights Are Lacking

Many commercial data brokers do not extend any right of correction to individuals. They explain that since the information came from public records, the individual must correct the public record in order to amend the dossier held by the data broker. This policy does not recognize the potential for error that is inherent in commercial data brokers' information collection methods. Commercial data brokers send "stringers" to copy paper records into their databases. These stringers often copy the records by hand, and thus can make errors in transcription. There is no systematic way to test how accurate these transcriptions are.

The IRSG Principles Have Failed

The Individual Reference Services Group (IRSG) was formed in order to manage fomenting criticism regarding companies that sold personal information. The IRSG created "principles" for the sale of personal information, but dissolved shortly after passage of the Gramm-Leach-Bliley Act in 1999.

The Principles set forth a weak framework of protections, allowing companies to sell non-public personal information "without restriction" to "qualified subscribers," which include law enforcement agencies. So-called "qualified subscribers" need only state a valid purpose for obtaining the information and agree to limit redissemination of information. Under IRSG Principles, individuals can only opt-out of the sale of personal information to the "general public," but ChoicePoint does not consider its customers to be members of the general public.

The IRSG Principles have been carefully crafted in order to ensure maximum flexibility by CDBs. They have failed to set forth a reasonable degree of protection for individuals. These self-regulatory initiatives served their purpose—to stop Congress from creating real, enforceable rights while allowing privacy-invasive activities to continue.

Accordingly, recommended protections are suggested in the next section to promote privacy.

Suggestions for Reform

George Washington Law Professor Daniel J. Solove and I formulated a sixteen point strategy to address commercial databrokers. The full strategy can be accessed at http://ssrn.com/abstract=681902. I wish to present several of the approaches today.

Universal Notice

There is no general knowledge about the companies using personal information. In order to grant consent, gain access, or otherwise exercise one's rights with regard to personal information maintained by data brokers, credit reporting agencies, and other institutions, people must know about what institutions are collecting their data. Accordingly, we have suggested that any company "primarily engaged in interstate collection, maintenance, and/or sale of personally identifiable information" should register with government consumer protection authorities. Such registration information could be made available online, allowing individuals to learn of data brokers and their rights with respect to them.

Access to and Accuracy of Personal Information

ChoicePoint and other data brokers collect detailed dossiers of personal information on practically every American citizen. Most people haven't even heard of these companies. Even if they do know about these companies, people have no way of knowing what information is maintained about them, why it is being kept, to whom it is being disseminated, and how it is being used. The records maintained by these companies can have inaccuracies. This wouldn't matter much if the information were never used for anything important. But the data is being used in ways that directly affect individuals – by businesses for background checks, creditors for assessing financial reputations, the government for law enforcement purposes, and private investigators for investigation. Accordingly, we suggest that individuals should have the ability to visit a centralized source to access and correct information from data brokers at no cost.

Secure Identification

Businesses and financial institutions currently grant access to people's records when the accessor merely supplies a Social Security Number, date of birth, mother's maiden name, or other forms of personal information that is either available in public records or sold by data brokers. This makes the repositories of individuals' personal data and their accounts woefully insecure, as identity thieves can readily obtain the information needed to gain access and usurp control. Accordingly, we suggest that companies develop methods of identification which (1) are not based on publicly available personal information or data that can readily be purchased from a data broker; and (2) can be easily changed if they fall into the wrong hands. Biometric identifiers present problems because they are impossible to change, and if they fall into the wrong hands could prove devastating for victims as well as present ongoing risks to national security.

Social Security Number Use Limitation

Numerous businesses and organizations demand that a person provide a Social Security Number and then use that number as a password for access to accounts and data. Many schools and other organizations use Social Security Numbers on identification cards, thus ensuring that when a wallet is lost or stolen, one's Social Security Number is exposed. The use of Social Security Numbers is so extensive that as simple a transaction as signing up for cell phone service often requires disclosing one's Social Security Number. Accordingly, we suggest that unless

specifically authorized by statute or regulation, business and other privacy sector entities shall be barred from using Social Security Numbers for identification purposes.

Access and Use Restrictions for Public Records

Our current policy for public records was developed in a day where all information was on paper, dispersed across the country in small courthouses. Information was poorly indexed; periodically, it was destroyed by fire, improper storage, or negligence. Access was difficult enough. Aggregation was impossible. Today, massive database companies sweep up the data in public record systems and use it to construct dossiers on individuals for marketers, private investigators, and the government. This is what ChoicePoint does. These uses of public records turn the justification for public records on its head. Public records are essential for effective oversight of government activities, but commercial data brokers have perverted this principled purpose, and now public records have become a tool of businesses and the government to watch individuals.

States that allow broad access to public records are supplying troves of data to law enforcement. For instance, ChoicePoint's AutoTrackXP services include thirty-six extra databases on Florida residents and seven extra on Texans. Access to information on Florida residents is particularly broad. It includes marriage records, beverage licensees, concealed weapons permits, day care licensees, handicapped parking permits, "sweepstakes," worker compensation, medical malpractice, and salt water product licensees.

Accordingly, we suggest that access to personal information in public records shall be restricted for certain purposes. For example, accessing public records to obtain data for commercial solicitation should be prohibited. Other purposes shall be permitted: monitoring the government, research, educational purposes, tracing property ownership, and other traditional non-commercial purposes. Furthermore, state and local agencies that maintain public record systems must make substantial efforts to limit the disclosure of Social Security Numbers, phone numbers, addresses, and dates of birth.

Curbing Excessive Uses of Background Checks

Background checks are cheaper now than ever before, leading to a situation where individuals are being screened for even menial jobs. We risk altering our society to one where the individual can never escape a youthful indiscretion or a years-old arrest, even for a minor infraction. Background checks are frequently being used by employers even for jobs that do not involve security-related functions, the handling of large sums of money, or the supervision of children or the elderly. Accordingly, we suggest that background checks should only be performed in contexts where fiduciary relationships are involved, where a large amount of money is handled, where employment involves care taking, or any of the jobs enumerated by the Employee Privacy Protection Act, 29 U.S.C. § 2007. Whether background checks are performed by employers or by companies hired to do the screening, the employee or prospective employee shall receive a copy of the actual investigation.

Limiting Government Access to Business and Financial Records

Increasingly, the government is gathering personal information from businesses and financial institutions. Companies such as ChoicePoint have multi-million dollar contracts with government agencies to supply them with personal information. The Fourth Amendment is often inapplicable because in a series of cases, including *United States v. Miller*, 425 US 435 (1976) and *Smith v. Maryland*, 442 US 735 (1979), the Court has held that whenever a third party possesses personal information, there is no reasonable expectation of privacy. In the Information Age, it is impossible to live without extensive information about one's life existing in the hands of various third parties: phone companies, cable companies, Internet Service Providers, merchants, booksellers, employers, landlords, and so on. Thus, the government can increasingly obtain detailed information about a person without ever entering her home. Accordingly, we recommend that whenever the government attempts to access personal information from third parties that maintain record systems of personal information (databases or other records of personally identifiable information on more than one individual), the government should be required to obtain a special court order that requires probable cause and particularized suspicion that the information sought involves evidence of a crime. Exceptions should exist for reasonable law enforcement needs, including emergency circumstances.

Finally, I wish to note that the Solove/Hoofnagle approach would preserve the rights of the states to continue to innovate new protections for privacy.

Conclusion

Thank you for holding this hearing on information aggregators. We have long suspected, and recent events now have confirmed, that commercial data brokers present a serious risk to privacy that needs to be addressed by robust privacy law. We look forward to continuing to working with the Committee to provide information on this topic and other privacy issues.