

Regulating Commercial Data Brokers in the Wake of Recent Identity Theft Schemes

By Joshua Apfelroth

Introduction

TECHNOLOGY HAS INCREASED the ability of companies to compile and organize the personal information of individuals and organizations. Companies that market this type of personal information are often referred to as commercial data brokers (CDBs). Over the past year, the use of CDBs as a medium for criminals to obtain information for use in identity theft schemes has placed the security of these companies in the public spotlight. As a result of several high profile breaches in security, Congress is prepared to enact legislation to regulate the CDB industry, with the intention of tightening CDBs' privacy policies. Whereas Congress and CDBs agree that regulation of the industry is necessary, there is contention as to what type of legislation Congress should enact. While the CDB industry prefers legislation focusing mostly on punishing criminals who use their data to commit identity theft, many members of Congress believe that it is necessary to pass legislation that will regulate the manner by which CDBs collect and distribute information. Because of these competing interests, Congress is faced with the difficult task of regulating an industry that places consumers' identities at risk, while ensuring that the legislation they pass does not unduly burden CDBs' ability to provide important public benefits.

Identity Theft

THE TECHNOLOGICAL EXPLOSION of recent decades has resulted in the ability of CDBs to efficiently collect and organize the personal information of millions of Americans. This information ranges from general information, such as one's name, phone number and address, to specific information, such as the type of cars a person has owned, a person's credit history, and whether he or she has a criminal record.¹ Companies such as Choicepoint, Inc., Lexis-Nexis, Westlaw, Dun & Bradstreet and Experian, Inc. have made millions of dollars through the collection and sale of such personal information to individuals, businesses, and to local, state, and the federal government. The information is often packaged in ways that assist a particular industry or organization.² Some of the largest markets for these services are small businesses, the insurance industry, the financial industry, and law enforcement.³ The government also frequently uses this data to investigate crimes, make employment decisions and fight terror-

ism.⁴ Businesses, both large and small, access this information in order to screen new tenants, clients or employees.⁵

Unfortunately the services that CDBs provide are not always used for legitimate business means. There are people who use the CDBs' services as an intermediary to aid in identity theft schemes. Identity theft occurs when a person uses the identity of another in order to commit fraud.⁶ A type of identity theft frequently occurs when a person obtains the social security number of another and uses it to open new lines of credit, known as "tradelines."⁷ After opening a new tradeline under the guise of their victim, the identity thief can then obtain credit cards, wireless phone service, and utilities under the victim's name.⁸ Identity thieves also use their victims' information to engage in more complicated schemes. Such schemes include taking out an auto loan in a victim's name, filing bankruptcy to discharge debts incurred using the new identity, and obtaining a job and subsequently filing fraudulent tax returns under their victim's identity.⁹

"As a result of several high profile breaches in security, Congress is prepared to enact legislation to regulate the CDB industry, with the intention of tightening CDBs' privacy policies."

In 2003, a Federal Trade Commission (FTC) survey revealed that over a one year period, nearly ten million people discovered that they were victims of identity theft.¹⁰ In other words, 4.6% of the American adult population knowingly fell victim to identity theft.¹¹ This overwhelming statistic excludes those who are unaware that they are victims of identity theft; this is likely a large number considering the difficulty people have in detecting that they are victims of identity theft. These

crimes have translated into approximately \$48 billion in business losses, \$5 billion in losses to individuals, and nearly 300 million hours spent by victims trying to resolve the problem.¹²

Recent events at large CDBs, such as Choicepoint and Westlaw, accompanied by the overwhelming statistics stated above, have brought the issue of CDBs' role in identity theft to the forefront of the agenda of American politics, public policy organizations and citizens. As a result, Congress and consumer rights organizations are calling for stricter laws aimed towards defending the American public against identity theft.

What Type of Information Do CDBs Collect?

CDBs OBTAIN INFORMATION from many different sources. CDBs collect some information themselves and purchase other information. However, all of the information that CDBs gather can be classified under one of three categories: (1) Public Record Information, (2) Publicly-Available Information and (3) Non-Public Information. Public Record Information consists of that information which appears in public records,¹³ includ-



ing birth and death records, tax lien records, property records, court records, voter registrations and licensing records.¹⁴ Publicly-Available Information differs from Public Record Information in that Publicly-Available Information is unavailable in public records; it is publicly available through other public mediums, such as print publications, telephone directories, and Internet sites.¹⁵ The most controversial of the information that CDBs collect is Non-Public Information, which is usually pur-

chased from outside sources. Non-Public Information consists of identifying information, such as one's name, phone number, address, and social security number.¹⁶ Non-Public Information also includes a person's credit card number, magazine subscriptions, travel destinations and other records received during a person's business transaction.¹⁷ Finally, information gathered from a person's application for credit, employment or insurance application, and information obtained from an individual's website registration, contest or warranty is considered Non-Public Information.¹⁸

Events That Have Raised Questions About The Security of Information Held by CDBs

ONE OF THE MOST WELL KNOWN CASES of identity theft by thieves using fraudulently obtained personal records obtained through a CDB occurred in February 2005, at Choicepoint, Inc. One man led a ring of identity thieves and compromised more than 145,000 records.¹⁹ The ring obtained fraudulent business licenses and other fraudulent documents to open fifty accounts with Choicepoint. Ring members were able to pose as businesses seeking information about potential employees and customers. For over a year, the criminals had access to Choicepoint's collection of personal data, and for \$100 to \$200 per account, they were able to gain access to individuals' addresses, social security numbers and phone numbers.²⁰

Other incidents have also highlighted the need to ensure that personal information on computers is securely protected. In the past year, security breaches at LexisNexis, Westlaw, Bank of America, PayMaxx, T-Mobile, Science Applications International Corporation and George Mason University have put people at risk of identity theft.²¹

Current Laws In Place to Restrict the Sale of Personal Information

THERE IS NO SINGLE FEDERAL LAW that encompasses the sale of all consumer information. Instead, Congress passed industry-specific regulations governing the dissemination of personal information. Aside from scattered federal laws, limited state legislation exists to help minimize the risks associated with CDBs. As a result of this piecemeal legislation, CDBs have the ability to take advantage of the loopholes inherent in such legislation. The statutes already in place are too specific to ensure complete privacy of the records housed by CDBs. For example, the Fair Credit Reporting Act (FCRA) focuses on oversights of the credit reporting system and limits the sale of consumer information.²² The FCRA prohibits, with several listed exceptions, the distribution of "consumer reports" by "consumer reporting agencies" (CRA) except for "permissible purposes," while ensuring that the consumer reporting agencies make reasonable

efforts to verify the identity of prospective recipients.²³ Consumer reports are defined as reports that contain information that is gathered and sold to businesses to facilitate consumer-related decisions. The FCRA governs CDBs to the extent that the information they distribute constitutes a consumer report. To distribute “consumer reports,” a CRA must meet one of the permissible purposes set forth in the FCRA. Most relevant to the distribution of data by CDBs is that under the FCRA, reports may be provided for a business to make credit, insurance or employment decisions. Another loophole that CDBs may take advantage of is that CRAs/CDBs may also distribute consumer reports if the person or organization to whom such reports are being distributed has a legitimate business need.²⁴ The limiting nature of the term “consumer reports” and the substantial exceptions that the FCRA provides does not leave the public with much protection to ensure the proper dissemination of personal information by CDBs.²⁵

The Gramm-Leach-Bliley Act (GLBA), which Congress passed in 1999, limits the type of information that can be distributed by “financial institutions.”²⁶ The GLBA prohibits financial institutions from disclosing nonpublic personal information to non-affiliated third parties without first allowing consumers’ notice of the disclosure and an opportunity to opt-out of the disclosure.²⁷ CDBs are governed by the GLBA to the extent that they fall under the “financial institution” classification. However, there are exceptions under which a financial institution does not have to follow the notice guidelines of the GLBA. If the information is disclosed to a CDB pursuant to a GLBA exception, the CDB may only use this information “in the ordinary course of business to carry out the activity covered by the exception under which they received the information.”²⁸ Under a GLBA exception, CRAs and CDBs often receive what is called “credit header information” from financial institutions, consisting of a person’s name, address, and social security number.²⁹ Whether or not the CDB receives the information directly from the financial institution, or from a CRA who originally received the information from a financial institution, the CDB is subject to the limitations of the GLBA.³⁰

In 2003, California enacted the strongest of the state privacy laws. The California legislature enacted these privacy laws under circumstances similar to those Congress currently faces. In April, 2002, a hacker accessed California’s Stephen P. Teale’s Data Center, gaining access to the payroll information of 225,000 state employees. In early May, the State Controller’s Office discovered the security breach, but did not notify the employees until the end of May, leaving nearly a month for the hacker to misuse the information. In light of this security breach and the increasingly popular crime of identity theft, the California legislature passed the Security Breach Information Act (Act). As a result of the Act, all companies that do business

within the State of California must inform consumers whenever their personal data *may have been* compromised. Under this Act, if the company could prove that they provided protection prior to the public breach by encrypting the compromised information, then they are exempt from the notification requirement. If the company fails to secure personal data or notify consumers of a possible breach of security breach, the affected consumers can sue the company in civil court. The purpose of this legislation is to provide incentive for CDBs to strengthen their security to avoid incurring both the costs of notifying thousands of customers of potential breaches and the potential punishments mandated by the statute.

The FCRA, GLBA and the Security Breach Information Act provide protection to consumers against the distribution of specific personal information by certain industries. State laws, Section 5 of the FTC Act, the Driver’s Privacy Protection Act and the Health Information Portability and Accountability Act

“In 2003, a Federal Trade Commission (FTC) survey revealed that over a one year period, nearly ten million people discovered that they were victims of identity theft. In other words, 4.6% of the American adult population knowingly fell victim to identity theft.”

are other examples of such laws. While all of these laws may create obstacles for the CDBs to conduct business, none of them have been effective in preventing the erroneous distribution of people’s personal information to identity thieves.

Recommended Changes to Current Privacy Laws

CONGRESS MUST BALANCE the legitimate interests of CDBs with the public interest in regulating the distribution of private information. In finding a solution, it is important to look at the competing forces influencing the decisions of the legislature. First, there is the question of how much the legislature wants to interfere with the capitalist system. There is clearly a legitimate market for the distribution of personal information. Many companies, government agencies, and individuals use it for legitimate purposes. In fact, the information is often used to

protect the public from such dangers as terrorism and crime, as well as economic harm caused by deadbeat creditors. In addition, CDBs create jobs and income for a significant number of Americans. Regulation of the CDB market will certainly come at a price. Any regulatory barrier put in place that creates additional obstacles for CDBs to conduct business will increase the operating costs of CDBs.

Recently, the CEOs of Choicepoint and LexisNexis testified before the subcommittee of the U.S. House Energy and Commerce Committee regarding data security regulation. The two CEOs made it clear that, in addition to conforming to federal and state laws, CDBs often have internal privacy policies posted on their website. The CEOs' testimony outlined the companies' attempts at making their privacy policies more effective.

On March 17, 2005, LexisNexis revised its privacy policy, further restricting the full display of social security numbers and driver's license numbers.³¹ According to the revised policy, LexisNexis will not provide a full social security number to any client that does not fit into one of five categories; each category focuses on their company's services being used in law enforcement and the detection of fraud.³²

Choicepoint also revised its policies regarding the dissemination of certain types of information. Choicepoint exited the consumer sensitive data market not covered by the FCRA.³³ In other words, Choicepoint will not sell sensitive consumer data,

“There is no single federal law that encompasses the sale of all consumer information.”

including social security and driver's license numbers unless there is a specific consumer-driven transaction or benefit, or where the information supports federal, state or local criminal justice and government purposes.³⁴ Furthermore, Choicepoint now requires additional screening of their customers, using bank references and site visits to verify the credibility of small businesses before giving them personally identifiable information.³⁵ The company also created an Office of Credentialing, Compliance and Privacy, which reports to the Board of Directors Privacy Committee.³⁶ Lastly, Robert McConnell, a former member of the Secret Service and former chief of the Nigerian Organized Crime Task Force, was appointed to act as a liaison to law enforcement officials.³⁷

Aside from their revised internal privacy policies, these two CDB industry leaders have voiced support for certain regula-

tion of the CDB industry. Choicepoint stated in the hearings that it would strongly support the increasing of criminal penalties against identity thieves.³⁸ On top of that, Choicepoint also stated that it would endorse a “single, reasonable, nationwide mandatory notification requirement of any unauthorized access to personally identifiable information.”³⁹ LexisNexis stated that it too would support harsher penalties for identity thieves and a mandatory notification requirement. While LexisNexis did not offer support for a mandatory notification statute, it added that they do support legislation that would impose data security



modeled after the GLBA.⁴⁰ This GLBA-type data security regulation would be a significant and potentially costly change for the predominantly unregulated industry.

Naturally, LexisNexis and Choicepoint are concerned with the economic effect any new legislation will have on the industry. LexisNexis and Choicepoint supplemented their testimony with statements that maintained their desire for reasonable and efficient regulations that do not hamper the ability of CDBs to provide the legitimate benefits of their services. In his testimony, Kurt Sanford, President and Chief Executive Officer for Corporate and Federal Markets at LexisNexis stated:

[I]t is critical that any legislation being considered ensure that legitimate businesses, government agencies and other organizations continue to have access

to identifying information that they depend on for important purposes, including fraud detection and prevention, law enforcement and other applications...legislation must strike the right balance between protecting privacy and ensuring continued access to critically important information....⁴¹

Despite CDBs strengthening their privacy policies in the wake of recent security breaches, many Congressmen have still expressed concerns about the protection of consumer personal information.

Senator Nelson of Florida introduced a bill regarding CDB regulation entitled The Information Protection and Security Act.⁴² This bill calls for FTC regulation of CDBs in order to protect the rights of consumers and to ensure fair competition amongst CDBs.⁴³ The proposed legislation will call upon the FTC to: (1) promulgate rules that would require CDBs to authenticate users before allowing access to personally identifiable information; (2) ensure that CDBs have procedures in place to guarantee the maximum accuracy of their information; and (3) allow consumers the right to check on the

“Any regulation of an industry is costly; therefore, the more oversight and the less flexibility members of an industry have, the more the companies will have to spend on compliance with the regulations.”

information obtained by the CDBs to correct errors.⁴⁴

On the same day, Representative Stearns, a Republican of Florida, proposed a bill that would require CDBs to: (1) give notice of their privacy policies to the public; (2) allow consumers the opportunity to limit the sale or disclosure of their information; and (3) compel CDBs to prepare a policy that is designed to prevent the unauthorized disclosure or release of personally identifiable information.⁴⁵ This bill calls for more self-regulation by CDBs; however, CDBs' implementations of new policies would be subject to FTC approval.⁴⁶

Aside from the already proposed bills, Senator Feinstein of California will likely take this opportunity to push her Notification of Risk to Personal Data Act, which would require businesses and government agencies to notify victims whose information was likely obtained by criminals.⁴⁷ Senator Corzine

of New Jersey also expressed concern with the lack of legislation aimed at preventing the careless distribution of personal identifying information.⁴⁸ Senator Corzine's recent statement during a hearing of the U.S. Senate Committee on Banking, Housing and Urban Affairs mapped out his upcoming bill, the Identity Theft Prevention and Victim Notification and Assistance Act (IPVNA). Similar to Senator Nelson's and Congressman Stearns' bills, Senator Corzine's bill would appoint the FTC as the primary regulator of CDBs.⁴⁹ IPVNA would also authorize the FTC to write rules regarding the accuracy and security of collected information and to consider extending the requirements of the FCRA and GLBA to CDBs.⁵⁰ In addition to the preventative measures being proposed by Senator Corzine, the bill would also call for civil actions against CDBs that do not comply with the Act and would also incorporate Senator Feinstein's proposed notification requirement.⁵¹

Industry Concerns Regarding Regulation

IN 1999, THE CATO INSTITUTE argued against the implementation of California privacy rules requiring CDBs to satisfy elaborate notice and consent laws in the distribution of consumer data.⁵² Federal legislation proposed by several members of Congress would mandate the elaborate notice and consent requirements that the CATO Institute opposed. CATO Institute argued that such elaborate laws would hurt commerce, because they impede the ability of small businesses to compete with larger competitors.⁵³ While large businesses can often see and speak to their customers, resulting in their ability to know their customers' desires, small and internet businesses often never meet their customers. Regulations that hinder small and internet businesses from researching their markets will have a harmful impact on these businesses.

The CATO Institute argues that in the long run, consumers and the economy benefit when businesses acquire information that is specifically directed to their market.⁵⁴ The ability of companies to receive marketing information tailored to their preferences will reduce the cost of market research and customer solicitation through random mass mailings and advertising.⁵⁵ This reduction in marketing costs will pass through to the consumer. In turn, the cheaper these companies can sell their goods, the more they can compete with larger business, driving down the price of goods even more. The CATO Institute argues that unimpeded access to consumer data has the effect of balancing out the inherent unfairness small businesses are subject to when competing with large businesses.⁵⁶ This, in turn, will stimulate commerce by driving down the price of goods.

Arguments like those presented by the CATO Institute are not uncommon, and there are many who highlight the benefits that CDBs provide to the public. Other concerns of CDBs and their supporters center around the cost to the industry of any

imposed regulations on the industry. In 2001, Robert Hahn, director of the American Enterprise Institute - Brookings Joint Center for Regulatory Studies reported in a study that expansive privacy legislation would cost businesses between \$9 billion and \$36 billion.⁵⁷ On a smaller scale, Hahn estimated that companies will have to spend \$100,000 each in order to comply with privacy regulations.⁵⁸ In obtaining his final statistics, the author's research revealed that only an estimated 10% of targeted businesses will make the investments in complying with the laws; the other businesses would stop collecting and distributing personal information.⁵⁹ The notification requirement that several Congressmen are proposing on the federal level will also have economic effects on CDBs. Aside from the costs compa-



nies will incur in implementing preventative security measures, the notifying of those whose personal information may have been compromised has a price tag. For instance, when hackers broke into the San Diego State University servers, the university was required to notify 207,000 students of the breach at a cost of \$200,000.⁶⁰

Conclusion

Proposed legislation and testimony from two major CDBs illustrate the opposing viewpoints concerning what should be done to prevent identity theft resulting from CDB data collection and distribution. The CDB industry realizes that privacy

laws are necessary; however, to what extent oversight is necessary is a point of contention. Congress must decide whether the FTC should have an affirmative role in determining the way CDBs administer security policies, or whether CDBs should be given the discretion to perform self-regulation subject to FTC approval. Congress must also decide whether it is appropriate to focus on the prevention of security breaches or how to remedy the security breaches once they occur. Finally, Congress must resolve whether to focus on punishing the criminal who fraudulently obtains the information from the CDB and/or the CDB that fails to provide the proper security to the consumers whose data it collects. Any regulation of an industry is costly; therefore, the more oversight and the less flexibility members of an industry have, the more companies will have to spend on compliance with the regulations. All of these concerns must be addressed with a general goal in mind: how can Congress protect consumers from a lack of security at CDBs, while not imposing too strongly upon the legitimate services that CDBs provide?

BLB

Joshua Apfelroth is a third year JD candidate at American University, Washington College of Law. Mr. Apfelroth received his undergraduate degree from American University and is an Articles Editor on the Administrative Law Review. Mr. Apfelroth would like to thank Maya Grassi for her hard work in assisting with this piece. He would also like to acknowledge the support and encouragement received from his parents, Bruce and Debby Apfelroth. Mr. Apfelroth intends to pursue a career in commercial litigation.

ENDNOTES: *Joshua Apfelroth*

¹ Chris J. Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595 (Summer 2004).

² *Id.*

³ *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information Before the Comm. on Banking, Hous. & Urban Affairs*, 109th Cong. 2 (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission) [hereinafter *Recent Developments*].

⁴ *Id.*

⁵ *Id.*

⁶ *Identity Theft: Prevention and Victim Assistance Before the Subcomm. on Oversight & Investigations of the House Comm. on Energy & Commerce*, 107th Cong. 3 (2003) (statement of Betsy Broder, Assistant Director of the Division of Planning and Information, Bureau of Consumer Protection, Federal Trade Commission) [hereinafter *Prevention and Assistance*].

⁷ Federal Trade Commission, TAKE CHARGE: FIGHTING BACK AGAINST IDENTITY THEFT, available at <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#How> (last visited August 30, 2005)

⁸ *Id.*

⁹ *Id.*

¹⁰ *Prevention and Assistance*, *supra* note 6, at 3.

¹¹ *Id.*

¹² *Id.*

¹³ *Recent Developments*, *supra* note 6, at 3-4.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ Robert O'Harrow, Jr., *ChoicePoint Data Cache Became a Powder Keg: Identity Thief's Ability to Get Information Puts Hear on Firm*, WASH. POST, Mar. 5, 2005, at A01.

²⁰ Evan Perez, *ChoicePoint is Pressed to Explain Database Breach*, WALL ST. J., Feb. 25, 2005, at A8.

²¹ Declan McCullagh, 'Perfect Storm' for New Privacy Laws?, TECHREPUBLIC, Mar. 1, 2005, at http://techrepublic.com.com/5100-22_11-5594192.html (last visited September 10, 2005).

²² 15 U.S.C. § 1681; Hoofnagle, *supra* note 1, at 11; *Recent Developments*, *supra* note 3, at 7-11.

²³ 15 U.S.C. § 1681; Hoofnagle, *supra* note 1, at 11; *Recent Developments*, *supra* note 3, at 7-11.

²⁴ See *Recent Developments*, *supra* note 3, at 8 (stating that making unsolicited phone calls or mailings based on a consumer report is not usually noted as a "legitimate business need").

²⁵ 15 U.S.C. § 1681; Hoofnagle, *supra* note 1, at 11; *Recent Developments*, *supra* note 3, at 7-11.

²⁶ 15 U.S.C. §§ 6801-09; Hoofnagle, *supra* note 1, at 11-12; *Recent Developments*, *supra* note 3, at 11-13.

²⁷ 15 U.S.C. §§ 6801-09; Hoofnagle, *supra* note 1, at 11-12; *Recent Developments*, *supra* note 3, at 11-13.

²⁸ 15 U.S.C. §§ 6801-09; Hoofnagle, *supra* note 1, at 11-12; *Recent Developments*, *supra* note 3, at 11-13.

²⁹ 15 U.S.C. §§ 6801-09; Hoofnagle, *supra* note 1, at 11-12; *Recent Developments*, *supra* note 3, at 11-13.

³⁰ 15 U.S.C. §§ 6801-09; Hoofnagle, *supra* note 1, at 11-12; *Recent Developments*, *supra* note 3, at 11-13.

³¹ LexisNexis, *LexisNexis Data Privacy Policy*, March 17, 2005.

³² *Id.*

³³ *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint Before the Subcomm. on Commerce, Trade and Consumer Protection of the House Energy &*

Commerce Committee, 109th Cong. 2-5 (2005) (statement of Derek Smith, Chairman and CEO, ChoicePoint, Inc.).

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.* at 3.

³⁷ *Id.* at 4.

³⁸ *Id.* at 9-10.

³⁹ *Id.*

⁴⁰ *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint Before the Subcomm. on Commerce, Trade and Consumer Protection of the House Energy and Commerce Committee*, 109th Cong. 10-12 (2005) (statement of Kurt P. Sanford, President and CEO, U.S. Corporate and Federal Government Markets, LexisNexs).

⁴¹ *Id.* at 12.

⁴² Information Protection & Security Act (Introduced in Senate), S. 500, 109th Cong. (1st Sess. 2005).

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ Consumer Privacy Protection Act of 2005 (Introduced in House), H.R. 1263, 109th Cong. (1st Sess. 2005).

⁴⁶ *Id.*

⁴⁷ Tom Zeller, Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005 at C1.

⁴⁸ *Recent Developments*, *supra* note 3 (statement of Senator John S. Corzine).

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² Solveig Singleton, CATO Institute, *How Privacy Regulation Will Chill Commerce* (Dec. 13, 1999), available at <http://www.cato.org/dailys/12-13-99.html> (last visited August 25, 2005).

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ Jane Black, *What Price Privacy?*, BUSINESS WEEK ONLINE, June 7, 2001, available at http://www.businessweek.com/bwdaily/dnflash/jun2001/nf2001067_517.htm (last visited August 30, 2005).

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ *Id.*