The ChoicePoint Dilemma

How Data Brokers Should Handle the Privacy of Personal Information

Before 2005, data broker ChoicePoint suffered fraudulent access to its databases that exposed thousands of customers' personal information. We examine ChoicePoint's data breach, explore what went wrong from the perspective of consumers, executives, policy, and IT systems, and offer recommendations for the future.

Paul N. Otto, Annie I. Antón, and David L. Baumer
The Privacy Place, North Carolina State University

Over the past 20 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 US, culling data from three major categories: public records, publicly available information, and nonpublic information. Ironically, much of the demand for the informational products that data brokers supply 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, so government agencies have increasingly turned to data brokers for consumer information. There are thousands of data brokers, large and small, operating in the US 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. (See testimony from Chris Hoofnagle, EPIC's West Coast Director, at http://epic.org/privacy/choicepoint/.)

In 2005, there was a significant increase in the disclosure of data breaches, with more than 150 breaches exposing more than 57 million records containing personal information to unauthorized access. (The Privacy Rights Clearinghouse maintains a list of announced data breaches at http://privacyrights.org/ar/ChronDataBreaches.htm.) The first major incident announced in 2005 was the fraud committed against ChoicePoint, a US-based commercial data broker.[1] At the time, much of the general public wasn't familiar with the data broker industry, nor had it paid much attention to the risk data breaches pose. The massive data security breach at ChoicePoint was seemingly a tipping point. Ever since the ChoicePoint news, the data broker industry, as well as the privacy and security of personally identifiable information (PII), has been subject to increasing public and congressional attention.

In addition to data brokers, several entities with more benign reputations, including universities, financial institutions, large retailers, and government agencies, have also reported data breaches. Such 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 breaches (the *Javelin 2006 Identity Fraud Survey Report* found that out of the 47 percent of identity theft victims surveyed who knew how their personal information was obtained, six percent faulted data breaches; see http://bbb.org/Alerts/article.asp?ID=651), but there's increased risk from each and every record containing PII that's lost, stolen, and exposed.

Identity theft is a growing epidemic in the new millennium: the US Federal Trade Commission (FTC) received 255,565 consumer complaints of identity theft in 2005, making it the biggest consumer concern for the sixth straight year.[2] The FTC estimates that more than 27 million people were identity theft victims between 2000 and 2004, with nearly 10 million in 2004 alone. The cost

Table 1. ChoicePoint's customers by revenue for 2005.

CUSTOMER	TOTAL REVENUE (%)	REVENUE (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

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 US$4,000 in income.[3]

In this article, we focus on a ChoicePoint data breach that received widespread publicity and was the subject of legal action by the FTC. Using this data breach for illustrative purposes, we examine the privacy risks inherent in the buying and selling of personal information. Our work is based on information obtained from various public sources, coupled with published reports that we assumed to be accurate. We reference official ChoicePoint press releases and company statements directly, whereas other facts were verified in at least two sources.

The business of information sharing

In 1997, the credit agency Equifax spun off its underperforming insurance information division as ChoicePoint. Reportedly, the split was also intended to help the business avoid laws restricting how credit agencies sell information; as a data broker, instead of a financial services company, ChoicePoint wouldn't be subject to such laws. In the company's capacity as a consumer reporting agency, however, ChoicePoint's transactions remain highly regulated. Since the spin-off, ChoicePoint has acquired at least 60 companies and hundreds of thousands of customers, and now employs approximately 5,500 employees. ChoicePoint's original focus was to provide credit data to insurance underwriters, but the company now sells data to more than 50 percent of the top 1,000 US companies and has the largest background screening business in the US. 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."[4] Table 1 presents a complete breakdown of ChoicePoint's customers by revenue.

ChoicePoint has accumulated more than 19 billion public records, equaling more than 250 Tbytes of data in its databases.[5] This article, building on other efforts,[6] 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.

The ChoicePoint case

On 14 February 2005, MSNBC.com reported that fraudulent parties ("fraudsters") posing as legitimate businesses accessed ChoicePoint's databases and that up to 35,000 Californians might have been affected.[1] 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 in order to pose as check-cashing companies and debt-collection firms.[7] The business licenses were obtained by using previously stolen identities to provide real people's names, social security numbers (SSNs), phone numbers, and addresses. The fraudsters then faxed copies of business licenses and applications to ChoicePoint, 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, they performed roughly 17,000 searches of ChoicePoint's databases. Criminal investigators discovered more than 800 instances of identity theft in which fraudsters used the stolen information to access the personal information that ChoicePoint had stored. According to ChoicePoint, these security breaches eventually cost the company US$27.3 million in 2005 alone to cover legal fees, notify victims, and seek audits.[4]

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. The statute (Cal. Civ. Code §1789.29a) requires any organization doing business in California to disclose data breaches to California residents when unauthorized access to unencrypted per-

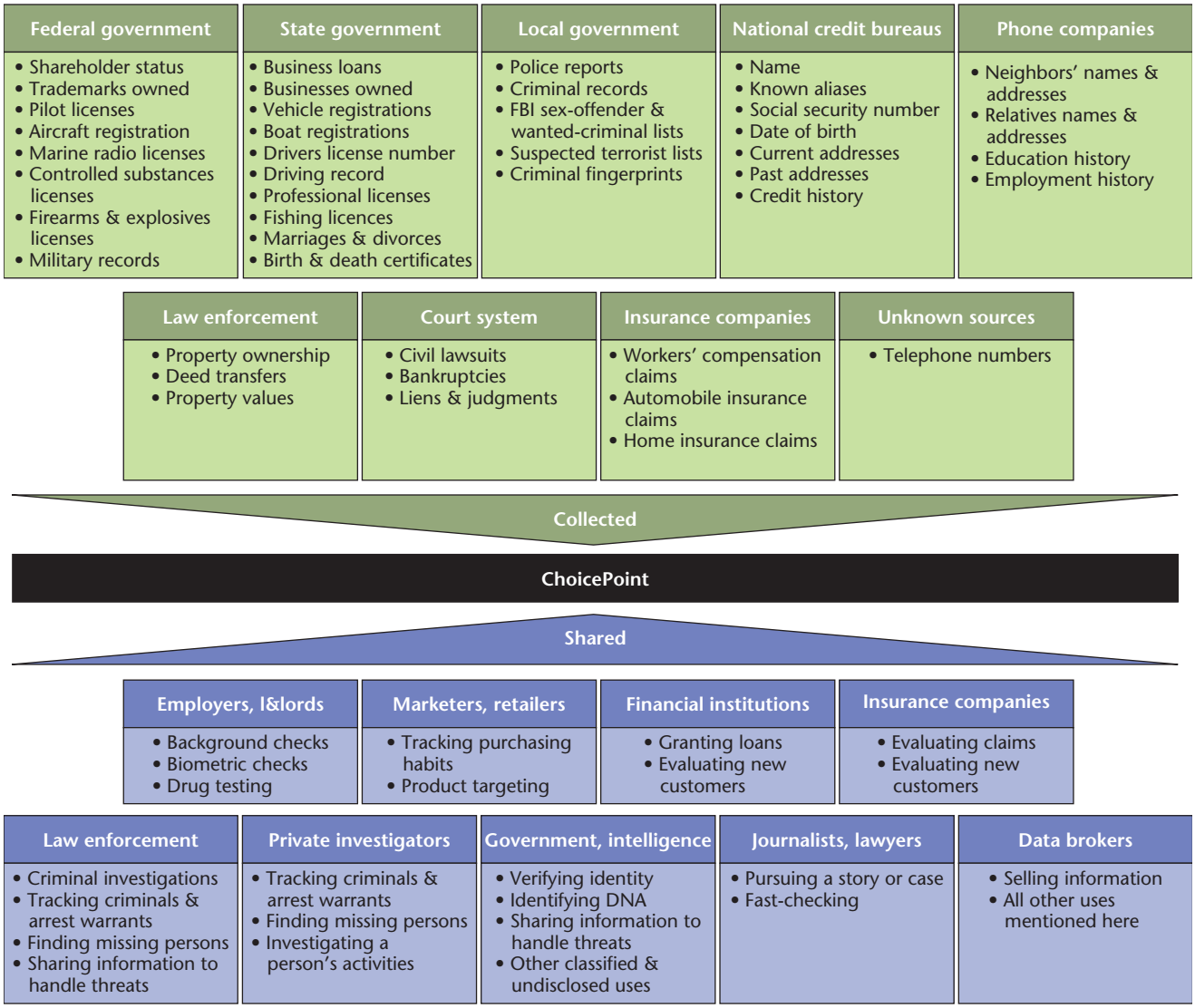

Figure 1. ChoicePoint's information flow model. The blue boxes below the center ChoicePoint rectangle represent data leaving the data broker, and the green rectangles above ChoicePoint's name reflect sources of data entering the company.

sonal information occurs. In testimony before the US Congress, a ChoicePoint executive admitted that without this law, it's possible that consumers would never have learned about the data breach.[8] The fact that ChoicePoint initially limited its fraud investigation to transactions occurring on or after the California law took effect further illustrates the act's impact.

SEC and FTC investigations

Formal disclosure of the ChoicePoint security breach occurred on 4 March 2005, when ChoicePoint filed a Form 8-K—required whenever a firm subject to US Securities and Exchange Commission (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 investigating 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 separately launched an inquiry into both the fraud and ChoicePoint executives' stock trading.

The FTC concluded its investigation in 2006 by announcing a landmark US$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 to compensate identity theft victims. (The full text of the FTC complaint and settle-

ment appears at http://ftc.gov/os/caselist/choicepoint/choicepoint.htm.) The FTC claimed that ChoicePoint violated the terms of the Fair Credit Reporting Act (FCRA) when it shared personal credit data with unauthorized users and misled customers in its privacy statements by claiming that its database was secure. As part of the settlement, ChoicePoint didn't admit any wrongdoing, but instead agreed to implement new security and access procedures and to fund a third-party security audit every two years for the next 20 years.

The SEC's inquiry into ChoicePoint largely examined whether ChoicePoint executives violated securities laws by engaging in insider trading. ChoicePoint's board approved the sale of stock by the company president and CEO one day before the arrest of the main fraud suspect and one month after ChoicePoint first discovered the fraud. Most likely, such information, if known to the public, would have affected ChoicePoint's stock price. 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.

Lawsuits

The data breach also spawned several lawsuits by private citizens against ChoicePoint, both from consumers and shareholders. (These lawsuits have been discussed in ChoicePoint's various SEC filings after the data breach.) The first lawsuit (*Goldberg v. ChoicePoint*) was filed within a week of the data breach becoming public, with claims that ChoicePoint was both fraudulent and negligent in its handling of the breach and employed unfair business practices. Another lawsuit (*Salladay v. ChoicePoint*), filed within a month of ChoicePoint's public disclosure, alleged that the company violated the FCRA and various privacy rights by disclosing personal information, and sought 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 were consolidated into a single class-action suit (*Harrington et al. v. ChoicePoint*) that is still ongoing.

The consumer lawsuits seek to represent all 163,000 individuals that ChoicePoint notified, rather than merely 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.[9] These lawsuits seek to establish a new precedent—namely, that plaintiffs are entitled to a monetary remedy when subjected to identity theft risk, rather than having to show actual damages directly resulting from 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 that information to the public. The fate of these ongoing lawsuits (*In re ChoicePoint Inc. Securities Litigation*, *In re ChoicePoint Inc. Derivative Litigation*) likely hinges on the outcome of the SEC investigation into the potential insider trading.

ChoicePoint's evolving policies

Given our experience in analyzing more than 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 because the fraudsters were able to evade detection for more than a year. As a starting point, we focused on the ways ChoicePoint customers established identities to access the databases prior to the breach.

Before gaining access to the ChoicePoint databases, potential customers were required to establish identity and their reasons for seeking access. For this purpose, ChoicePoint accepted business licenses via fax as well as by mail. Once the business license was in ChoicePoint's possession, the company then verified it by checking facts such as the principals listed 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 these fraudulent new customers' identities.

Once ChoicePoint verified a new customer, this customer received a username and password combination with which to access the database. According to court papers filed by the FTC, customer search histories weren't stored, nor were the results archived or all accesses logged. After the data breach, a company spokesperson stated that ChoicePoint "has no way of knowing whether anyone's personal information actually has been accessed."[1]

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, these individuals or businesses enjoyed largely unsupervised and unfettered access to the wealth of information inside the databases. The major hurdle appears to have been the initial identity verification, which was easily bypassed with stolen identities.

Policy changes after the data breach

Following the 2005 data breach, ChoicePoint made numerous changes in its policies and procedures, many of which were mandated by the consent decree it agreed to in lieu of further court action (ChoicePoint keeps a running list of its changes at www.privacyatchoicepoint.com/common/pdfs/CPPrivacyFactSheet.pdf). Upon discovering the data breach, the company's initial reaction was to close all 50 suspicious accounts and stop accepting faxed versions of business licenses. Furthermore,

the company increased its verification procedures for establishing customer identity and announced that any nongovernmental, privately held business must be recredentialed to maintain access to its databases.

ChoicePoint also 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 purposefully 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 have changed for both new and existing customers. Existing customers face 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 more than 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 their new Office of Credentialing, Compliance, and Privacy, which would monitor ChoicePoint's activities and report directly to its 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 of any future data breaches.

The company also mobilized to correct many of its early mistakes. It established a Web site dedicated to privacy issues (www.privacyatchoicepoint.com) and created an independent office to handle privacy matters. Additionally, it offered 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 (Statement on Auditing Standards No. 70), which defines the standards an auditor must use to assess an organization to evaluate ChoicePoint's data management practices and underwent a total of 43 third-party audits in 2005 and 40 such audits in 2006. In addition, it hired Ernst & Young to review and improve the company's practices regarding privacy, credentialing, and compliance.

ChoicePoint's online privacy policies

To better understand ChoicePoint's privacy practices, we employed a content-analysis technique, called *goal-mining* (the extraction of goals from text artifacts),[10] to analyze ChoicePoint's online privacy policies. We downloaded new versions from ChoicePoint's Web site (http://choicepoint.com/privacy) and accessed older versions dating back to 2000 via the Internet Archive (http://archive.org). We extracted the goals using a Web-based privacy goal management tool (PGMT) developed by our team at North Carolina State University. We also analyzed the evolution of the privacy policy to examine how ChoicePoint's privacy practices have changed over the past six years.

We extracted a total of 53 unique taxonomy goals from the most recent privacy policy, with four of those repeated twice within the document. Previous research has established a goals taxonomy, which distinguished privacy protection goals from vulnerabilities.[10] 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 haven't 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 data that's collected and sold, both on- and offline. Their privacy policy has consistently focused on information buyers, rather than the consumers whose information is being traded.

There's no way for individual consumers to prevent the kind of data breach that occurred at ChoicePoint.

Discussion

The ChoicePoint data breach has changed the legal landscape for data brokers. We now examine how federal and state governments have reacted to the data breach epidemic, as well as the rights and responsibilities that consumers have with respect to their PII.

Legal landscape

Before 2003, companies had little incentive to report data breaches to the public, but given recent trends in legislation and public accountability, undisclosed breaches are increasingly a substantial legal risk.[11] However, a single federal statute that comprehensively regulates data privacy issues doesn't yet exist; 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, and, as a result, more than a dozen bills were brought before various Congressional committees in 2005. Although no bill has passed to date, the continuing revelation of negligent storage and handling of PII augurs in favor of Congress establishing federal regulation governing data security. Data brokers are a powerful special interest with allies among law enforcement and financial institutions, so 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.

Individual states have been much quicker than the federal government in responding to the identity theft threat. At the start of 2005, only two states had security freeze laws in effect, and another two had laws coming into effect that year, but by the end of the year, 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, but by September 2006, 33 additional states had passed similar legislation; some states, such as New York, enacted even tougher measures to enforce notification.

Consumer rights and responsibilities

Although many states have already passed notification laws, and federal legislation is still under consideration, data brokers entered 2007 essentially as unregulated as they were in 2005. Due to this lack of regulation, data brokers generally chose to exclude consumers from every aspect of their operations, leaving them little access or control over their own personal information. With the exception of medical and financial information, data brokers aren't required to obtain permission of their data subjects in the US before collecting, processing, and transmitting information. The default rule for information sharing in the US is that of opt-out, rather than opt-in. Data brokers typically have no business relationship or interactions with the individual whose information is being traded. Unless consumers actively seek to prevent the sharing of their PII or threaten to create adverse publicity, companies are free to do almost anything they want with the data they collect. Furthermore, there's no way for individual consumers to prevent the kind of data breach that occurred at ChoicePoint. In general, the only legal protection individuals currently have comes from government lawsuits, such as the FTC's action 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. For example, consumers nationwide are now entitled to a free copy of their credit reports from each of the three credit bureaus once per year.[12] Careful monitoring helps consumers detect identity theft sooner rather than later.

Existing and proposed extensions to consumer rights to manage their own credit reports could 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. This alert is intended to stave off fraudulent requests for credit, when a consumer suspects that an identity thief might strike. Several states are considering extending this privilege into the right to freeze a credit file, which would prevent any creditors from issuing credit for that consumer until the file is "thawed," allowing the consumer to better control his or her credit (see http://consumersunion.org/pub/core_financial_services/001872.html).

Many dossiers on consumers exist 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.[12] ChoicePoint now offers free annual copies of its personal public records searches to consumers at http://choicetrust.com, even though no law currently requires such access.

Prior to the data breach, ChoicePoint stated that it couldn't correct errors in its records but that consumers must locate the original source from which ChoicePoint gathers 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 11 reports received as part of the study contained at least one error, with eight of the 11 containing errors in basic biographical information.[13] After the data breach became public, the company 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."[14] Although announced soon after the data breach became public, the new system isn't 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 maintains a site detailing what consumers should do to minimize their risk (www.consumer.gov/idtheft). One such responsibility is to check 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 (http://privacyrights.org/ar/infobrokers.htm). Consumers can also contact each company with which they have a relationship to request opting out of information transfers, although no binding legal requirements require companies to respect such wishes.

Despite the lack of an ownership right to personal information in the US, consumers deserve 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 provide consumers a low-cost means of eliminating harmful errors from their records.

Recommendations

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

Have a plan to deal with breaches

ChoicePoint had to quickly devise a plan of action for dealing with both the data breach and the media, as the company had only two weeks to strategize before the breach became public.[15] 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 suffered similar data breaches in the past, the company should have been prepared. A clear sign of this lack of preparation is evident in the original notification letter, signed "J. Michael de Janes, Chief Privacy Officer" (view the letter at http://csoonline.com/read/050105/choicepoint_letter.html). This was apparently the first and last use of this title for de Janes (who was really the company's general counsel); it appears as though the company realized its lack of a privacy chief and thus created the position on the spot.[16]

The CEO's lack of early knowledge about the data breach gives rise to further concern. ChoicePoint's vice president testified before the US 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.[17] The CEO separately confirmed in an interview that he didn't know about the fraud until late December at the earliest.[18] 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 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.[11] They should have detailed plans for how the company will respond, and they should have key personnel, such as chief privacy officers, chief security officers, and chief information security officers, active and involved with the planning process. Any strategy should include a plan for notifying the public in the case of such a data breach.

Provide prompt and accurate notification

During the data breach's news coverage, ChoicePoint was plagued by inconsistencies between the facts and what spokespeople—including the CEO—told the public. The first inconsistency involved whether only Californians were affected. When the data breach first hit the news (five months after it was first discovered), a spokesman said that ChoicePoint didn't "have any evidence at this point that the situation has spread beyond California."[19] Another spokesman said ChoicePoint learned that non-California residents were at risk two

Despite the lack of ownership rights to personal information, consumers deserve to see what information companies have about them.

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.[20] 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 that ChoicePoint belatedly admitted to the nationwide scope. 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.

Many companies realized the need to promptly alert the public of data breaches—before the news media could break the story.

Another major inconsistency involved ChoicePoint's claim that this data breach was the first of its kind for the company. Within three weeks of the first news, the media exposed a previous data breach that ChoicePoint suffered in 2002.[21] 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 realized the need to promptly alert the public of data breaches—before the news media could break the story. 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 changes being made to address problems will soften the blow and likely maintain public trust in their operations.

Verify customers' identities to preserve privacy

ChoicePoint failed to adequately leverage its own business processes. It 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. A promotion 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."[22] A company spokesman 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.[7] The FTC alleged that ChoicePoint didn't catch the fraudsters using suspended business licenses, personal phone numbers, or varying addresses. These errors should have triggered immediate warnings that fraudulent access to the database was being attempted.

Perform regular security audits

As noted earlier, the FTC's ruling against ChoicePoint included a provision requiring a regular security audit every two years for the next 20 years. Such a policy should be extended to all companies trafficking in personal information and should extend beyond the 20-year stipulation.[11] 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.

Maintain an audit trail

Given the risk of unauthorized access, data brokers should log all access to their databases. 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 and demonstrate due diligence, should a data breach occur.

Store personal information in encrypted form

Although encrypting data wouldn't have helped in the ChoicePoint case, numerous data breaches announced since then have involved the loss or theft of unencrypted personal information. Encryption of sensitive data minimizes the risk to that data if identity thieves acquire it. Several federal bills under consideration would make exceptions for requiring notification if the data were encrypted; therefore, companies can avoid disclosing breaches if they maintain sensitive data strictly in encrypted form.

Express the company's overall privacy practices clearly

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 make clear to both consumers and customers how it will store and protect sensitive information, 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 about online and offline information transactions. If a company doesn't live up to its privacy policy, it exposes itself to legal liability, which is a powerful incentive to adhere to its own promises.

Legislation is needed to regulate the flow of personal information in the age of data brokers and rampant identity theft. In the meantime, the ChoicePoint data breach has taught us that companies must be more diligent in how they handle personal information, as well as how they handle the aftermath of a data breach. Improving security safeguards and strengthening privacy protections will help fight the identity theft epidemic, but ultimately consumers must be diligent in monitoring their personal information and credit reports.

Acknowledgments

This work was supported by US National Science Foundation Information Technology Research grant #522931.

References

1. B. Sullivan, "Database Giant Gives Access to Fake Firms," 14 Feb. 2005; www.msnbc.msn.com/id/6969799/.
2. US Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data," *Consumer Sentinel*, 25 Jan. 2006; http://consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.
3. Identity Theft Resource Ctr., "Identity Theft: The Aftermath 2004," Sept. 2005; http://idtheftcenter.org/aftermath2004.pdf.
4. Gartner Group, "Case Study: ChoicePoint Incident Leads to Improved Security, Others Must Follow," 19 Sept. 2006; www.choicepoint.com/news/choicepoint_1996.pdf.
5. R. O'Harrow, *No Place To Hide*, Free Press, 2005.
6. R. O'Harrow, "In Age of Security, Firm Mines Wealth of Personal Data," *The Washington Post*, 20 Jan. 2005; www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html.
7. H.R. Weber, "ChoicePoint's Mission Turned on Head in Personal Info Breach," *The Associated Press*, 17 Feb. 2005; downloaded from Lexis-Nexis.
8. J. Krim, "Consumers Not Told of Security Breaches, Data Brokers Admit," *The Washington Post*, 14 Apr. 2005; www.washingtonpost.com/wp-dyn/articles/A51722-2005Apr13.html.
9. Huggins v. Citibank, N.A., et al, 585 S.E.2d 275 (S.C. 2003); www.judicial.state.sc.us/opinions/displayOpinion.cfm?caseNo=25691.
10. A.I. Antón and J.B. Earp, "A Requirements Taxonomy to Reduce Website Privacy Vulnerabilities," *Requirements Eng. J.*, vol. 9, no. 3, 2004, pp. 169–185.
11. R. Moffie, D.L. Baumer, and R. Tower, "Identity Theft and Data Security," *Internal Auditing*, vol. 20, no. 5, 2005, pp. 29–37.
12. Privacy Rights Clearinghouse, "Alert: The ChoicePoint Data Security Breach," 19 Feb. 2005; http://privacyrights.org/ar/CPResponse.htm.
13. D. Pierce and L. Ackerman, "Data Aggregators: A Study of Data Quality and Responsiveness," 19 May 2005; http://privacyactivism.org/docs/DataAggregatorsStudy.html.
14. B. Husted, "Exec: ChoicePoint Will Be More Open," *Atlanta Journal-Constitution*, 1 April 2005; downloaded from Lexis-Nexis.
15. B. Husted, "Boss Keeps Low Profile amid Crisis," *Atlanta Journal-Constitution*, 19 Feb. 2005; downloaded from Lexis-Nexis.
16. S.D. Scalet, "The Five Most Shocking Things about the ChoicePoint Debacle," *CSO Magazine*, 1 May 2005; http://csoonline.com/read/050105/choicepoint.html.
17. J. Peterson, "Data Collectors Face Lawmakers," *Los Angeles Times*, 16 Mar. 2005; downloaded from Lexis-Nexis.
18. B. Husted, "Data Theft from ChoicePoint," *Atlanta Journal-Constitution*, 25 Feb. 2005; downloaded from Lexis-Nexis.
19. R. Konrad, "Californians Warned that Hackers May Have Stolen Their Data," *The Associated Press*, 15 Feb. 2005; www.usatoday.com/tech/news/computersecurity/hacking/2005-02-16-choicepoint-hacked_x.htm.
20. R. O'Harrow, "ID Data Conned from Firm," *The Washington Post*, 17 Feb. 2005; www.washingtonpost.com/wp-dyn/articles/A30897-2005Feb16.html.
21. H.R. Weber, "ChoicePoint Had another Identity Theft," *The Associated Press*, 2 Mar. 2005; www.signonsandiego.com/news/computing/20050302-1402-choicepoint.html.
22. M. Kempner, "Checklist Failed ChoicePoint," *Atlanta Journal-Constitution*, 20 Feb. 2005; downloaded from Lexis-Nexis.

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); he is also a JD student at Duke University Law School. His research interests include software requirements engineering, security and privacy requirements, policy specification, and legal compliance. Otto has a BS in computer engineering from the University of Virginia and an MS in computer science from North Carolina State University. 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 director of The Privacy Place and a Cyber Defense Lab member. Her research interests include software requirements engineering, information privacy and security policy, regulatory compliance, software evolution, and process improvement. Antón 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, Sigma Xi, 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's 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). Baumer 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.*