

ChoicePoint: Personal Data and a Loss of Privacy (A)

On September 27, 2004, ChoicePoint, a company that stores and sells critical personal information, discovered possible fraudulent activity within their network of databases.¹ Upon further inquiry, ChoicePoint security officials realized that they may have allowed identity thieves in the Los Angeles area, who acted as legitimate business clients, to access people's personal information. In mid-October the company began working with the Los Angeles Sheriff's Department (LASD) and soon discovered that an identity theft ring had set up over 50 fake companies that posed as legitimate business clients. The illegitimate companies inquired and received everything from social security numbers to credit reports, more than enough information to steal someone's identity. The security breach effectively put 35,000 Californians and 110,000 people across the country at an increased risk of identity theft.²

An Arrest is Made

The LASD, working with ChoicePoint, were able to set up a successful sting operation which resulted in the arrest of one of the data thieves. On October 26, 2004, Olutunji Oluwatosin was arrested after receiving a fax from ChoicePoint requesting an additional signature for one of the illegitimate companies the thieves had previously set up. The contact information for the fake company was that of a local Kinkos and when Mr. Oluwatosin arrived to pick up the fax he was apprehended by the LASD.

Instructions from LASD to Delay Announcement of Breach. The LASD originally instructed ChoicePoint to delay any public announcement of the security breach because it would have hindered an ongoing investigation. However, there are some inconsistencies with regard to how long ChoicePoint was told to wait. Company officials maintain that they were told to hold off any announcement until January while a representative of the LASD has said that they instructed ChoicePoint to start disclosing problems in November.³ At any rate, ChoicePoint will have to disclose the security breach at some time in the near future. California state law mandates that its citizens be informed when their personal information is compromised.

A Questionably Timed Executive Stock Sale. On November 3rd, whether or not the security breach was known at the time to ChoicePoint executives, Derek Smith, CEO, and Douglas Curling, President and COO, adopted plans for prearranged stock sales over a six month period.⁴ The plans, which had previously been approved by the board of directors, call for the sale of 24% of the executives combined stock in the company. The executives started to sell their ChoicePoint shares on November 9th, before any public announcement of the security breach.

ChoicePoint

ChoicePoint was founded in 1997 by Equifax, an information management company, when it spun-off its insurance services group. Former Equifax Vice President and Senior Vice President of Finance and Administration Derek Smith and Doug Curling, respectively, joined ChoicePoint at its inception and have helped evolve the company into being the premier provider of decision-making intelligence to businesses and government.⁵ ChoicePoint now stores private information such as social security numbers, credit ratings, and criminal history reports on its databases and makes this information available to qualified clients.

After the events of September 11, 2001, the United States government's need for background information increased exponentially as did ChoicePoint's services to various government agencies. The acquisitions of Templar Corp. which employs an information sharing system originally envisioned by the departments of Defense and Justice and IMapData Inc., an information gathering company whose clients include intelligence and homeland security agencies, further enabled ChoicePoint to increase business with the federal government.⁶ Through their strategic acquisitions, over 60 in all, and the increased use of data brokers by the federal government and businesses, ChoicePoint has experienced rapid growth. ChoicePoint now employs 5,500 people and is listed on the New York Stock Exchange under the symbol CPS. The company registered record annual revenue in 2004 of over 884 million dollars.⁷

Corporate Communications at ChoicePoint. The communications team at ChoicePoint is relatively small and has had no experience with situations such as this. The team is made up of James Lee, Chief Marketing Officer, who is in charge of all internal and external messaging, and three other persons, two of which are dedicated to employee communications.⁸ The fraudulent activity coupled with a questionably timed stock sale by company executives agreeably puts the communications team at ChoicePoint in a crisis situation.

Derek Smith and Douglas Curling. Derek Smith joined ChoicePoint as CEO after its spin off from Equifax in 1997 and became Chairman in 1999. Mr. Smith is seen by many in the industry as being on the leading edge of information technology.⁹ He has written several books including: *A Survival Guide in the Information Age*, a book that contains ways to safeguard you and your family from identity theft, and *Risk Revolution; The Threats Facing America & Technology's Promise for a Safer Tomorrow*.¹⁰ Derek Smith is an advocate for using technology to combat terrorists and criminals and he believes it is possible to make our nation more secure while protecting civil liberties.¹¹ Smith serves on the board of the Society of International Business Fellows and The Educational Foundation of Georgia State University and is an honor graduate of Pennsylvania State University.¹²

Douglas Curling, like Derek Smith, joined ChoicePoint at its inception. He has held the positions of Chief Financial Officer, Chief Operating Officer, and is now President Chief Operating Officer and Director. Mr. Curling has been responsible for ChoicePoint's acquisitions which successfully diversified revenue sources. Douglas Curling emphasizes efficient internal organization in the ever changing technology industry.¹³

The Data Brokerage Industry

The data brokerage industry is a relatively new industry. The technological advances of the past decade have paved the way for new kinds of companies such as ChoicePoint and Lexis Nexis, a rival firm, to exist. Through the increased power of computers, lowered costs of data storage, and the ever increasing speed of the Internet, these companies are able to aggregate, store, and retrieve large amounts of information in a quick manner. The information collected by these firms range from as detailed as someone's social security number, driving, criminal, and credit records to as general as one's college alma mater.¹⁴ However, for a business opportunity to exist for these firms there must be customers who would like to purchase this information.

Fortunately for data-brokers, there are more than enough potential businesses and governmental agencies that would like to get their hands on such data. Businesses use information such as criminal records and social security numbers to help in wise hiring decisions and credit reports are used when contemplating whether or not to grant credit. Governmental and law enforcement agencies rely on data brokers to compile and use information to solve crimes and protect the nation from terrorists. Data brokers are able to provide the agencies with information that would otherwise be non accessible due to several privacy laws that restrict the government's ability to obtain personal information.¹⁵ Technology breakthroughs and large customer bases have allowed data brokers to experience large profits and growth, a trend that is likely to continue in the future. Today the data brokerage stands as a 5 billion dollar industry.¹⁶

Current Regulation

The data brokerage industry is, more or less, unregulated. There are certain laws such as the Fair Credit Reporting Act (FCRA) which regulates companies that issue consumer credit reports but their main objective is to make sure credit reports are not distributed for marketing purposes.¹⁷ In 1997, the Federal Trade Commission issued a set of principles for data brokerage firms in an effort to set up acceptable best practices for the industry. Nevertheless, these principles mostly deal with certain types of information not to be used for marketing purposes. California disclosure law, Senate Bill 1386, is the only law of its kind that requires data brokers like ChoicePoint to report any potential release of their personally identifiable information.¹⁸ Any other federal or state disclosure laws regarding breaches of data security are limited to certain types of businesses such as financial institutions.¹⁹

Privacy and Identity Theft in Today's High Tech World

Individual privacy today is at an all time low. The technological advances of the computer and Internet have allowed for virtually anyone to collect data on people. Internet companies have devised ways to track internet users as they travel through the internet (devices known as cookies), grocery stores issue discount cards that track what people buy and when they buy it, and federal and state governments have put an increasingly amount of public information on the internet.²⁰

Arguments can be made on both sides of the issue. The quick accessibility of information on the Internet in many cases has allowed for an easier and more efficient lifestyle. Businesses that track our buying behavior are more capable of pointing us in the direction of other items we may want and often offer us discounts on frequently purchased products. And as more records are put online by government the faster we can get a hold of duplicate records such as birth certificates and voter registration cards when we need them. Companies like ChoicePoint have provided many benefits to society as they have actively participated in finding many abducted children, have helped track down numerous deadbeat dads, and have provided information to law enforcement agencies that has led to the arrest of criminals.²¹

On the other hand, privacy advocacy groups such as Privacy Rights Clearinghouse point out that this enhanced accessibility to personal information makes us vulnerable to not only identity theft but also incorrect data profiles. One of the biggest problems with aggregating information from a variety of sources is errors and omissions in the data. These mistakes and holes in someone's profile create opportunity for misunderstandings between the party using the information and the individual that is portrayed. This can especially be a problem when the incorrect profiles are used in the hiring and credit granting decisions, as the individual does not get a chance to review their information. Privacy Rights Clearinghouse quotes *The Unwanted Gaze: The Destruction of Privacy in America* by Jeffrey Rosen.

“Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge.”²²

One thing known for sure is that personal information that gets into the hands of the wrong people can prove harmful to both our pocket books and our reputations. Identity theft is one of the fastest growing crimes in the United States. According to a Federal Bureau of Investigation report, in upwards of 900,000 people are victims of credit theft in this nation each year.²³ At an average cost of \$1,000 for victims to repair the destruction done by identity theft, this delinquency is costly to the individual and at an average cost to financial institutions of \$6,767 per crime it puts a toll on the economy.²⁴ To make matters worse, a survey done by The Privacy Rights Clearinghouse showed that 12% of identity theft victims suffered damage done to their good names and were left with unjust criminal records due to the thieves' activity.²⁵

ChoicePoint's Actions

A public announcement by ChoicePoint is inevitable. With the arrest of one of the identity thieves, the LASD's investigations will begin to wrap up soon. Whether instructions were to start disclosing the security breach in November or January, it remains clear that at some point ChoicePoint will have to go public with the problem. How should ChoicePoint come out with the information? Should ChoicePoint inform only those Californians that may be affected by the breach? Which individuals or groups should ChoicePoint be concerned with as they make the announcement? What changes, if any, should ChoicePoint make in the future? As they get closer and closer to the public announcement, these questions and more will have to be answered by James Lee and the communications team at ChoicePoint.

References

- ¹ Gasparino, Charles and Kathryn Williams. "When Secrets Get Out," *Newsweek*. March 14, 2005.
- ² Sullivan Bob. "Data Theft Affects 145,000 Nationwide," *MSNBC*. February 18, 2005.
- ³ Gasparino, Charles and Kathryn Williams. "When Secrets Get Out," *Newsweek*. March 14, 2005.
- ⁴ Weber, Harry R. "ChoicePoint's top two execs sold shares before breach made public," *Associated Press* February 25, 2005.
- ⁵ <http://www.choicepoint.com/about/overview.html>
- ⁶ O'Harrow Jr., Robert. "ChoicePoint finds wealth in information," *The Washington Post*. January 20, 2005.
- ⁷ <http://www.choicepoint.com/choicepoint/news.nsf/1e81a178107b63b18525687f005493a7/e865631fe8b8db3385256f94007b77cb?OpenDocument>
- ⁸ Interview with James Lee, Chief Marketing Officer at ChoicePoint Inc., April 18, 2005.
- ⁹ Interview with Steve Harris, former Vice President of Communications at General Motors Inc., April 11, 2005.
- ¹⁰ <http://www.amazon.com/exec/obidos/search-handle-url/index=books&field-author=Derek%20Smith/104-0206806-9081573>
- ¹¹ <http://choicepoint.com/about/senior.html>
- ¹² http://ceoleadership.com/institute/director_bio/smith.html
- ¹³ <http://choicepoint.com/about/senior.html>
- ¹⁴ Baker, William B. "What You Need to Know About ChoicePoint," *Privacy in Focus*. March 2005.
- ¹⁵ O'Harrow Jr., Robert. "ChoicePoint finds wealth in information," *The Washington Post*. January 20, 2005.
- ¹⁶ Rigby, Bill and Theo Kolker. "Continuing and Growing Consumer Fraud," *TBR News*. April 12, 2005.
- ¹⁷ Baker, William B. "What You Need to Know About ChoicePoint," *Privacy in Focus*. March 2005.
- ¹⁸ "The ChoicePoint incident" *Red Herring*. February 23, 2005.

¹⁹ Baker, William B. “What You Need to Know About ChoicePoint,” *Privacy in Focus*. March 2005.

²⁰ <http://www.privacyrights.org/ar/Privacy-IssuesList.htm#F>

²¹ Interview with Steve Harris, former Vice President of Communications at General Motors Inc. April 11, 2005.

²² Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. Vintage, June

²³ <http://www.fbi.gov/publications/leb/2002/june2002/june02leb.htm>

²⁴ <http://www.identity-theft-protection.com/stats.html>

²⁵ <http://www.privacyrights.org/ar/Privacy-IssuesList.htm#F>

ChoicePoint:

Personal Data and a Loss of Privacy (B)

Public Disclosure, Finally

On February 14, 2005, ChoicePoint, Inc., the Alpharetta, Ga.-based data collection giant who suffered a security breach in late September of 2004, finally disclosed the problem to the public. As letters were sent out, by law, to the 35,000 California residents who were potential victims of identity theft, ChoicePoint made the internal decision to also send letters of notification to other 110,000 Americans who were potential victims. Of the 145,000 potential victims, authorities were certain that at least 750 had become victims of identity theft.¹ ChoicePoint was not required by law to notify the potential victims in the other 49 states, but it made the internal decision to do so because ChoicePoint knew that the moment the California letters were sent out the spotlight was going to turn quickly and brightly to every aspect of their operations for the foreseeable future. And ChoicePoint was right. Public disgust, media fire, and, as a result of the two, heat from legislators are now just a few of the very difficult obstacles facing ChoicePoint as the debate over privacy becomes a central issue in American society and American politics.

What Went Wrong Inside ChoicePoint

More than fifty phony businesses were created by identity thefts to exploit ChoicePoint's systems and commit identity theft. Posing as legitimate insurance agencies, check-cashing companies, and other outfits that would have normally been allowed to subscribe to ChoicePoint's services, the identity thefts gained access to the 19 billion data files that ChoicePoint has compiled in its databases.² Once inside a thief has access to seemingly endless amounts of personal information on nearly every American adult. Current and former addresses, credit information, employment history, motor vehicle records, police and criminal records, assets and property, insurance claims, and family history make up just a portion of the list of information that can literally be pulled up in minutes for anyone with access to ChoicePoint's files. Mark Noeldner, a leading banking professional in the South Bend, IN area and an adjunct professor at the University of Notre Dame states, "There is virtually no limit to the amount of personal information that you can gather about other individuals if you subscribe to one of the data brokers."³ Clearly, access to such personal information would not make it a difficult task for a criminal to steal an individual's identity and create fraudulent bank accounts and credit cards, robbing individuals of thousands of dollars.

But ChoicePoint is Good for America

Chairman and CEO of ChoicePoint, Derek Smith, the charismatic, 50-year-old company founder, privacy expert, and author of books on how to protect one's family from identity theft in today's high-technology world, has his and ChoicePoint's reputation entirely at stake. Building ChoicePoint over the last 8 years, spinning off a small unit of Equifax that stored information to

help insurers and banks tell if customers were creditworthy, Smith, along with friend, colleague, and ChoicePoint President and COO, Doug Curling, crafted an image for ChoicePoint and a message about privacy that both centered around the fact that broadening the ability to check backgrounds can reduce crime and make the U.S. economy more efficient. “The way to protect society is to restore the very best of small-town life,” Derek Smith wrote in “Risk Revolution,” which was published in July 2004, just a couple months before the security breach at ChoicePoint. He continued, “Technology, responsibly used...can rekindle the sense of community, security, and safety.” In a March 2005 interview, Derek Smith further emphasized the importance of ChoicePoint and other data collection firms, warning of the problem today “that Americans have more and more relationships with people we know less and less about.”⁴ Identity theft through a security breach at Smith’s own firm certainly calls into question just how “beneficial” or “good for America” such easy access to so much personal information is for families and individuals across America.

Not a Rotten Apple, But a Rotten Barrel

“We’re going to see this over and over. This is not about a rotten apple. It’s about a rotten barrel. And it’s only because of California’s law that we’re beginning to see it and smell it,” says Chris Jay Hoofnagle, associate director of the Electronic Privacy Information Center, a digital-rights group in Washington D.C.⁵ Such are the claims made by many privacy activists as more and more security breaches at massive data collectors result in identity theft for innocent Americans. Only in the last decade have credit reporting agencies that cater to specific clients, like banks or potential employers, been surpassed by firms like ChoicePoint and Lexus-Nexus that are essentially one-stop shops for nearly any party that needs and is able to purchase the endless amounts of consumer information. As the data collection industry grew exponentially, with firms like ChoicePoint completing 60+ acquisitions in the last seven years, regulations have not been put in place at the same speed to protect all parties involved, particularly American consumers. Quite simply, it was not entirely possible to foresee how much information these firms were collecting and, even if that was possible, to see what problems could arise from the emergence of these firms.

Public Attitude Turns Sour

Clearly, as the firms have grown in both breadth and depth, individuals, like Hoofnagle, and groups, like the Electronic Privacy Information Center, have been keeping a close-eye on and are now calling for, at least some, rules to govern these new-age firms. Hoofnagle points out a seemingly obvious, but still very important fact, that the sheer size and scope of what the data brokers are able to offer is largely unknown to many of the ordinary consumers whose information these firms buy and sell. He makes another strong point about the likely reaction of the American consumer, “When individuals understand the amount and detail in the information that these companies are selling, their attitudes are likely to sour.” Attitudes have soured, as

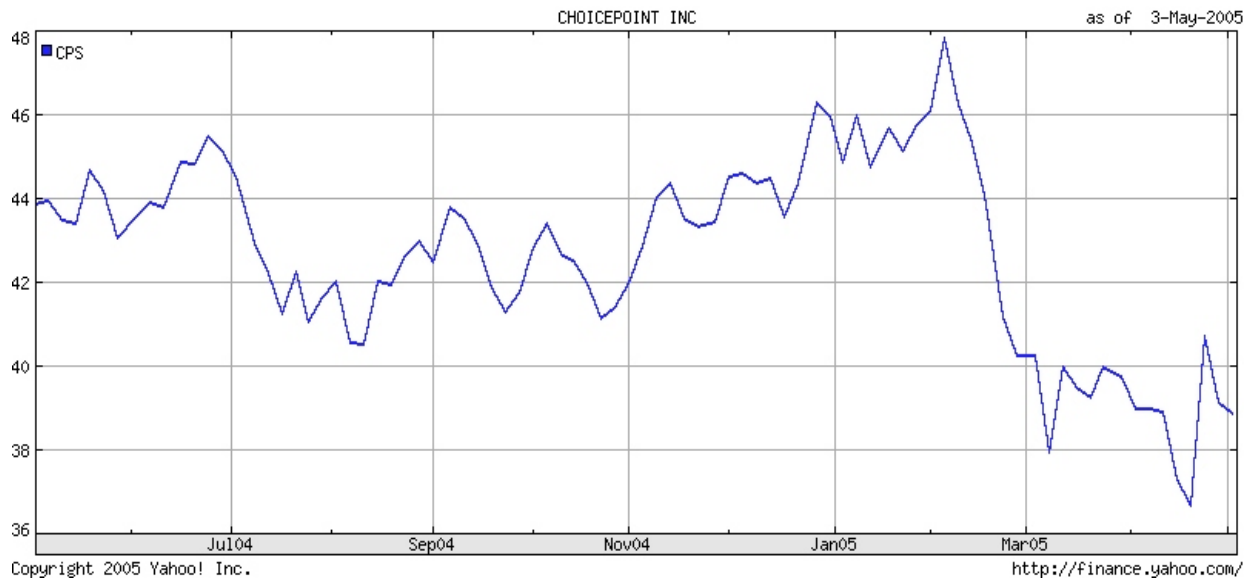
evidenced by a class-action lawsuit led by Eileen Goldberg, one of the recipients of the 34,000 letters ChoicePoint sent out to California residents on February 14th, 2005, and the increased pressure on legislators and regulators to take action concerning the data collection firms and the security breaches. ⁶

ChoicePoint as Poster Child

As Steve Harris, former Senior Vice President for Corporate Communication at General Motors noted, the data collection security breach is “not a ChoicePoint specific issue, it’s an industry issue”, but “ChoicePoint has become the poster child for the issue.”⁷ With the security breach and identity theft at ChoicePoint being covered tirelessly by the media, ChoicePoint faces difficult Corporate Communication issues moving forward convincing the public and regulators that increased security measures and new regulation will prevent such theft from happening again and that, in fact, massive data collection firms do bring more benefit to society than they do harm.

Stock Plummet

Prior to the public disclosure of the security breach, ChoicePoint shares were trading, on February 4th, at the company’s 52-week high of \$47.95. Following the release of the news of possible identity theft on February 14th, 2005, the stock plummeted over the next three weeks from \$45.49 on February 14th to \$37.97 on March 8th, a decline of nearly 17%.⁸ Fueled by the fact that at least 750 cases of identity theft were confirmed on February 14th and that, according to testimony from L.A. County Sheriff’s Department Detective Duane Decker, the personal information of as many as 4 million people could have been downloaded, this sharp decline indicates that ChoicePoint needs to act fast to reassure investors, the public, regulators, and all potential victims that the problem can be resolved and that the firm can rebound strongly from the problem that ChoicePoint spokesman James Lee says, “We never saw getting this big.”⁹



Didn't Know Until January

Another alarming issue for ChoicePoint as a whole, but also personally for executives Smith and Curling, concerns the millions in stock sales, specifically \$16 million in profits, made by the two executives in the three month period leading up to the public disclosure of the security breach. On October 26th, the day before the sting operation to catch Olatunji Oluwatosin, the only member of the identity theft ring caught to date, Smith and Curling cleared large prearranged stock sales with ChoicePoint directors.¹⁰ Set in motion shortly thereafter, the stock sale programs were set to last six months and would result in Smith selling up to 11% of his stake in the company and Curling 13% of his stake.¹¹ Halted in March, the two executive stock sale programs have come under very close investigation by the Securities and Exchange Commission. Millions of dollars of stock sales prior to the announcement of guaranteed negative news certainly provides grounds for investigation, although Smith has said that the two executives did not know about the October database breach until January. The SEC will certainly investigate Smith's claims in depth, and in the meantime, ChoicePoint's Corporate Communications team must be prepared to tackle the very probing, challenging questions that will inevitably come its way concerning the stock sales.

Corporate Communication Issues Moving Forward

ChoicePoint's Corporate Communication team has very complex issues lying ahead in dealing with an alarmed public, an outraged victims pool, a prying media, and a ready-to-act legislature. ChoicePoint is in the limelight and has every opportunity to turn all the negative occurrences into positive lessons learned that could solidify the firm's place and importance in American society.

On the other hand, ChoicePoint has every opportunity to lose complete control of the situation, make excuses, point fingers, and crash and burn in a corporate era filled by scandal, mistrust, and corporate malfeasance. ChoicePoint's future will be predicted by the ability of the firm's current and future Corporate Communications department to respond effectively and accurately to the many challenging questions ahead concerning the security breach, proper future legislation and regulation, internal security controls, executive stock sales, and future business strategy.

References

¹ Zeller Jr., Tom. "ChoicePoint Suffers Fall in Share Price," *The New York Times*. February 23, 2005.

² Holland, Jesse J. "Senate Panel to Discuss Identity Thefts," *Associated Press*, February 25, 2005.

³ Interview with Mark Noeldner, local banking professional in South Bend, IN and adjunct professor at the University of Notre Dame. April 22, 2005.

⁴ Perez, Evan and Rick Brooks. "For ChoicePoint, a theft lays bare the downside," *The Wall Street Journal*. May 3, 2005.

⁵ Zeller Jr., Tom. "ChoicePoint Suffers Fall in Share Price," *The New York Times*. February 24, 2005.

⁶ Zetter, Kim. "California Woman Sues ChoicePoint," *Wired*. February 24, 2005.

⁷ Interview with Steve Harris, former Vice President of Communications at General Motors Inc. April 11, 2005.

⁸ Yahoo! Finance. Historical Prices, CPS, ChoicePoint.

⁹ Interview with James Lee, Chief Marketing Officer at ChoicePoint Inc. April 18, 2005.

¹⁰ Sullivan, Bob. "Data Theft Affects 145,000 Nationwide" *MSNBC*. February 18, 2005.

¹¹ Perez, Evan and Rick Brooks. "For ChoicePoint, a theft lays bare the downside," *The Wall Street Journal*. May 3, 2005.