Order Code RS22137
Updated May 3, 2007



CRS Report for Congress

Data Brokers: Background and Industry Overview

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

Disclosures of breaches of the customer databases of LexisNexis and ChoicePoint have raised interest in the business and regulation of data brokers, companies that collect personal information from public and private records and sell this information to public and private sector entities. The growth of this industry has generally tracked the increase in government and private sector use of personal information. The vast amount of personal information that data brokers collect and the improper access to such data, however, have spurred concern as to the dangers of identity theft. Identity theft is reportedly the fastest growing crime in America. This report provides an overview of the data brokerage industry and more specific background on LexisNexis and ChoicePoint.

Introduction[1]

In the first few months of 2005, two leading data brokers, LexisNexis and ChoicePoint, announced that unauthorized individuals had breached their security measures and obtained personal information (e.g., Social Security numbers, addresses) about hundreds of thousands of individuals. These companies and others like them — so-called "data brokers" — operate largely free from federal and state regulation.[2] The recent scandals have led to calls for tighter regulation of the data brokerage industry, creating the need for more complete information on the types of businesses that make up this industry, and the types of services they provide. This report provides an overview of the industry and specific case studies of ChoicePoint and LexisNexis.

---

[1] This report was originally prepared by Nathan Brooks, Legislative Attorney.

[2] *See* CRS Report RL33005, *Information Brokers: Federal and State Laws*. In certain circumstances, laws restrict the collection and use of specific kinds of personal information. For example, the Gramm-Leach-Bliley Act regulates access to and use of consumer financial information under certain circumstances. 15 U.S.C. §§ 6801-6809.

The Data Brokerage Industry

Personal information for background checks is of course essential for employers and criminal investigators. Businesses that have been able to use the Internet to quickly provide such information have grown tremendously over the past several years, as the events of September 11, 2001, and the subsequent war on terror have put a premium on accurate identification of individuals in both the public and private sectors.[3] "Data brokers" — companies like ChoicePoint, LexisNexis, Axciom, Experian, US Search, and Information Search — have prospered by fulfilling this need.[4] Law enforcement, in particular, has found data brokers useful, as these private companies maintain and organize personal information on individuals in a manner that may not be legally available to government actors.[5] The Privacy Act, for example, requires federal agencies to limit the amount of information on American citizens that these agencies maintain and disseminate.[6] The Act establishes the principle that the government should "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs."[7]

Most data brokers sell data that they collect from public records (e.g., driver's license records, vehicle registration records, criminal records, voter registration records, property records, occupational licensing records) or from warranty cards, credit applications, etc.[8] In addition, data brokers purchase so-called "credit headers" from credit reporting agencies. Information on a credit header generally includes a person's name, Social Security number, address, phone numbers, and birth date.[9] While the release of certain information, such as data associated with a credit report, is subject to federal law, data brokers are largely free from state and federal regulation.[10]

---

[3] Title III of the USA PATRIOT Act (P.L. 107-56), for example, mandated "Know Your Customer" requirements — and stiff penalties for failing to comply — on a wide array of financial institutions. *See* CRS Report RL31208, *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, Title III of P.L. 107-56 (USA PATRIOT Act)*, by M. Maureen Murphy.

[4] *See* Robert O'Harrow, Jr., "In Age of Security, Firms Mine Wealth of Personal Data," *Washington Post*, January 20, 2005, at A1.

[5] For a discussion of how, in light of these limitations, agencies find data brokers useful, *see* Glenn R. Simpson, "FBI's Reliance on the Private Sector Has Raised Some Privacy Concerns," *Wall Street Journal*, April 13, 2001.

[6] 5 U.S.C. § 552a.

[7] 5 U.S.C. § 552a(e)(2).

[8] *See* Note, *The Internet: Privacy Lost, Identities Stolen*, by Stephanie Byers, 40 Brandeis L.J. 141, 144 (2001).

[9] *Id.*

[10] *See* Protecting Consumers' Data: Policy Issues Raised by Choicepoint: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce, 109th Congress, 1st sess. (2005).

Generally, companies or government agencies purchase from data brokers information about an individual — including his or her Social Security number.[11] The vast majority of these transactions are conducted via the Internet, rather than person-to-person.[12] Of course, the anonymity of most data brokerage transactions has opened the door for criminals to pose as legitimate businesses and obtain vital information about an individual — usually a Social Security number — and steal his or her identity. It has been reported in the past, for example, that identity thieves — using stolen credit card numbers — have obtained information about victims and transferred funds from the victims' accounts, written phony checks against those accounts, etc.[13] As the following case studies show, the danger of identity theft remains, despite the implementation of tighter safeguards by data brokers.

Case Studies: ChoicePoint and LexisNexis

While the growth of companies that gather and sell information has tracked the rise of personal computers since the early 1980's, two events led to the exponential growth of data brokerage firms since 2000: (1) The explosion of the Internet throughout the 1990's; and (2) the development by Florida-based programmer John Asher of parallel programming software allowing a researcher to use bits of information about an individual (e.g., name, Social Security number) to search several databases simultaneously and find more information about that person within seconds. Asher built two companies on this technology, and later sold the companies to ChoicePoint and LexisNexis, who have used the technology to become two of the most successful data brokers in the world.[14]

ChoicePoint. One of the largest and most profitable data brokers in the United States is Georgia-based ChoicePoint. ChoicePoint sells data to a wide variety of entities, from insurers to law enforcement.[15] Originally formed as a spin-off of credit reporting agency Equifax in 1997, ChoicePoint has grown to dominate the data brokerage market by purchasing a number of smaller, more specialized data brokers and operating several

---

[11] *See* United States Government Accountability Office, Report to Congressional Committees: Personal Information: Agency and Reseller Adherence to Key Privacy Principles, GAO-06-421 (April 4, 2006).

[12] For information on the Internet and identity theft generally, *see* CRS Report RS22082, *Identity Theft: The Internet Connection*, by Marcia S. Smith.

[13] *See, e.g.,* Robert O'Harrow, Jr., "Identity Thieves Thrive in Information Age," *Washington Post*, May 31, 2001, at A1 (recounting the story of Rita Johnson, who was the victim of identity theft. Criminals stole credit card statements and other documents containing personal information from Mrs. Johnson's mailbox. They used this information to pose as legitimate employers and obtain from data brokers various Social Security numbers, which the criminals then used to order more credit cards and raid bank accounts).

[14] *See* Stephen Pounds, *Identity Complex: Data Brokers Files Are Extensive, As Are Their Destinations*, Palm Beach Post, April 10, 2005.

[15] *See, e.g.,* Chris Jay Hoofnagle, *Big Brother's Little Helper: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. Int'l L. & Com. Reg. 595 (2004).

subsidiaries in various states.[16] ChoicePoint's total annual revenue has grown in this time period from $585 million in 2000 to over $1 billion in 2006.[17]

The products ChoicePoint offers reflect the sophistication in the data brokerage industry that demand and competition have created. ChoicePoint not only groups personal information together according to what type of background check is being conducted (e.g., pre-employment screenings) but also "Soundex" searches that allow customers to search for personal information based on how names sound, rather than how they are spelled.[18] In addition, ChoicePoint allows law enforcement to link suspects to former addresses, neighbors, etc.[19]

As mentioned above, the data brokerage industry has grown increasingly close to law enforcement and counterterrorism agencies in the last few years, and ChoicePoint's relationship with law enforcement and counterterrorism agencies is indicative of this fact.[20] ChoicePoint has multi-million dollar contracts with the Departments of Homeland Security and Justice, and the company maintains federal agency-specific websites to facilitate searches by officers from those agencies.[21]

Up until recently, ChoicePoint guarded access to its information by requiring customers to provide business records on file with government agencies, copies of drivers' licenses, and other information identifying customers as legitimate businesses. Unfortunately, at least one criminal ring began creating sham businesses and identities in order to get around these requirements, and a Los Angeles-based sting operation in 2004 uncovered evidence leading authorities to conclude that the ring had accessed ChoicePoint's information on roughly 145,000 people.[22] As the scandal unfolded, ChoicePoint drew heated criticism for refusing to notify many of those whose personal information had been accessed. At first, ChoicePoint only notified victims residing in California, as that is the only state with a law requiring such notification when personal information is compromised.[23] Only after a public outcry did ChoicePoint agree to notify victims outside of California.

---

[16] *Id.* at 602.

[17] Choicepoint 2006 Annual Report, found at [http://media.corporate-ir.net/media_files/irol/95/95293/reports/choicepoint_ar06.pdf] (last visited May 3, 2007).

[18] *See* Hoofnagle, *supra* note 15, at 601-602.

[19] *Id.* A complete list of Choicepoint's products and services can be found at [http://www.choicepoint.net/business/all/all_products.html] (Last visited May 3, 2007).

[20] *See, e.g.,* Glenn R. Simpson, "FBI's Reliance on the Private Sector Has Raised Some Privacy Concerns," *Wall Street Journal*, April 13, 2001.

[21] *See* United States Government Accountability Office, n. 11, *supra*, at 19-36.

[22] *See* Robert O'Harrow, Jr., "Choicepoint Data Cache Became a Powder Keg," *Washington Post*, March 5, 2005, at A1.

[23] Cal. Civ. Code §§ 1798.82, 1798.29. Similar legislation has been enacted in 35 states. *See* [http://www.ncsl.org/programs/lis/cip/priv/breach.htm] (Last visited May 3, 2007). *See also* CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens.

The Federal Trade Commission (FTC) brought a compliant for civil penalties, permanent injunction, and other equitable relief alleging that ChoicePoint did not have reasonable procedures to screen prospective subscribers, and turned over consumers' sensitive personal information to subscribers whose applications raised "red flags."[24] The FTC also alleged that ChoicePoint approved as customers individuals who lied about their credentials and used commercial mail drops as business addresses. In addition, according to the FTC, ChoicePoint applicants reportedly used fax machines at public commercial locations to send multiple applications for separate companies. The FTC charged that ChoicePoint violated the Fair Credit Reporting Act (FCRA) by furnishing consumer reports to subscribers who did not have a permissible purpose to obtain them, and by failing to maintain reasonable procedures to verify both their identities and how they intended to use the information.[25] The agency also charged that ChoicePoint violated the Federal Trade Commission Act by making false and misleading statements about its privacy policies.[26]

In 2006, ChoicePoint agreed to pay $10 million in civil penalties and $5 million in consumer redress to settle Federal Trade Commission charges that its security and record-handling procedures violated consumers' privacy rights and federal laws. The settlement requires ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional until 2026.[27]

LexisNexis. LexisNexis has been one of the leading information research engines for over two decades. In August, 2004, LexisNexis' parent company, London-based Reed Elsevier, purchased data broker Seisint (an Asher creation) for $775 million and made it a unit of LexisNexis. Among other things, Seisint provides data for Matrix, a crime and terrorism database that, until recently, was funded by the federal government.

Very soon after the ChoicePoint scandal, LexisNexis reported that unauthorized individuals had accessed the personal information of about 32,000 customers of the

---

[24] *U.S. v. ChoicePoint Inc*. Complaint, Civil No. 1:06-cv-00198-GET (N. D. Ga. 2006) at [http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf].

[25] 15 U.S.C. § 1681 *et seq.* Under the Fair Credit Reporting Act (FCRA), consumer reporting agencies have particular responsibilities with respect to ensuring that a consumer's information is used only for purposes that are permissible under the act, for protecting the consumer's information from potential identity thieves, and for correcting information in a consumer's report that may be incorrect or the result of fraud. The act and the requirements set forth therein only apply to entities that fall within the definition of a "consumer reporting agency," and only to products that fall within the definition of a "consumer report."

[26] 15 U.S.C. §§ 41-58. Under the FTC Act, the Federal Trade Commission is empowered, among other things, to prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce; and to seek monetary redress and other relief for conduct injurious to consumers.

[27] *U.S. v. ChoicePoint Inc*. (D. Ct. for the Northern District of Georgia, Atlanta Division), FTC File No. 052-3069 (January 26, 2006), available at [http://www.ftc.gov/opa/2006/01/choicepoint.htm].

company's data brokerage unit by entering in the passwords of legitimate customers.[28] A few weeks later, that estimate had risen to over 300,000.[29] These individuals somehow acquired passwords of paying customers of Seisint's "Acurint" service, which generally charges $4.50 for packaged information about an individual. Using the legitimate passwords, the hackers were able to access personal information ranging from social security numbers to home addresses to drivers' licenses numbers.

Conclusion

As the market for personal information has grown — particularly in light of the war on terror — so too has grown the data brokerage industry. The ChoicePoint and LexisNexis scandals, however, have spurred debate over the security of personal information collected and sold by data brokers.[30]

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

---

[28] El-Rashidi, Yasmine, *LexisNexis Reports Data Breach; Personal Records Are Hacked as Concerns About Security and Identity Theft Intensify*, *Wall Street Journal*, March 10, 2005, p. A3

[29] *See* Associated Press, *LexisNexis Theft Much Worse Than Thought*, April 12, 2005, found at [http://msnbc.msn.com/id/7475594/] (Last visited May 3, 2007).

[30] *See* CRS Report RL33273, *Data Security: Federal Legislative Approaches*, by Gina Marie Stevens.