

The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information

Paul N. Otto, Annie I. Antón, David L. Baumer

The Privacy Place
North Carolina State University
Raleigh, NC 27695-8207, USA
{ pnotto | aianton | david_baumer }@ncsu.edu

Affiliations

Paul N. Otto is a PhD student in the computer science department at North Carolina State University, where he is a member of The Privacy Place (<http://theprivacyplace.org>). His research interests include software requirements engineering, security and privacy requirements, policy specification, and legal compliance. He has a BS in computer engineering from the University of Virginia. He is a student member of the ACM, the IEEE, and the International Association of Privacy Professionals (IAPP). Contact him at pnotto@ncsu.edu.

Annie I. Antón is an associate professor in the North Carolina State University College of Engineering, where she is a Cyber Defense Lab member and director of The Privacy Place. Her research interests include software requirements engineering, information privacy and security policy, software evolution, and process improvement. She has a BS, an MS, and a PhD in computer science from the Georgia Institute of Technology. She is a member of the ACM, the IAPP, and a senior member of the IEEE. Contact her at aianton@ncsu.edu.

David L. Baumer is a professor in the North Carolina State University College of Management, where he is a member of The Privacy Place and director of the NCSU Cyberlaw Initiative. He is the author of *Cyberlaw and E-Commerce and Environment of Business in the Information Age* (McGraw-Hill, 2002 and 2004). He has a JD from the University of Miami and a PhD in economics from the University of Virginia. Contact him at david_baumer@ncsu.edu.

Keywords

information security, data privacy, data brokers, ChoicePoint

Abstract

In 2005, there was a significant increase in the number of security and privacy breaches disclosed to the public. Leading the charge was ChoicePoint, a data broker that suffered fraudulent access to its vast databases of personal information. ChoicePoint and other data brokers exist in a largely unregulated environment, in which there appears to be little concern for the security and privacy of the personal information they store on virtually every U.S. citizen. In this paper we examine the details of ChoicePoint's data breach. Our analysis explores what went wrong from the perspective of consumers and executives as well as policy and IT systems. Based on our study, we provide seven specific recommendations for information traders and system designers, and discuss what consumers can do to manage the risk of identity theft.

Introduction

Over the past twenty years, a new industry has emerged based on gathering, processing and selling personal information. Sellers in this market – often called data brokers – have assembled dossiers on virtually every adult in the United States, culling data from three major categories: public records, publicly-available information, and non-public information. Ironically, much of the demand for the informational products supplied by data brokers comes from agencies in executive branches of government, both at the local and national levels. Laws enacted to protect consumer privacy have sometimes hampered investigations by law enforcement and the government. Increasingly government agencies have turned to data brokers for consumer information. There are thousands of data brokers, large and small, operating in the United States today. These data brokers exist in a largely unregulated market space and thus structure their operations to avoid privacy protection laws that restrict information gathering and sharing by government agencies and credit bureaus.¹

In 2005, there was a significant increase in the disclosure of data breaches, with over 150 breaches exposing over 57 million records containing personal information to unauthorized access.² The first major incident announced in 2005 was the fraud committed against ChoicePoint, a commercial data broker based in the United States [MSN05]. At the time, much of the general public was not familiar with the data broker industry, nor had it paid much attention to the risk posed by data breaches. The massive data security breach at ChoicePoint seems to be a tipping point. Ever since the ChoicePoint news, the data broker industry as well as the privacy and security of personally identifiable information (PII) have been subject to increasing public and congressional attention.

In addition to data brokers, data breaches have been reported by a number of entities with more benign reputations, including universities, financial institutions, large retailers, and government agencies. These announcements have given rise to confusion among citizens and consumers who are concerned about protecting their personal information. With thousands of companies gathering, buying, and selling information, even vigilant consumers have little control over their personal data. Unfortunately, every registration, employment, or appointment is a new opportunity for personal information to reach data brokers and identity thieves alike. Statistically, only a small percentage of identity theft victims have resulted from data breaches³, but there is increased risk from each and every record containing PII that is lost, stolen, and exposed.

The problem of identity theft is a growing epidemic in the new millennium. The Federal Trade Commission (FTC) received 255,565 consumer complaints of identity theft in 2005; identity theft was the biggest consumer concern for the sixth straight year [FTC06]. The FTC estimates that over 27 million people were identity theft victims between 2000 and 2004, with nearly 10 million in 2004 alone. The cost of identity theft is largely borne by the victims. In reclaiming his or her identity, the average victim spends 330 hours and loses more than \$4,000 in income [ITRC04].

This paper focuses on a ChoicePoint data breach that received wide publicity and was the subject of legal action by the Federal Trade Commission. Using this data breach for illustrative purposes, we examine the privacy risks inherent in the buying and selling of personal information. Although a complete explication of the facts has not occurred, the main facts are not in dispute. Our work is based upon information obtained from various public sources, coupled with published reports that are assumed to be accurate. The following analysis is derived from our examination of these materials. We reference official ChoicePoint press releases and company statements directly, whereas other facts are verified in at least two sources.

¹ See testimony of Chris Hoofnagle, West Coast Director of EPIC, located at: <http://epic.org/privacy/choicepoint/>.

² The Privacy Rights Clearinghouse maintains a list of announced data breaches at <http://privacyrights.org/ar/ChronDataBreaches.htm>.

³ The Javelin 2006 Identity Fraud Survey Report found that out of the 47% of identity theft victims surveyed who knew how their personal information was obtained, 6% faulted data breaches; see <http://bbb.org/Alerts/article.asp?ID=651>.

In this article, we provide some background on ChoicePoint, including the information flows and policies in place before the data breach became public, review the details of the fraud and its ensuing fallout, and provide an analysis of ChoicePoint’s policies. We then discuss the lessons learned from the data breach, review consumers’ rights and legislation, and end with our recommendations to data brokers and other companies trading in personal information.

The Business of Information Sharing

In 1997, the credit agency Equifax spun off their underperforming insurance information division as ChoicePoint Inc. Reportedly, the split was also intended to help the business avoid laws that restrict how credit agencies sell information; as a data broker, instead of a financial services company, ChoicePoint would not be subject to such laws. In the company’s capacity as a consumer reporting agency, however, ChoicePoint’s transactions remain highly regulated.⁴ Since the spin-off, ChoicePoint has made at least 60 acquisitions and grown to having hundreds of thousands of customers, while employing approximately 5,500 employees. ChoicePoint’s original focus was on providing credit data to insurance underwriters. The company now sells data to over 50% of the top 1,000 U.S. companies and has the largest background screening business in the United States. ChoicePoint’s customers depend on the company for many business-critical tasks, “ranging from employee screening, homeland security compliance and mortgage processing to home, auto and commercial insurance policy underwriting” [Gar06]. Table 1 presents a complete breakdown of ChoicePoint’s customers by revenue:

Customer	% of total revenue, 2005	Revenue in millions of dollars
Insurers	38.5%	\$407.5
Business services	35.9%	\$380.2
Government services	14.0%	\$148.2
Marketing services	8.6%	\$91.5
Other	2.9%	\$30.5

Table 1: Breakdown of ChoicePoint’s Customers by Revenue (2005)

ChoicePoint has accumulated over 19 billion public records, equaling over 250 terabytes of data in its databases [Har05]. This manuscript, building upon efforts such as [WP05a], presents a comprehensive list of the information available from ChoicePoint on any given individual, as well as the various recipients of that information. Figure 1 provides a visual overview of where ChoicePoint acquires information, the information gathered, the groups receiving data from ChoicePoint, and the purpose of data purchases:

⁴ The Fair Credit Reporting Act strictly limits the recipients of credit bureau data. See Section 604 Permissible Purposes of Consumer Reports [15 U.S.C. § 1681b].

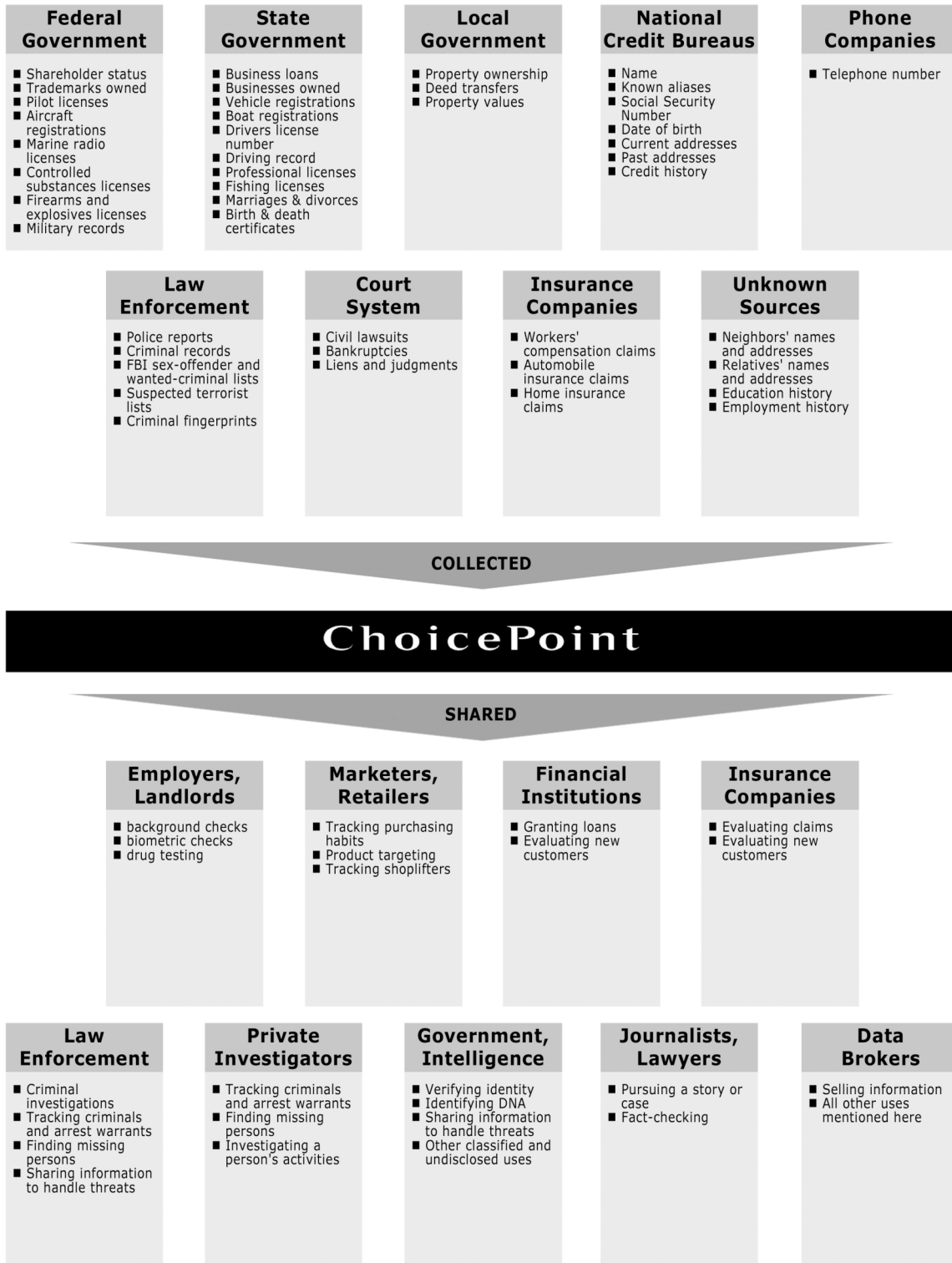


Figure 1: The Information Flow Model of ChoicePoint's Operations. The rounded boxes below the center ChoicePoint rectangle represent data leaving ChoicePoint, while the rectangles above ChoicePoint's name reflect sources of data entering the company.

The ChoicePoint Case

On February 14, 2005, MSNBC.com reported that fraudulent parties (hereinafter “fraudsters”) posing as legitimate businesses accessed ChoicePoint’s databases and that up to 35,000 Californians may have been affected [MSN05]. Within a week, it was clear that the ChoicePoint data breaches affected consumers nationwide. By the end of 2005, ChoicePoint had notified roughly 163,000 victims that their personal information had been fraudulently accessed.

The fraud against ChoicePoint actually began before September 2003, when fraudsters acquired fake business licenses, posing as check-cashing companies and debt-collection firms [AP05b]. The business licenses were obtained by using previously stolen identities to provide the names, SSNs, phone numbers and addresses of real people. The fraudsters then faxed copies of their business licenses and applications, seeking to set up access accounts. When ChoicePoint performed routine background checks on the (stolen) identities, they discovered no criminal records, thus enabling the fraudsters to escape detection. The fraudsters set up 50 accounts in this fashion, acquiring access codes and passwords for each new account. In total, the fraudsters performed around 17,000 searches of ChoicePoint’s databases. Criminal investigators discovered over 800 instances of identity theft in which the stolen information was used to access personal information stored by ChoicePoint. According to ChoicePoint, these security breaches eventually cost the company \$27.3 million in 2005 alone to cover legal fees, notify victims, and seek audits [Gar06].

The Role of the Security Breach Information Act

The California Security Breach Information Act was instrumental in exposing the ChoicePoint data breach to authorities and the public. This law requires any organization doing business in California to disclose data breaches to California residents when unauthorized access to unencrypted personal information occurs.⁵ In testimony before the U.S. Congress, a ChoicePoint executive admitted that without this law, it is possible that consumers would not have been informed about the data breach [WP05c]. The fact that ChoicePoint initially limited its fraud investigation to transactions occurring on or after the California law took effect further illustrates the impact of the California Act.

SEC and FTC Investigations

Formal disclosure of the ChoicePoint security breach occurred on March 4, 2005, when ChoicePoint filed a Form 8-K – required whenever a firm that is subject to SEC regulation is the target of a government lawsuit – with the SEC, which disclosed that two government agencies were investigating the company. By that time, the FTC had begun an investigation into ChoicePoint’s compliance with security and privacy laws, requesting that the company provide information and documents detailing the fraud and its credentialing process. The SEC launched an inquiry into the fraud, as well as stock trading by ChoicePoint executives.

The FTC concluded its investigation in 2006 by announcing a landmark \$15 million settlement with ChoicePoint, which consisted of a \$10 million civil penalty – the largest assessed in FTC history – and the creation of a \$5 million fund for compensating identity theft victims.⁶ The FTC claimed that ChoicePoint violated the terms of the Fair Credit Reporting Act (FCRA) in sharing personal credit data with unauthorized users and misled customers in its privacy statements claiming its database was secure.⁷ ChoicePoint did not admit any wrongdoing as part of the settlement, but agreed to implement new security and access procedures and to fund a third-party security audit every two years for the next twenty years.

The SEC’s inquiry into ChoicePoint largely focuses on whether ChoicePoint executives violated the securities laws by engaging in insider trading. ChoicePoint’s board approved the sale of

⁵ California Civil Code § 1789.29a

⁶ The full text of the FTC complaint and settlement (a “Stipulated Final Judgment and Order”) is at <http://ftc.gov/os/caselist/choicepoint/choicepoint.htm>

⁷ The FTC has authority to enforce the Fair Credit Reporting Act 15 U.S.C. §§ 1681-1681x and the Federal Trade Commission Act, 15 U.S.C. § 45(a), which prohibits unfair and deceptive trade practices.

stock by the company president and CEO a day before the arrest of the main fraud suspect and one month after ChoicePoint first discovered the fraud was taking place. Most likely such information, if known to the public, would have affected the price of ChoicePoint's stock. The top two ChoicePoint executives earned upwards of \$17 million through their stock sales. The focus of the SEC inquiry is whether ChoicePoint's top executives used the knowledge of the breach and impending disclosure to profit by selling stock in advance. The SEC investigation is still ongoing, and no results have been released to date.⁸

Lawsuits

The data breach also spawned several lawsuits by private citizens against ChoicePoint, both from consumers and shareholders. The first lawsuit was filed within a week of the data breach becoming public, claiming ChoicePoint was both fraudulent and negligent in its handling of the breach and employed unfair business practices.⁹ Another lawsuit filed within a month of ChoicePoint's public disclosure alleges that the company violated the FCRA and various privacy rights in disclosing personal information.¹⁰ This lawsuit seeks the right for individuals to exclude themselves from ChoicePoint's databases. More consumer lawsuits were filed in the first half of 2005; several of these lawsuits were consolidated into a single class-action suit.¹¹

The consumer lawsuits seek to represent all 163,000 individuals who were notified by ChoicePoint, rather than only the 800 identity theft victims. In the past, lawsuits that allege harm in the form of increased risk of identity theft due to the defendant's negligence, without a showing of an actual occurrence of identity theft, have failed.¹² These cases were brought to establish a new precedent, namely, that plaintiffs are entitled to a monetary remedy when they are subjected to the risk of identity theft rather than having to show actual damages due to identity theft.

ChoicePoint also faces class-action lawsuits brought by shareholders alleging foul play and claiming harm from the five-month delay between company officials learning of the data breach and releasing this information to the public. The fate of these lawsuits likely hinges on the outcome of the SEC investigation into the potential insider trading.¹³

ChoicePoint's Evolving Policies

Given our experience in analyzing over 100 Internet privacy policy documents at ThePrivacyPlace.Org, we decided to examine ChoicePoint's existing policies before the data breach became public. We know that ChoicePoint's policies proved to be insufficient or flawed in thwarting fraud against the company, as the fraudsters were able to evade detection for over a year. As a starting point, we focus on the ways ChoicePoint customers established identities in order to access the databases prior to the breach.

Before gaining access to the ChoicePoint databases, potential customers were required to establish identity and the reason for seeking access. ChoicePoint accepted business licenses via fax as well as by mail. Once the business license was in ChoicePoint's possession, the company then verified the license by checking facts such as the principals on the business license or the provided phone numbers and web sites. ChoicePoint used its own credentialing services – products touted to its customers as crucial identity verification procedures – to establish the identity of new customers.

Once a new customer was verified, the customer received a username/password combination with which to access the database. According to court papers filed by the FTC, customer search histories were not stored, nor were the results archived or all accesses logged. A company

⁸ Under Section 10(b) of the 1934 Securities Act it is illegal for company executives to trade company stock while in possession of material insider information not available to the public. 15 U.S.C. § 78a et seq.

⁹ *Goldberg v. ChoicePoint, Inc.*, C.D. Cal., CV05-2016J

¹⁰ *Salladay v. ChoicePoint, Inc.*, C.D. Cal., CV05-1683

¹¹ *Harrington, et al. v. ChoicePoint*, C.D. Cal., CV05-1294

¹² See, for example, *Huggins v. Citibank, N.A., et al*, 355 S.C. 329

¹³ *In re ChoicePoint Inc. Securities Litigation*, U.S. District Court, Northern District of Georgia, CV05-686, and *In re ChoicePoint Inc. Derivative Litigation*, Superior Court of Fulton County, Georgia, CV05-103219

spokesperson stated after the data breach that ChoicePoint “has no way of knowing whether anyone’s personal information actually has been accessed” [MSN05].

Before news of the data breach broke in 2005, the effect of ChoicePoint’s policies were that once a customer established an identity with the company, that individual or business enjoyed largely unsupervised and unfettered access to the wealth of information inside ChoicePoint’s databases. The major hurdle appears to have been the initial identity verification, which was easily bypassed using stolen identities.

Policy Changes after the Data Breach

ChoicePoint made numerous changes in its policies and procedures since the 2005 data breach.¹⁴ The company’s initial reaction upon discovering the data breach was to close all 50 suspicious accounts. ChoicePoint also stopped accepting faxed versions of business licenses. Furthermore, the company increased its verification procedures for establishing customer identity and announced that any non-governmental, privately-held business would have to be re-credentialed to maintain access to its databases.

ChoicePoint announced several new policies coinciding with its 2005 SEC Form 8-K filing and disclosure report. The key announcement was an explanation of the conditions under which personal information would be sold; these conditions can be characterized as either government requests or consumer-based transactions, such as verifying employment history or home address. ChoicePoint also began masking part of the SSN and driver’s license number for many of its customers. Some small-business customers were completely cut off from ChoicePoint’s databases. Private investigators, debt collectors, and check-cashing companies, among others, found their access to personal information severely curtailed or cut off by the end of 2005.

The policies on credentialing changed for both new and existing customers. Existing customers faced increased on-site visits and auditing to verify authenticity, but all new business customers now go through an on-site visit before receiving any access. Midway through 2005, ChoicePoint announced that it had already turned away over 200 new customers after enacting its more stringent policies. The company also added new, more rigorous requirements for access codes, passwords, and account deactivation.

Although the aforementioned policy focused on specific customers and business segments, ChoicePoint also enacted a major structural change. Within a month of the data breach becoming public, the company announced the creation of an Office of Credentialing, Compliance and Privacy that would monitor ChoicePoint’s activities and report directly to the Board of Directors. The new office tackled several policy changes in 2005, including expanding on-site visits, establishing policies for compliance with privacy laws and regulations, improving screening for prospective ChoicePoint employees, and working on a new policy for notifying consumers in any future data breaches.

ChoicePoint also mobilized to correct many of its early mistakes. It established a web site dedicated to privacy issues at ChoicePoint and created an independent office to handle privacy matters.¹⁵ Additionally, ChoicePoint pledged to offer all victims one year of free credit monitoring services. The company also continued investigating its databases for further signs of fraud even months after the data breach was made public.

ChoicePoint brought in outside help to evaluate its business and privacy practices. The company engaged in several SAS 70 audits to evaluate ChoicePoint’s data management practices and underwent a total of 43 third-party audits in 2005, while expecting to complete upwards of 30 audits in 2006 [Gar06]. In addition, ChoicePoint hired Ernst & Young to review and improve the company’s practices regarding privacy, credentialing, and compliance.

ChoicePoint’s Online Privacy Policies

¹⁴ ChoicePoint maintains a list of its major changes in a “Privacy Enhancements Fact Sheet” at <http://www.privacyatchoicepoint.com/common/pdfs/CPPrivacyFactSheet.pdf>. Virtually all of these changes were mandated by the consent decree ChoicePoint agreed to with the FTC in lieu of further court action.

¹⁵ ChoicePoint’s new privacy-focused website is at <http://www.privacyatchoicepoint.com>

To better understand ChoicePoint's privacy practices, we employed a content analysis technique, goal-mining (the extraction of goals from text artifacts) [AE04], to analyze ChoicePoint's online privacy policies. We downloaded recent versions from ChoicePoint's web site and accessed older versions dating back to 2000 via the Internet Archive.¹⁶ The extracted goals were gleaned using a web-based Privacy Goal Management Tool (PGMT) developed at North Carolina State University (NCSU). We also analyzed the evolution of the privacy policy over the past six years to examine how ChoicePoint's privacy practices have changed over time.

We extracted a total of 53 unique taxonomy goals from the most recent privacy policy, with four of those goals repeated twice within the document. Previous research has established a goals taxonomy, distinguishing privacy protection goals from vulnerabilities [AE04]. Our application of PGMT criteria to ChoicePoint's current privacy policy yielded 19 vulnerabilities and 34 privacy protection goals. The protection goals largely focused on notice/awareness and enforcement/redress whereas the vulnerabilities largely involved information monitoring, collection and transfer practices.

In using the PGMT, we found that ChoicePoint's online privacy policies have not changed significantly since the fraud began in 2003. Taking the online policies as a reflection of ChoicePoint's overall privacy practices, the company focuses much of its attention on information monitoring, collection and transfer, which seems to reflect its goals as a data broker. The promised protections largely emphasize enforcement policies, should violations occur, as well as notice and awareness of how the privacy policy will be maintained. Overall, the policy fails to provide consumers with information on how ChoicePoint will manage and safeguard the data that is being collected and sold, both online and offline. The privacy policy has consistently focused on the information buyers, rather than the consumers whose information is being traded.

Discussion

Legal Landscape

Before 2003, there was little incentive for companies to report data breaches to the public. Given recent trends in legislation and public accountability, undisclosed breaches are increasingly a substantial legal risk [MBT05]. However, there is still no single federal statute comprehensively regulating data privacy issues; several federal, state, and local groups currently have overlapping jurisdiction, and cooperation among various government agencies is largely ad hoc. After the ChoicePoint data breach, legislators and regulators expressed dismay with the lack of rules governing the data broker industry. By the end of 2005, over a dozen bills had been drawn up and brought before various committees in Congress. Although no bill passed in 2005 or 2006, the continuing revelation of negligent storage and handling of PII augurs in favor of passage of federal regulation governing data security in 2007. However, data brokers are a powerful special interest with allies among law enforcement and financial institutions. Whether a comprehensive data privacy law will be enacted at the federal level remains highly uncertain. ChoicePoint, for its part, has publicly offered support for some form of legislation governing data brokers.

Some individual states have been much quicker in responding to the identity theft threat to their citizens. At the start of 2005, only two states had security freeze laws in effect, and another two states had laws coming into effect that year. By the end of 2005, 12 states had security freeze legislation on the books. At the time of the ChoicePoint breach, only California had a statute that required notification to consumers in the event of unauthorized accesses to personal information. However, by September 2006, 33 additional states had passed legislation similar to California's disclosure law; some states, such as New York, enacted even tougher measures to enforce notification.

Consumer Rights and Responsibilities

¹⁶ ChoicePoint's privacy policy is available at <http://choicepoint.com/privacy> and the Internet Archive's Wayback Machine is available at <http://archive.org>

Although many states have already passed notification laws, and federal legislation is under consideration, data brokers entered 2007 essentially as unregulated as they were in 2005. Unregulated, data brokers generally chose to exclude consumers from every aspect of their operations, leaving them little access or control over their own personal information. Except for medical or financial information, data brokers are not required to obtain permission of their data subjects in the U.S. before collecting, processing, and transmitting information. The default rule for information sharing in the United States is that of opt-out, rather than opt-in. Typically, data brokers have no business relationship or interactions with the individual whose information is being traded. Unless the consumer actively seeks to prevent the sharing of his or her PII or threatens to create adverse publicity, companies are free to do almost anything with the data they collect. Furthermore, there is no way for individual consumers to prevent the kind of data breach that occurred at ChoicePoint. In general, the only legal protection individuals have is provided by government suits such as the action filed by the FTC against ChoicePoint. The net result is that consumers must be vigilant and watch for signs of identity theft.

Consumers do, however, have the right to see much of their financial information, whether the transaction was with or without their consent, as a result of new changes to the FCRA. Consumers nationwide are entitled to a free copy of their credit reports from each of the three credit bureaus once per year [PRC05]. Careful monitoring enables the consumer to detect identity theft sooner rather than later.

Existing and proposed extensions to consumer rights in managing their credit reports may better safeguard individuals against the harms of identity theft. The Fair and Accurate Credit Transaction Act (FACTA) permits consumers to file a 90-day fraud alert with the credit bureaus for free.¹⁷ This alert is intended to stave off fraudulent requests for credit, when a consumer knows that an identity thief might strike. Several states are considering extending this privilege into the right to freeze a credit file. A credit freeze would prevent any creditors from issuing credit for that consumer until the file is 'thawed', allowing the consumer to better control the use of his or her credit.¹⁸

There are many dossiers on consumers beyond credit reports, but individuals' rights to access these dossiers vary based on the information type and provider. If a prospective employer, landlord, or insurer uses a data broker's report to screen a consumer, that consumer has the right to a free copy. Information is available online for consumers about how to obtain free copies of certain reports created by ChoicePoint and other data brokers [PRC05]. ChoicePoint now offers free annual copies of its personal public records searches to consumers, even though no law currently requires such access.¹⁹

In the past, ChoicePoint stated that it cannot correct errors in its records, but that consumers must locate the original source from which ChoicePoint is gathering the information and correct any mistakes there. In contrast, the right to access and correct erroneous financial information has been a part of the FCRA since its passage in 1970. Preliminary research discovered a high error rate in ChoicePoint's records on individuals: all eleven reports received as part of the study contained at least one error, with eight of the eleven containing errors in basic biographical information [PA05]. Recently, ChoicePoint has announced plans to give individuals a way to review and correct their personal information via a single point of access. According to a ChoicePoint spokeswoman, this new system would give consumers the "right to access, right to question the accuracy and prompt a review, and right to comment if a negative record is found to be accurate" [AJC05d]. Although announced soon after the data breach became public, the new system is not yet available to consumers.

In the current, largely unregulated market for personal information, individuals must assume certain responsibilities to protect themselves from information leakage and identity theft. The FTC

¹⁷ (Pub. L. 108-159, 111 Stat. 1952)

¹⁸ There are other variations of credit freezes; see http://consumersunion.org/pub/core_financial_services/001872.html

¹⁹ ChoicePoint provides this service at <http://choicetrust.com>

maintains a consumer web site detailing what consumers should do to minimize their risk.²⁰ One such responsibility is to check one's credit reports regularly for any errors or signs of unauthorized activity. Consumers must also be diligent in attempting to opt out of any undesired personal information sharing. The Privacy Rights Clearinghouse maintains a list of online data brokers that offer some sort of opt-out opportunity.²¹ Consumers can also contact each company with which they have a relationship to request opting out of information transfers, although there are no binding legal requirements that companies will respect such wishes.

Despite the lack of an ownership right to personal information in the United States, consumers deserve access to see what information companies have about them. Data brokers, as well as all other companies collecting and selling personal information, should inform the affected consumers and provide mechanisms for correcting errors. By allowing consumers such access, companies will strengthen goodwill and trust in their operations and will provide consumers a low-cost means of eliminating harmful errors from their records.

Recommendations

We conducted the preceding investigation by making use of publicly available material to provide a holistic analysis of the ChoicePoint 2005 data breach. We conclude with several recommendations for all companies trading in personal information. Note that ChoicePoint has already addressed the first four recommendations in dealing with its 2005 data breach.

Companies must have a plan of action in place for dealing with data breaches.

ChoicePoint had to quickly devise a plan of action for dealing with the data breach and the media, as the company had only two weeks to strategize before the breach became public [AJC05a]. The lack of a plan or the infrastructure to handle a data breach created problems in disseminating information and handling public relations. Given that ChoicePoint has suffered similar data breaches in the past, the company should have had a plan of action ready to address the media and the public. A clear sign of this lack of preparation was evidenced in the original notification letter, signed "J Michael de Janes, Chief Privacy Officer".²² This was apparently the first and last use of this title for de Janes; it appears as though the company realized their lack of a privacy chief and thus created the position on the spot [CSO05].

The CEO's lack of early knowledge about the data breach gives rise to further concern. ChoicePoint's vice president testified in the Senate that he was the first executive to learn of the data breach, finding out in mid-November; he then told the president in late November [LA05]. The CEO separately confirmed in an interview that he did not know about the fraud until late December at the earliest [AJC05c]. ChoicePoint's failure to share business-critical information throughout the chain of command highlights a weakness in dealing with such fraud situations. To ChoicePoint's credit, the CEO has stated that, in the future, he will be informed of any and all investigations from the beginning.

Given the increasing prevalence of data breaches since early 2005, companies handling sensitive data must realize the risks and plan accordingly [MBT05]. Companies should have detailed plans for how the company will respond. Companies should also have key personnel, such as Chief Privacy Officers, Chief Security Officers, and Chief Information Security Officers, active and involved with the planning process. The comprehensive strategy should include a plan for notifying the public in the case of such a data breach, which directly leads into the next recommendation.

Companies should provide prompt, straightforward and accurate notification of data breaches.

During the data breach news coverage, ChoicePoint was plagued by inconsistencies between the facts and what spokespeople — including the CEO — told the public. The first inconsistency

²⁰ See <http://www.consumer.gov/idtheft>

²¹ This list, along with information on how to opt out, is available at <http://privacyrights.org/ar/infobrokers.htm>

²² The letter is available at http://csoonline.com/read/050105/choicepoint_letter.html

involved whether only Californians were affected by the data breach. When the data breach first hit the news (5 months after the breach was first discovered), a spokesman said ChoicePoint did not “have any evidence at this point that the situation has spread beyond California” [AP05a]. Another spokesman said ChoicePoint learned that non-California residents were at risk two days after the data breach became public, and ChoicePoint publicly acknowledged the nationwide risk the day after the company became aware of the nationwide impact [WP05b]. The media and security experts were openly skeptical of the notion that the breach would be limited by geography, and the media reflected a firm belief in ChoicePoint belatedly admitting to the nationwide scope [AP05c]. Given that ChoicePoint was able to announce so quickly that another 110,000 people were at risk and would be receiving notification letters, it seems unlikely that the company generated that list a mere day after first discovering non-California victims.

Another major inconsistency involved ChoicePoint’s claim that this data breach was the first of its kind for the company [AP05d]. Within three weeks of the first news, however, the media exposed a previous data breach that ChoicePoint suffered in 2002 [AP05d]. The company later admitted that it had in fact suffered similar attacks in the past, contradicting what spokespeople and the CEO had publicly stated.

Following ChoicePoint’s disclosure, many companies have realized the need to alert the public of data breaches promptly, before the news media breaks the story first. In the ChoicePoint situation, inconsistencies in the statements of spokespeople and even the CEO led to increased distrust and ill will. Companies that fully disclose verified data breaches and announce the policy changes being made to address problems will soften the blow and likely maintain public trust in their operations.

Information resellers should carefully verify the identities of all customers to preserve privacy and security of consumer information.

ChoicePoint failed to adequately leverage its own business processes. ChoicePoint markets and promotes services for identity verification and fraud prevention for other businesses, yet failed to use these same services to prevent large-scale fraud against its own databases. One of the promotions for ChoicePoint’s services includes the line: “You need to be confident that a business is legitimate and protect your company’s assets and reputation” [AJC05b]. Ironically, ChoicePoint was not able to complete this task successfully with its own customers. A spokesman for the company said in the first week of the news breaking that this data breach had “nothing to do with a failure of technology or a failure of security procedures,” yet ChoicePoint purports to safeguard against this very type of fraud via its business products [AP05b]. The FTC alleged that ChoicePoint did not catch the con artists using suspended business licenses, personal phone numbers, or the use of varying addresses within a single application. These errors should have triggered immediate warnings that fraudulent access to the database was being attempted.

Regular security audits should be a vital part of any data governance strategy.

The FTC’s ruling against ChoicePoint included a provision requiring a regular security audit every two years for the next twenty years. Such a policy should be extended to all companies trafficking in personal information and should be carried out beyond the 20-year stipulation [MBT05]. By performing such regular audits, companies would both fortify themselves against data breaches and provably maintain commercially reasonable security levels, which is the FTC’s standard for negligence in data breaches.

Data brokers should log and maintain an audit trail of all accesses to their databases.

Given the risk of unauthorized access, data brokers should be logging all access to their databases of personal information. Such monitoring would allow companies to detect unauthorized access and prevent another data breach like the one ChoicePoint suffered. Auditing access can also allow data brokers to affirmatively defend against allegations of negligence, should a data breach still occur.

All personal information should be stored in encrypted form.

While encrypting data would not have helped in the ChoicePoint case, numerous data breaches announced since the ChoicePoint incident have involved the loss or theft of unencrypted

personal information. Encryption of sensitive data minimizes the risk of that data should it be acquired by identity thieves. Several federal bills under consideration would make exceptions for requiring notification if the data was encrypted, and therefore companies may also avoid disclosing breaches if they maintain sensitive data strictly in encrypted form.

Privacy policies should express a company's overall privacy principles and practices.

ChoicePoint's privacy policy fails to provide information on how ChoicePoint actually secures and protects consumers' personal information. Instead, the policy focuses more on the company's guarantees about enforcement, should a policy violation occur. A data broker's privacy policy should instead allow both consumers and customers to understand how sensitive information will be stored and protected, and enumerate the rights that consumers have to protect the privacy of that information. An online privacy policy is the public statement of how a company plans to protect privacy, and thus should include information on online and offline information transactions. Finally, if a company does not live up to its privacy policy, it exposes itself to legal liability, which is a powerful incentive to adhere to its own promises.

Acknowledgements

This work was supported by NSF ITR Grant #522931.

References

- [AE04] A.I. Antón and J.B. Earp, "A Requirements Taxonomy to Reduce Website Privacy Vulnerabilities," *Requirements Engineering Journal*, vol. 9, no. 3, August 2004, pp. 169-185.
- [AJC05a] B. Husted, "Boss keeps low profile amid crisis," *Atlanta Journal-Constitution*, February 19, 2005, L/N.
- [AJC05b] M. Kempner, "Checklist failed ChoicePoint," *Atlanta Journal-Constitution*, February 20, 2005, L/N.
- [AJC05c] B. Husted, "Data theft from ChoicePoint," *Atlanta Journal-Constitution*, February 25, 2005, L/N.
- [AJC05d] B. Husted, "Exec: ChoicePoint will be more open," *Atlanta Journal-Constitution*, April 1, 2005, L/N.
- [AP05a] R. Konrad, "Californians warned that hackers may have stolen their data," *The Associated Press*, February 15, 2005, L/N.
- [AP05b] H.R. Weber, "ChoicePoint's mission turned on head in personal info breach," *The Associated Press*, February 17, 2005, L/N.
- [AP05c] R. Konrad, "Calls for federal regulation grow as data retailer scandal widens," *The Associated Press*, February 18, 2005, L/N.
- [AP05d] H.R. Weber, "ChoicePoint Had Another Identity Theft," *The Associated Press*, March 2, 2005, L/N.
- [CSO05] S.D. Scalet, "The Five Most Shocking Things About the ChoicePoint Debacle," *CSO Magazine*, May 1, 2005, <http://csoonline.com/read/050105/choicepoint.html>.
- [EAA05] J.B. Earp et al, "Examining Internet Privacy Policies Within the Context of User Privacy Values," *IEEE Trans. On Engineering Management*, vol. 52, no. 2, May 2005, pp. 227-237.
- [FTC06] FTC Consumer Sentinel, "Consumer Fraud and Identity Theft Complaint Data," January 25, 2006, <http://consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>.
- [Gar06] Gartner, "Case Study: ChoicePoint Incident Leads to Improved Security, Others Must Follow," September 19, 2006, http://www.choicepoint.com/news/choicepoint_1996.pdf
- [Har05] R. O'Harrow, *No Place To Hide*, Free Press, January 2005.
- [ITRC04] Identity Theft Resource Center, "Identity Theft: The Aftermath 2004," September 2005, <http://idtheftcenter.org/aftermath2004.pdf>.

- [LA05] J. Peterson, "Data Collectors Face Lawmakers," *Los Angeles Times*, March 16, 2005, L/N.
- [MSN05] B. Sullivan, "Database giant gives access to fake firms," *MSNBC*, February 14, 2005, MSNBC.com.
- [MBT05] R. Moffie, D.L. Baumer, and R. Tower, "Identity Theft and Data Security," *Internal Auditing*, vol. 20, no. 5, September/October 2005, pp. 29-37.
- [PA05] Pierce, Deborah and Linda Ackerman, "Data Aggregators: A Study of Data Quality and Responsiveness," May 19, 2005, <http://privacyactivism.org/docs/DataAggregatorsStudy.html>.
- [PRC05] Privacy Rights Clearinghouse, "Alert: The ChoicePoint Data Security Breach," February 19, 2005, <http://privacyrights.org/ar/CPResponse.htm>.
- [WP05a] R. O'Harrow, "In Age of Security, Firm Mines Wealth of Personal Data," *The Washington Post*, January 20, 2005, L/N.
- [WP05b] R. O'Harrow, "ID Data Conned From Firm," *The Washington Post*, February 17, 2005, L/N.
- [WP05c] J. Krim, "Consumers Not Told Of Security Breaches, Data Brokers Admit," *The Washington Post*, April 14, 2005, L/N.