INFORMATIONAL PRIVACY V. THE COMMERCIAL SPEECH DOCTRINE: CAN THE GRAMM-LEACH-BLILEY ACT PROVIDE ADEQUATE PRIVACY PROTECTION?

Julia C. Schiller

I. INTRODUCTION

For most Americans today, bank accounts, credit cards, and insurance policies are necessities. When an individual applies for one of these items, it is necessary to provide a great deal of information to these institutions.[1] The information ranges from the individual's name, address, telephone number, and Social Security number to, in some circumstances, income and medical history.[2] What that individual does not realize, if she did not read the financial institutions' privacy policy very closely, is that these institutions may share or sell that information to telemarketers and profiling companies.[3] The individual who wishes to have a bank account may therefore be, in effect, required to trade her privacy in order to obtain the necessary services.[4]

This paper examines the development of privacy and the new threats to informational privacy created by new technologies and computers that aid in the collection and dissemination of information. Part III examines the Financial Services Modernization Act and the privacy regulations established therein. This paper considers whether the Act is effective in protecting consumers' confidential financial information from misuse. The sharing of an individual's confidential information by financial institutions is commercial speech. Part IV defines the commercial speech doctrine and argues that Congress can, and should, go further to protect the privacy and confidentiality of an individual's personal information under the Financial Services Modernization Act without violating the First Amendment's commercial speech doctrine.

II. THE STATUS OF PRIVACY

The concept of privacy has been reflected throughout American history. Over one hundred years ago, in 1890, Samuel Warren and Louis Brandeis first identified the right to privacy as "the right to be let alone."[5] Central to this concept of privacy is autonomy, the ability to define and express oneself.[6] Eric Jorstad commented that privacy involved the power to welcome and exclude others at will.[7] For example, "Whom do you welcome in your kitchen? In your bedroom? In the c: drive of your computer?"[8] A failure to recognize privacy could mean that, "what is whispered in the closet shall be proclaimed from the house-tops."[9]

---

1 Brandon McKelvey, *Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure From the Threat of Identity Theft*, U.C. DAVIS L. REV. 1077, 1078 (2001) [hereinafter McKelvey].

2 *See* Jane Bryant Quinn, *Your Money is Safer Than Your Privacy*, WASH. POST, July 22, 1999, *at* http://www.washingtonpost.com/wp-srv/business/longterm/quinn/columns/072299.htm (last visited Feb. 1, 2003) [hereinafter Quinn, *Money is Safer Than Your Privacy*]; *see also* McKelvey, *supra* note 1, at 1078.

3 Jane Bryant Quinn, *New Privacy Law Gives Consumers 'Opt Out' Rights*, WASH. POST, May 15, 2001, *at* http://www.washingtonpost.com/wp-srv/business/longterm/quinn/columns/051501.htm (last visited Feb. 1, 2003) [hereinafter Quinn, *Opt Out Rights*].

4 Beth Givens, *Financial Privacy: The Shortcomings of the Federal Financial Services Modernization Act*, Presentation before the California Bar Association, Sept. 15, 2000, *at* http://www.privacyrights.org/ar/fin_privacy.htm (last visited Feb. 1, 2003) [hereinafter Givens].

5 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) [hereinafter Warren & Brandeis].

6 Eric Jorstad, *The Privacy Paradox*, 27 WM. MITCHELL L. REV. 1503, 1505 (2001) [hereinafter Jorstad].

7 *Id.*

8 *Id.*

9 Warren & Brandeis, *supra* note 5, at 193-95.

A. The Right of Privacy

Soon after Warren and Brandeis' ideas started to spread, courts began to react to the idea of privacy. In 1905, *Pavesich v. New England Life Insurance Co.* became the first case to recognize privacy as an independent right.[10] Since then, almost every state has taken steps to protect the right to privacy through various provisions in the United States Constitution.[11]

The United States Supreme Court has held that the liberty rights within the Constitution provide a basis for protecting privacy.[12] The landmark case of *Griswold v. Connecticut*[13] held that marital relationships lie within "a zone of privacy created by several fundamental constitutional guarantees."[14] In *Roe v. Wade*, the Supreme Court held that the right to privacy extended to a woman's decision whether or not to terminate her pregnancy.[15] The right of decisional privacy has since been extended to marriage,[16] contraception,[17] family relationships,[18] and education.[19]

Constitutional privacy has also embraced the sanctity of the home through the Fourth Amendment, which has been interpreted to mean that individuals have a right to be free from unreasonable searches and seizures.[20] The Supreme Court, in *Frisby v. Schulz*, recognized that the privacy of the home is "of the highest order in a free and civilized society."[21]

Throughout the historical development of the right of privacy, the Supreme Court has found three categories of privacy that the majority of cases have fit into: (1) decisional privacy, (2) physical privacy, and (3) informational privacy.[22] Decisional privacy encompasses the ability of an individual to make decisions independently and act free from intervention or regulation.[23] Physical privacy is tied to the Fourth Amendment's guarantee to be free from unreasonable searches and seizures.[24] In 2002, with the massive amounts of data collected about an individual's transactions on a daily basis, it is an individual's informational privacy that is at great risk.[25] According to Eugene Volokh, a UCLA law professor, informational privacy is, "my right to control your communication of personally identifiable information about me."[26]

B. Informational Privacy

The right to informational privacy was first ad-

---

[10] 122 Ga. 190, 214, 50 S.E. 68, 78 (1905) (finding that the use of an individual's name and picture in an advertisement was an invasion of privacy).

[11] Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1405 (1987) [hereinafter Graham].

[12] Carey v. Population Servs. Int'l, 431 U.S. 678, 683 (1977) (noting that one aspect of liberty is the right to personal privacy); Mike Hatch, *Electronic Commerce in the 21st Century: The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1463 (2001) [hereinafter Hatch].

[13] 381 U.S. 479 (1965) (invalidating a state law prohibiting the use and dissemination of information about the use of contraceptives).

[14] *Id.* at 485.

[15] Roe v. Wade, 410 U.S. 113, 153 (1973).

> This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.

Id.

[16] *See generally* Loving v. Virginia, 388 U.S. 1 (1967) (holding that statutes adopted to prevent marriage solely on the basis of racial classification violated the equal protection and due process clause of the Fourteenth Amendment).

[17] Eisenstadt v. Baird, 405 U.S. 438 (1972) (holding that statutes permitting married individual to obtain contraceptives to prevent pregnancy but prohibiting single people from obtaining them for the same purpose violated the equal protection clause).

[18] Prince v. Massachusetts, 321 U.S. 158, 166 (1944) (finding that there is a private realm of family life which the state cannot enter).

[19] Pierce v. Soc'y of Sisters, 268 U.S. 510, 535 (1925) (finding that parents and guardians have the right and duty to direct the upbringing and education of the children under their control to prepare children for additional obligations).

[20] U.S. CONST. amend. IV; *see also* Katz v. United States, 389 U.S. 347, 353 (1967) (finding that the Fourth Amendment protects not only places, but people from unreasonable search and seizure); Hatch, *supra* note 12, at 1463.

[21] Frisby v. Schulz, 487 U.S. 474, 484 (1988).

[22] *See generally* John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns-Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97 (1997) (providing background and historical information about the development of privacy in the United States).

[23] Thomas B. Kearns, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 979 (1999).

[24] *Id.* at 979-82.

[25] *See, e.g.*, Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153 (1997) (providing background information on how privacy may be invaded through the use of technology, such as the Internet).

[26] Eugene Volkh, *Freedom of Speech and information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1050-51 (2000).

dressed by the Supreme Court in *Whalen v. Roe*.[27] In *Whalen*, the plaintiff claimed invasion of privacy by a statute that required pharmacists and doctors to report prescriptions of drugs that were known to be abused.[28] These prescription reports were collected and stored in a centralized computer file.[29] The Court upheld the statute, finding that it was a legitimate exercise of the state's police power to control the distribution of potentially dangerous drugs.[30] The Court did, however state:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.[31]

Four months after *Whalen*, the Supreme Court addressed informational privacy in *Nixon v. Administrator of General Services*.[32] President Richard Nixon challenged, as violating his privacy, the Presidential Recordings and Materials Preservation Act, which allowed archivists to review and classify presidential papers and return those that were determined to be of a personal nature to Mr. Nixon.[33] The Court concluded that Mr. Nixon's privacy claim was weak, the public's interest in disclosure was strong, and that there were safeguards against abuse built into the Presidential Recordings and Materials Preservation Act.[34]

Despite the fact that the statutes in question were upheld, the majority of cases have interpreted *Whalen* and *Nixon* as supporting the proposition that there is a right to informational privacy.[35] The concept of privacy centers around the notion of protecting an individual's right to define one's self.[36] Central to the creation of one's identity, there is an inward and outward focus of personhood.[37] According to one commentator, Francis Chlapowski, "The inward focus of personhood is concerned with activities or decisions that affect only the actor. The outward focus of personhood. . . . is concerned with the individual identity which the world perceives."[38] When private information is not afforded protection and is disseminated publicly, it may shape the social identity of the individual, and thus have an impact on the actual identity the individual develops.[39] It is therefore necessary to allow an individual to control the dissemination of information about one's self.

C. Computers and Privacy

Computers have enhanced the ability of individuals and companies to collect, store, organize, and disseminate information rapidly and with great ease. The government and the private sector use computers to collect personal information.[40] Computers have created new ways to combine information, thus enabling the companies to create profiles of almost every individual.[41] These profiles are easily transferable from one person or company to another and have become valuable commodities.[42]

1. Profiling

Computers and sophisticated software enable computer operators who have "access to two or more databases to identify people on both files, discard duplicative information, and combine the rest to create a more informative entry."[43] These large databases allow companies to discover attitudes and interests of individuals to aid targeting advertisements.[44]

In addition, the development of the Internet

---

27 429 U.S. 589 (1977).

28 *Id.* at 591-93. The drugs included amphetamines, cocaine, methadone, methaqualone, and opium. *Id.* at 593 n.8.

29 *Id.* at 591-93.

30 *Id.* at 596-605.

31 *Id.* at 605.

32 433 U.S. 425 (1977).

33 *Id.* at 429.

34 *Id.* at 465.

35 *See generally* Francis S. Chlapowski, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. Rev. 133, 149 (1991) (discussing the development of informational privacy through Whalen) [hereinafter Chlapowski].

36 *See* Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. Ill. U. L. Rev. 479 (1990) (providing a thorough review of the development of the right to informational privacy and its current status under the law).

37 Chlapowski, *supra* note 35, at 151.

38 *Id.*

39 *Id.* at 154. Informational privacy is an element of personhood and is an essential element of an individual's identity. The disseminations of personal information takes the opportunity away from individuals to define themselves. *Id.*

40 Graham, *supra* note 11, at 1395.

41 *Id.* at 1402.

42 Chlapowski, *supra* note 35, at 158 (arguing that the right to control personal information should be controlled by the individual as property and should not be bought and sold on the market).

43 Graham, *supra* note 11, at 1400-01.

44 *Id.* at 1401. Computers are used to remember names,

has made an even greater amount of information available. The Internet invades privacy in very subtle ways that the individual user may not even be aware of.[45] In a study on Internet privacy, the Federal Trade Commission ("FTC") determined that as an individual begins to browse the Internet, companies begin to gather information about them through "registration pages, user surveys, and online contests, application forms, and order forms."[46] These methods are considered to be acceptable methods of gathering information because they require the active participation of the user.[47] However, there are also a variety of methods of collecting data that the user is not even aware of, such as the use of "cookies."[48]

The FTC defines a "cookie" as technology that "allows a Web site's server to place information about consumer's visits to the site on the consumer's computer in a text file that only the Web site's server can read."[49] This enables a Web site to assign a unique identifier to the user to recognize the same user on a subsequent visit.[50] Cookies pose a number of privacy concerns. First, once the cookie on a hard drive is accessed, it reveals a list of the Web sites the user has visited within a specified period of time.[51] This list may contain the personal information the user entered while visiting a previous site, such as passwords, e-mail addresses, or purchases made.[52] Second, many cookies have the ability to determine the exact location of the computer being used.[53] Companies are thus able to send the users offers and advertisements based upon the collection of cookie information about the user's interests.[54]

The use of the Internet and cookies has led to a rise in on-line profiling, which is "the practice of collecting information about consumers' interests, gathered primarily by tracking their movements online, and using the resulting consumer profiles to create targeted advertising on web sites."[55] The focus of the companies engaged in on-line profiling is to gather as much information as possible about individuals to target consumers and aid in personal marketing.[56]

When this personal information is used properly it has the ability to aid consumers' experiences. Consumers may receive valuable discounts on products that they usually purchase,[57] and companies may save time and money by offering products and services only to consumers who are truly interested.[58]

The concern over profiling centers around the unknown factor of who is following an individual's transactional records and sharing this information without any consent from the individual involved.[59] The knowledge that every transaction made could provide an unknown person with a partial picture into their private life is unsettling. According to Minnesota Attorney General Mike Hatch, "These pieces of information, when layered on top of one another, create a complete picture of each individual."[60]

The information obtained through computer databases and on-line profiling is not confined to merely demographic data. In 1999, *Forbes Magazine* ran a story in which one of its reporters, Adam Penenberg, challenged a Web detective agent, Dan Cohn, to investigate him. In the course of six days:

> he was able to uncover the innermost details of my life – whom I call late at night; how much money I have in the bank; my salary and rent. He even got my unlisted phone numbers, both of them. . . . . America, the country that made "right to privacy" a credo, has lost its privacy to the computer.[61]

---

ages, attitudes, and interests and opinions and try to predict customer buying behavior. *Id.*

45 Rachel K. Zimmerman, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty First Century*, 4 N.Y.U. J. LEGIS. & PUB. POL'Y 439, 441 (2000-2001) [hereinafter Zimmerman].

46 Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, *at* http://www.ftc.gov/reports/privacy3/toc.htm (last visited Jan. 21, 2002) [hereinafter *1998 Privacy Report*].

47 *Id.*

48 Zimmerman, *supra* note 45, at 442.

49 1998 Privacy Report, *supra* note 46, at n.4.

50 *Id.*

51 Zimmerman, *supra* note 45, at 443.

52 *Id.*

53 *Id.* at 443-44.

54 Privacy Rights Clearinghouse, *Privacy in Cyberspace: Rules of the Road for the Information Superhighway*, *at* http://www.privacyrights.org/fs/fs18-cyb.htm (last modified July 2002).

55 Scott Foster, *Online Profiling Is on the Rise: How Long Until the United States and the European Union Lose Patience With Self-Regulation?*, 41 SANTA CLARA L. REV. 255, 258 (2000) [hereinafter Foster].

56 *See* Hatch, *supra* note 12, at 1471; *see also* Lynie Arden, *Privacy Fears Online*, eRef.net, *at* http://www.eref.net/privacy/features/fears_online.asp (last visited Feb. 1, 2003) [hereinafter Arden].

57 Hatch, *supra* note 12, at 1474.

58 Foster, *supra* note 55, at 262-63.

59 *Id.* at 262.

60 Hatch, *supra* note 12, at 1471.

61 Adam L. Penenberg, *The End of Privacy*, FORBES, Nov.

This investigation also revealed that private information is available for sale to anyone for a very small price: an unlisted phone number for forty-nine dollars; a Social Security number for forty-nine dollars; a bank balance for forty-five dollars; a driving record for thirty-five dollars; tracing a cell phone number for eighty-four dollars.[62] This information may be used for valid, unobjectionable purposes, such as verifying employment, but this information may also be used for improper purposes.

2. *The Rise of Identity Theft*

Identity theft is among the "fastest growing financial crimes" in America[63] with more than 500,000 victims each year.[64] Identity theft occurs "when an individual appropriates another's name, address, Social Security number, or other identifying information to commit fraud."[65] It is very easy for criminals to obtain personal information. In public places, identity thieves may watch you at the automatic teller machine ("ATM") as you punch in the personal identification number or they may listen to telephone conversations for a credit card number.[66] Some identity thieves may even go through the trash to obtain records that reveal your name, address, and telephone number.[67] They may also simply intercept your mail if it is kept in a location that is readily available to the public.[68]

The increased use of computers has enabled the Internet to become a valuable source for identity thieves.[69] The Internet is a tool that has made it easier and cheaper to access data on just about anyone.[70] Not only can identity thieves use the Internet to obtain personal information about individuals, it is also possible to use the Internet to perpetrate the fraud with little risk of detection because the thief is never seen.[71] Once they have obtained an individual's name and credit card number, they can make use of it through on-line shopping.[72] The identity thief is not seen; they do not have to be verified; and they do not have to sign anything.[73]

Credit bureaus, the computerization of public records, and information brokers have also made it easier to obtain personal information. Credit bureaus provide credit reports, often including one's name, birth date, Social Security number, address, credit accounts and other public record information to credit grantors in an effort to help in determining whether to approve a loan.[74]

3. *Public Records*

Computerization of government public records has made information easier to access. Many states consider driver's licensing files to be public records.[75] Driving records generally contain the individual's full name, birth date, and address. Some states even use an individual's Social Security number as the license number.[76] In addition, voter registration, property records, and many court records are readily available. Beth Givens, director of the Privacy Rights Clearinghouse, has explained that, "[w]hen bits and pieces of information are gathered from several sources, the brevity of some of those pieces can be misleading."[77] When compiling the bits and pieces of in-

29, 1999, at 182.

62 *Id.*

63 Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 89 (2001).

64 Identity Theft and Pretext Calling, OCC Advisory Letter, AL 2001-4, (Apr. 30, 2001) [hereinafter OCC Advisory Letter].

65 FEDERAL TRADE COMMISSION, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON "IDENTITY THEFT" BEFORE THE SUBCOMMITTEE ON TECHNOLOGY, TERRORISM AND GOVERNMENT INFORMATION OF THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE, May 20, 1998, *at* http://www.ftc.gov/os/1998/9805/identhef.htm (last visited Jan. 12, 2002) [hereinafter STATEMENT OF THE FTC ON "IDENTITY THEFT"].

66 Ruby Bayan, *Avoiding Identity Theft*, eRef.net, *at* http://www.eref.net/privacy/fact_sheets/avoiding_identity_theft.asp (last visited Feb. 1, 2003) [hereinafter Bayan]; DEPARTMENT OF JUSTICE, IDENTITY THEFT AND FRAUD, *at* http://www.usdoj.gov/criminal/fraud/idtheft.html (last visited Feb. 1, 2003) [hereinafter DEPARTMENT OF JUSTICE].

67 Bayan *supra* note 66; DEPARTMENT OF JUSTICE *supra* note 66.

68 DEPARTMENT OF JUSTICE, *supra* note 66.

69 *Id.*

70 Arden, *supra* note 56.

71 Robert O'Harrow Jr., *Identity Thieves Thrive in Information Age, at* http://www.washtech.com, May 31, 2001 [hereinafter O'Harrow].

72 *Id.*

73 *Id.*

74 Stephanie Byers, *The Internet: Privacy Lost, Identities Stolen*, 40 BRANDEIS L.J. 141, 144 (2001) [hereinafter Byers].

75 *Id.*

76 STATEMENT OF FTC ON "IDENTITY THEFT," *supra* note 65. The Social Security number is the piece of information that aids the identity theft the most because it allows access to the individual's financial information. *Id.*

77 Beth Givens, *Public Records in a Computerized Network Environment: Privacy Implications*, Privacy Rights Clearinghouse First Amendment Coalition Conference, *at* http://www.pri

formation from various public records, the accumulated data may be sorted in many different ways to essentially create new records, which may be used for any range of reasons "beyond the original public policy reason for collecting them."[78] It is the totality of this information and how it is used that poses the greatest threat to an individual's privacy.[79]

4. *Information Brokers*

Information brokers make use of numerous databases, public records, and credit headers[80] sold by credit reporting agencies. The brokers then sell the accumulated data to individuals in search of information.[81] When the brokers sell the reports on-line, they have no way to verify the identity of the person seeking the information.[82] According to Brad Blower, the Assistant Director of the Financial Practices Division at the FTC, "[a]lthough information brokers provide a legitimate service, we are concerned that bad actors and practices by some in the industry may be fueling identity theft."[83] For the identity thief, this makes the Internet the ideal location to commit the crime.

5. *Impact of Identity Theft*

Identity theft impacts individual victims, banks, and credit grantors.[84] Identity thieves may open credit card accounts and apply for loans under the victim's name and never pay the bill; they may open checking accounts and write bad checks; or obtain goods or establish services that the identity thief would not be able to obtain using her real name.[85] Currently, federal law limits consumer liability for credit card fraud to fifty dollars per account,[86] making the financial institution and credit grantor appear to be the primary victim of identity theft because they suffer the direct financial loss.[87] But this view ignores the impact on the individual whose identity has been misappropriated. Victims of identity theft are left with the burden of spending "thousands of dollars and hundreds of hours"[88] trying to restore their credit history and prevent any further misuse of their information.[89] As the victims and costs of identity theft grew in number,[90] Congress was faced with the challenge of trying to protect individuals' personal information while trying to modernize the financial industry.

III. THE FINANCIAL SERVICES MODERNIZATION ACT

On November 12, 1999, President Clinton signed into law the Financial Services Modernization Act, commonly known as the Gramm-Leach-Bliley Act ("GLB Act" or "Act").[91] This law, which became effective on July 1, 2001, was a widely debated piece of legislation mainly due to the privacy provisions contained within it.[92]

A. Background Reasons for Passing the Gramm-Leach-Bliley Act

The GLB Act overturned key provisions of the Glass-Steagall Act,[93] which had divided the finan-

---

vacyrights.org/ar/speech1.htm (Sept. 23, 1995) (last visited Feb. 1, 2003).

78 *Id.*

79 *Id.*

80 STATEMENT OF FTC ON "IDENTITY THEFT," *supra* note 65. Credit header information is identifying information, which includes the name, address, Social Security number, and telephone number of the individual. This information is printed at the top of the credit report. *Id.*

81 Byers, *supra* note 74, at 144.

82 O'Harrow, *supra* note 71.

83 *Id.*

84 McKelvey, *supra* note 1, at 1085.

85 DEPARTMENT OF JUSTICE, *supra* note 66.

86 Truth in Lending Act, 15 U.S.C. §1643(a)(1)(B) (2000), *implemented by* Regulation Z, 12 C.F.R. §226 (2002).

87 STATEMENT OF FTC ON "IDENTITY THEFT," *supra* note 65.

88 McKelvey, *supra* note 1, at 1112.

89 *Id.*; *see also* OCC Advisory Letter, *supra* note 64, at 11 (explaining the monetary costs and nonmonetary harm suffered by identity theft victims, such as denial of credit).

90 Elizabeth A. Shack, *Increasing Reports of Identity Theft in Maryland Mirror National Problem*, THE DAILY RECORD, Jan. 25, 2003, at 19A. "Identity theft has been at the top of the FTC's list of fraud reporting since it was first tracked in 2000. By 2002, it accounted for 43 percent of the fraud complaints to the commission." *Id.*

91 15 U.S.C. §§6801-6809 (1999).

92 Kristina A.K. Hickerson, *Consumer Privacy Protection: A Call for Reform In An Era of Financial Services Modernization*, 53 ADMIN. L. REV. 781, 781-83 (2001).

93 Banking Act of 1933, Pub. L. No. 73-66, ch. 89, 48 Stat. 162 (1933) (codified in scattered sections of 12 U.S.C.). The Glass-Steagall Act was passed during the Great Depression in an attempt to restore confidence in the banking industry. The Act separated the commercial banking industry from investment banking activities because of the concern that banks had underwritten unsound securities and had been a factor in causing the stock market crash of 1929. *See generally*

cial industry into banking and securities halves.[94] The purpose of the GLB Act was "to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers."[95] The Act sought to accomplish this purpose by eliminating the barriers on affiliation between banks, insurance, and securities industries.[96] In eliminating these barriers, supporters of the act claimed that the financial industry would be able to provide one-stop shopping for financial services, which would create lower interest rates, lower credit costs, and create more available credit.[97] In addition, once these three industries affiliated, they would possess the ability to merge their customer information into one single database.[98] Realizing that this ability to share information could aggravate consumer concerns relating to the dissemination of their personal financial information, Congress enacted privacy protection provisions. It was these privacy provisions that created the greatest dispute.[99] There are a number of reasons why the information disclosed to financial industries was deemed to warrant protection.

1. *Confidentiality of Financial Information*

A financial institution owes its customers certain duties due to the contractual relationship between the two.[100] These duties may be express or implied, but many courts have been willing to find that it is an implied term of the contract between the customer and the bank that the bank will not disclose account information to third parties without the consent of the customer.[101]

Aside from the contractual relationship, the court in *Djowharzadeh v. City Nat'l Bank & Trust Co.* found that a duty of confidentiality exists because of the unique relationship between a bank and its customers.[102] Before a contractual relationship exists, a person seeking to open an account or apply for a loan is required to disclose a wide variety of very personal information.[103] This places the applicant in an inferior position to the bank,[104] which holds itself out as a trusted, secured institution.[105] Therefore, the *Djowharzadeh* court held that there is an implied duty to keep the contents of applications confidential.[106]

2. *Information Sharing is a Common Practice*

Despite these duties to keep information confidential, information sharing is a common practice within the financial industry. Financial institutions may enter into marketing agreements with telemarketers, and as a result of these agreements, telemarketers have access to the bank's customer information.[107] With this access, telemarketers often receive names, addresses, phone numbers, Social Security numbers, account balances and even credit limits.[108]

An example of this was revealed in June of 1999 when the Minnesota Attorney General's Office filed a lawsuit against U.S. Bank National Association and its parent holding company, U.S. Bancorp for violation of the Fair Credit Reporting

---

Joseph Jude Norton, *Up Against 'The Wall': Glass Steagall and the Dilemma of a Deregulated ('Regulated') Banking Environment*, 42 BUS. LAW. 327 (1987) (providing a background and evaluation of the Glass-Steagall Act) [hereinafter Norton].

94 Norton *supra* note 93, at 327.

95 *See* H.R. Conf. Rep. No. 106-434 (1999).

96 Richard Blackmon, *The Financial Services Modernization Act: The Death of Consumer Privacy*, eRef.net, *at* http://www.eref.net/privacy/fact_sheets/death_of_privacy.asp (last visited Feb. 1, 2003) [hereinafter Blackmon].

97 *Id.*

98 *Id.* (claiming that the lower interest rates and credit costs potentially achieved by the sharing of information may also create a privacy nightmare).

99 Pamela Yip, *One Stop Shopping for Financial Services; Some Say New Federal Law Can Save Customers Money, but Consumer Groups Raise Privacy Issues*, CHI. TRIB., Feb. 22, 2000, at C3.

100 Kristen S. Provenza, *Identity Theft: Prevention and Liability*, 3 N.C. Banking Inst. 319, 330 (1999) [hereinafter Provenza].

101 *See, e.g.*, Barnett Bank of West Fla. v. Hooper, 498 So. 2d 923, 925-26 (Fla. 1986) (holding that a bank has an implied contractual duty not to disclose information regarding customers' accounts); Sun First Nat'l Bank of Lake Wales v. Stegall, 395 So. 2d 1248, 1249 (Fla. Dist. Ct. App. 1981) (recognizing that banks have an implied contractual duty not to disclose a depositor's account information to third parties); McGuire v. Shubert, 722 A.2d 1087, 1090-91 (Pa. Super. Ct. 1998) (holding that banks have an implied contractual duty to keep customers' bank account information confidential); Provenza, *supra* note 100, at 330-335.

102 Djowharzadeh v. City Nat'l Bank & Trust Co., 646 P.2d 616, 619-20 (Okla. Ct. App. 1982).

103 *Id.* at 619.

104 *Id.*

105 *Id.* "The precarious position of the borrower and the relatively superior position of the bank mandates there be a counterbalancing special duty imposed on the part of the bank." *Id.*

106 *Id.* at 619-20.

107 Hatch, *supra* note 12, at 1491.

108 *Id.*

Act ("FCRA") and state law.[109] The lawsuit alleged that the bank disclosed the names, phone numbers, Social Security numbers, account balances, and credit limits of its customers to MemberWorks, a telemarketing firm, after telling them that "all personal information you supply to us will be considered confidential."[110] The bank settled the lawsuit for three million dollars and ceased participating in the marketing programs.[111] Following the lawsuit, a variety of other financial institutions admitted to engaging in similar practices.[112] The practice of banks selling confidential consumer information is contrary to what the reasonable person would expect and violates the trust that banks have been given.

Considering all of the technology available and how easy it is for identity thieves to obtain personal identifying information, customers expect financial institutions to demonstrate more care and respect for the confidential information they have been entrusted with.[113] This became apparent as Congress sought to modernize the financial industry.

B. Privacy Rights Within the Gramm-Leach-Bliley Act

The GLB Act states "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[114] This broad policy statement is to be given effect in three ways.

First, the agencies that the Act designates, the Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission, must establish standards relating to administrative, technical and physical safeguards.[115] These standards should allow for the security and confidentiality of customer records, for the protection against any dangers or hazards to the security of the customer records, and for the protection against unauthorized access to or use of the customer records.[116] Great care should be taken to prevent any inconvenience or harm to the customer.[117]

Second, financial institutions must notify the consumer before disclosing nonpublic personal information to a nonaffiliated third party.[118] This notice must provide the consumer with the opportunity to opt-out of the sharing of this information with nonaffiliated third parties.[119] Account numbers may not be disclosed for the purposes of telemarketing, direct mail, or other electronic mail marketing.[120] The only exception to the nondisclosure of account numbers is for consumer reporting agencies.[121]

Finally, financial institutions are required to disclose their privacy policy when a customer relationship is established with a consumer.[122] The disclosure must also be given to each consumer annually during the continuation of the customer relationship.[123]

1. Who Does the Act Apply To?

These provisions apply to any financial institution, defined as any institution, "the business of which is engaging in financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956."[124] In that regard the GLB Act authorizes a financial holding company to engage

---

109 *See* Hatch v. U.S. Bank Nat'l Ass'n, ND, Civ. Action No. 99-872 (D. Minn. filed June 9, 1999); FCRA, 15 U.S.C. §§1681 *et seq.* (2000); *see generally* Thomas P. Vartanian & Robert H. Ledig, *21st Century Money, Banking & Commerce: State Privacy Litigation*, E-Bank Futures (Aug. 31, 1999), *at* http://www.ffhsj.com/21stbook/updates/august/august3.htm (providing a detailed explanation of the allegations within the complaint).

110 Hatch v. U.S. Bank Nat'l Ass'n, ND, Civ. Action No. 99-872 (D. Minn. filed June 9, 1999); Hatch, *supra* note 12, at 1492.

111 Hatch, *supra* note 12, at 1492; Press Release, Minnesota Attorney General's Office, Minnesota Attorney General And U.S. Bancorp Settle Customer Privacy Suit, *at* http://www.prnewswire.com (June 30, 1999).

112 Hatch, *supra* note 12, at 1492.

113 Provenza, *supra* note 100, at 335.

114 15 U.S.C. §6801(a).

115 *Id.* §6804(a)(1).

116 *Id.* §6801(b).

117 *Id.* §6801(b)(3).

118 *Id.* §6802.

119 *Id.* §6802(b)(1)(B).

120 *Id.* §6802(d).

121 *Id.* §6802(e)(6)(A).

122 *Id.* §6803(a).

123 *Id.*

124 *Id.* §6809(3)(a); Section (k)(4) states:

> the following activities shall be considered to be financial in nature: (A) Lending, exchanging, transferring, investing for others, or safeguarding money or securities. (B) Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as princi-

in a wide, and expanding list of activities, ranging from insurance brokerage and data processing to various types of Internet services.[125]

In an effort to clear up some of the ambiguity as to what sort of entities would qualify as financial institutions, the FTC listed a number of entities it considered to be financial institutions and subject to the privacy provisions.[126] The list includes financial companies, credit bureaus, loan services, mortgage brokers, securities underwriters, broker-dealers, insurance underwriters and agents, real estate appraisers, trust companies, travel agencies, management consultants and counselors, automobile dealerships, data processors, and retailers who issue their own credit cards directly to the consumer, just to name a few.[127] Their activities are under the purview of the GLB Act regardless of the company's affiliation with a financial holding company.[128]

There is no bright-line test to determining whether the privacy rules apply. Each individual company has to evaluate whether it is engaged in a financial activity.[129] In addition, each company needs to determine whether its customers or consumers trigger the GLB Act.[130]

2. *Notice of Privacy Policy Requirement*

In order to understand whom a financial institution must provide notice to, it is important to understand the difference between a "consumer" and a "customer" under the GLB Act.[131] Under the GLB Act, a "consumer" is an "individual who obtains or has obtained a financial product or service from [a financial institution] that is to be used primarily for personal, family or household purposes, or that individual's legal representative."[132] A "customer" is a consumer who has a "continuing relationship" with the financial institution.[133] Under the GLB Act, financial institutions are not required to disclose the privacy policy if there is no intention of sharing information with nonaffiliated third parties.[134] Initial privacy policy disclosures must be given to customers at the time that a customer relationship is established and once a year during the continuation of the relationship.[135] This "customer relationship"[136] is established at the time the financial institution and the consumer enter into a continuing relationship.[137] The notice must be "clear and conspicuous"[138] and provided in a manner in which the consumer can reasonably be expected to receive the actual notice.[139]

The privacy notice must include the institution's policy with respect to: the categories of "nonpublic personal information" that are collected and disclosed;[140] the categories of third parties to whom nonpublic personal information

---

pal, agent, or broker for purposes of the foregoing, in any State. (C) Providing financial, investment, or economic advisory services, including advising an investment company . . . . (D) Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly. (E) Underwriting, dealing in, or making a market in securities.

Bank Holding Company Act of 1956, 12 U.S.C. §1843(k)(4)(A)-(E) (2000).

125 L. Richard Fischer, Richard G. Stephenson & Joan P. Warrington, *The Evolution of Privacy Rights*, 1241 PLI/CORP. 691, 703-704 (Apr. 16, 2001) [hereinafter Fischer].

126 Federal Trade Commission, Privacy of Consumer Financial Information, Final Rule, 16 C.F.R. §313.3(k)(2)(i)-(xii) (2000) [hereinafter FTC Final Rule]. Although citations only refer to the FTC's Final Rule, each of the other agencies designated by Congress with responsibilities under the GLB Act, promulgated an analogous set of regulations. *See* Comptroller of the Currency Final Rules, 12 C.F.R. §40.1 *et seq.*, Board of Governors of the Federal Reserve System Final Rules, 12 C.F.R. §216.1 *et seq.*, Federal Deposit Insurance Corporation Final Rules, 12 C.F.R. §332.1 et seq., Office of Thrift Supervision Final Rules, 12 C.F.R. §573.1 *et seq.*, National Credit Union Administration Final Rules, 12 C.F.R. §716.1 *et seq.*

127 FTC Final Rule, *supra* note 126, §313.3(k)(2)(i-xii).

128 Paul J. Polking and Scott A. Cammarn, *Overview of the Gramm-Leach-Bliley Act*, 4 N.C. BANKING INST. 1, 28 (2000).

129 Robert H. Ledig, *Gramm-Leach-Bliley Act Financial Privacy Provisions: The Federal Government Imposes Broad Requirements to Address Consumer Privacy Concerns*, pt. 2.1.1, *at* http://www.ffhsj.com/bancmail/bmarts/ecdp_art.htm (last visited Feb. 1, 2003) [hereinafter Ledig].

130 *Id.*

131 Therese G. Franzen & Leslie Howell, *Financial Privacy Rules: A Step By Step Guide to the New Disclosure Requirements Under the Gramm-Leach-Bliley Act and the Implementing Regulations*, 55 CONSUMER FIN. L.Q. REP. 17, 17-18 (2001) [hereinafter Franzen & Howell].

132 FTC Final Rule, *supra* note 126, §313.3(e)(1).

133 *Id.* §313.3(h).

134 Franzen & Howell, *supra* note 131, at 18.

135 *Id.*; 15 U.S.C. §6803(a).

136 15 U.S.C. §6803(a). The Act does not define a "customer relationship."

137 Ledig, *supra* note 129, pt. 2.1.2.3.1.

138 FTC Final Rule, *supra* note 125, §313.3(b)(1). ("Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.").

139 Ledig, *supra* note 126, pt. 2.1.2.2.

140 15 U.S.C. §6809(4)(A). "The term 'nonpublic personal information' means personally identifiable financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise

is disclosed; what information, if any, about former customers is disclosed and to whom; if nonpublic personal information is disclosed to a nonaffiliated third party, a separate statement of the categories of information disclosed and the categories of third parties with whom the institution has contracted; an explanation of the consumer's right to opt-out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods the consumer may use to exercise that right; any disclosures made under the Fair Credit Reporting Act;[141] and the policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.[142]

3. *Opt-Out of Disclosing Information to Nonaffiliated Third Parties*

The opt-out requirements are set out in Section 502 of the GLB Act.[143] A financial institution may not disclose directly or through an "affiliate"[144] any nonpublic personal information to a "nonaffiliated third party"[145] unless the institution has informed the consumer of the categories of information that would be disclosed and the consumer is given a reasonable opportunity to exercise the right to opt-out.[146] Thirty days is generally considered to be a reasonable amount of time to allow the consumer to opt-out.[147]

The FTC's privacy rule also requires that the customer be given a reasonable method to opt-out.[148] For example, the institution may designate a check-off box in a prominent position on the opt-out notice; may include a reply form with the opt-out notice; may provide a toll-free telephone number the consumer may call to opt-out; or may provide an electronic method to opt-out if the consumer has agreed to the electronic delivery of information.[149] The opt-out notice may be delivered at the same time as the privacy policy of the financial institution.[150] However, if the opt-out notice is provided at a later date than the privacy policy notice, a copy of the privacy policy must be provided to the consumer again.[151]

Even if the customer has not exercised the right to opt-out, the Act prohibits the financial institution from disclosing account numbers or access codes to a nonaffiliated third party.[152] This protects against telemarketers having direct access to the customers' accounts.[153]

4. *Exceptions*

The GLB Act does nothing to prevent information sharing among affiliates, which may be done without giving the consumer any notice or opportunity to opt-out.[154] In addition, a financial institution may provide nonpublic personal information to a nonaffiliated third party to perform ser-

obtained by the financial institution." *Id.* Nonpublic personal information includes any list or grouping of consumers that was created using nonpublic personal information. *Id.* §6809(4)(C)(i). The term nonpublic personal information also includes the information collected from Internet "cookies." *See* Fischer, Stephenson & Warrington, *supra* note 125, at 704.

141 15 U.S.C. §1681a(d)(2)(A)(iii) (relating to the ability to opt out of disclosing information among affiliates).

142 FTC Final Rule, *supra* note 126, §313.6(a)(1)-(9). The institution is not required to provide technical information about the specific safeguards in use. It may simply provide in general terms who is authorized to access the nonpublic personal information and whether there are safeguards in place to ensure that the policy is followed. *Id.*

143 15 U.S.C. §6802(b).

144 *Id.* §6809(6), "The term 'affiliate' means any company that controls, is controlled by, or is under common control with another company." *Id.*

145 *Id.* §6809(5), "The term 'nonaffiliated third party' means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution." *Id.*

146 *Id.* §6802(b)(1)(A)-(C); *see also* Franzen & Howell, *supra* note 131, at 21.

147 PRIVACY RIGHTS CLEARINGHOUSE, PROTECTING FINANCIAL PRIVACY IN THE NEW MILLENIUM: THE BURDEN IS ON YOU, *at* http://www.privacyrights.org/fs/fs24-finpriv.htm (last visited Feb. 1, 2003) [hereinafter PROTECTING FINANCIAL PRIVACY].

148 OFFICE OF THE COMPTROLLER OF THE CURRENCY, PRIVACY RULE: SMALL BANK COMPLIANCE GUIDE, pt. III, §F, at 36 (Dec. 2001) [hereinafter SMALL BANK COMPLIANCE GUIDE].

149 *See* FTC Final Rule, *supra* note 126, §313.7(a)(2)(B)(ii)(A)-(D); *see also* SMALL BANK COMPLIANCE GUIDE, *supra* note 148, at pt. III, §F, at 36. Staff of the agencies responsible for the supervision of banks and credit unions issued a series of Frequently Asked Questions to help financial institutions comply with the privacy regulations of the GLB Act. *See* Joint Release, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency & Office of Thrift Supervision, *Guidance on Financial Privacy* (Dec. 12, 2001) *at* http://www.federalreserve.gov/boarddocs/press/general/2001/200112122/default.htm (last visited Feb. 1, 2003).

150 FTC Final Rule, *supra* note 126, §313.7(c).

151 *Id.*

152 15 U.S.C. §6802(d).

153 *Id.*

154 PROTECTING FINANCIAL PRIVACY, *supra* note 147.

vices for or functions on behalf of the financial institution.[155] These services or functions include marketing of the financial institution's own products or services or financial products or services offered pursuant to a joint agreement between financial institutions.[156] The third party, however, must agree to maintain the confidentiality of the information.[157]

Section 502 also provides for a variety of other exceptions. A financial institution may, in certain circumstances, disclose nonpublic personal information to nonaffiliated third parties without complying with the notice and opt-out requirements.[158] The disclosure may be made as necessary to effect a transaction requested by the consumer, or in connection with servicing or processing financial products or services at the request of the consumer.[159] Disclosures may also be made when servicing the consumer's account, or with another entity, as part of a private label credit card program, or a proposed securitization, secondary market sale, or similar transaction related to the consumer's transaction.[160]

In addition, the FTC's Final Rule provides that the notice and opt-out requirements do not apply when nonpublic personal information is disclosed: (1) with the consent of the consumer, so long as the consumer has not revoked the consent; (2) in an effort to protect the confidentiality or security of the records; (3) to provide information to insurance rate advisory organizations, guaranty agencies, persons that are assessing the financial institutions' compliance with industry standards, and the consumers attorneys, accountants, and auditors; (4) to the extent permitted or required under provisions of law, to law enforcement agencies, a state insurance authority, self-regulatory organizations, or for an investigation on a matter related to public safety; or (5) to a consumer reporting agency in accordance with the Fair Credit Reporting Act.[161]

5. Enforcement Provisions

The GLB Act assigns authority for enforcing the subtitle's provisions to the FTC, the federal banking agencies, the National Credit Union Administration, and the Securities and Exchange Commission, according to their respective jurisdictions, and provides for enforcement of the subtitle by the States.[162] The GLB Act, however, does not provide for a private right of action for consumers to sue the financial institution directly for violation of the statute.[163] The consumer must complain to the agency having jurisdiction over them and that agency may bring a court action against the financial institution.[164] However, some state laws, such as the Unfair and Deceptive Practice Laws, may enable the consumer to claim that a violation of the GLB Act violated other rights granted to the individual by the state.[165]

C. Does the Gramm-Leach-Bliley Act Protect the Privacy of Your Information?

Privacy in any context is a complex issue because what one person considers an invasion of privacy another person may view as a timely offering of a beneficial service. However, in today's marketplace, where it is so easy to collect and compile large amounts of personal information for a variety of purposes, consumers should have the right to control the distribution of their financial information.[166] Although some believe the current protections are sufficient,[167] the GLB Act does not go nearly far enough, especially given that allowing the affiliation of banking, securities, and insurance industries will only accelerate the sharing of private data.[168] Most of the shortcomings of the GLB Act have to do with the consum-

155 15 U.S.C. §6802(b)(2).

156 *Id.*

157 *Id.*

158 *Id.* §6802(b)(2); FTC Final Rule, *supra* note 125, §313.13.

159 FTC Final Rule, *supra* note 126, §313.14.

160 *Id.* §6802(e)(1)(A)-(C).

161 FTC Final Rule, *supra* note 126, §313.15; Fair Credit Reporting Act 15 U.S.C. §§ 1681 *et seq.* (1994 & Supp. V 1999).

162 15 U.S.C. §6805.

163 PROTECTING FINANCIAL PRIVACY, *supra* note 146.

164 *Id.*

165 *Id.*; Mark E. Budnitz, *Consumer Privacy in Electronic Commerce: As the Millenium Approached, Minnesota Attacked, Regulators Refrained, and Congress Compromised*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 821, 882 (2000) [hereinafter Budnitz].

166 Robert O'Harrow Jr., *Night and Day, Computers Collect Information*, WASH. POST, May 16, 2001, at G10.

167 145 CONG. REC. S13, 786 (daily ed. Nov. 3, 1999) (statement of Sen. Phil Gramm) (commenting that the full disclosure requirement of the institution's privacy policy is the ultimate protection of privacy); 145 CONG. REC. S13, 876 (daily ed. Nov. 4, 1999) (statement of Sen. Chuck Hagel) (noting that more privacy provisions would be harmful to financial institutions).

168 *See* Givens, *supra* note 4.

ers' inability to control how their financial information is used.[169]

Pursuant to Section 508 of the GLB Act, the federal banking regulators and the FTC are currently requesting comments to study the actual information sharing practices among financial institutions and their affiliates.[170] The study addresses the purposes for sharing customer information with both affiliated and nonaffiliated third parties; the extent and adequacy of the security measures implemented to protect confidential customer information; the potential risk to the privacy of the customer created by information sharing; the potential benefits to financial institutions and customers from information sharing; the sufficiency of existing privacy laws and the adequacy of financial institutions' privacy policies and disclosures; the opportunity for different approaches for consumers to protect their privacy; and the possibility of further restrictions on the sharing of information.[171] The results of this study may have an impact on some of the current shortcomings of the GLB Act addressed below.[172]

1. *The Act Does Not Prevent the Sharing of Information Among Affiliates*

Senator Richard Shelby of Alabama was one of the strongest opponents of the privacy provisions of the GLB Act, stating "[u]nder this bill, the consumer has little, if any, ability to protect the transfer of his or her personal nonpublic financial information."[173] The failure of the opt-out to apply to affiliate sharing and the many exceptions to the opt-out provisions provide very little protection of a consumer's nonpublic personal information.[174]

Privacy advocates argue that increased affiliation will result in greater dissemination of information.[175] Financial institutions may share their consumer information with their affiliates without consent from the individual whose information is involved. The consumer does not even have the right to opt out of this affiliate sharing.[176] Beth Givens, director of the Privacy Rights Clearinghouse, argues that affiliate sharing is "no different than third party sale in terms of the final results. The fact that a law has been passed enabling the affiliation of these three industries does not somehow magically make the sharing of customer data between and among these industries benign and without harmful effect."[177] Making it legal to share the sensitive information that these three industries possess does not erase the potential for fraud and profiling.[178]

The GLB Act also has another very important hole in it. While affiliates may have access to an individual's nonpublic personal information, the individual does not.[179] The GLB Act does nothing to provide the consumer with the opportunity to access the information that the financial institution has compiled.[180] Although the consumer may dispute any nonpublic personal information that has been shared, the consumer has no opportunity to correct any inaccuracies.[181]

2. *The Protections Provide For Opt-Out, Not Opt-In*

One of the issues that had been highly debated during the drafting of the privacy sections of the GLB Act was whether to adopt an opt-in or an opt-out provision.[182] An opt-out provision does not require true consent for the dissemination of per-

---

169 *Id.*

170 Department of the Treasury, *In re* Public Comment for Study on Information Sharing Practices Among Financial Institutions and Their Affiliates, *Notice and Request for Comments*, 67 Fed. Reg. 7213 (Feb. 15, 2002).

171 *Id.* at 7214 (requiring the receipt of all responses by Apr. 1, 2002).

172 Federal Trade Commission, *In re* Standards for Safeguarding Customer Information, *Final Rule*, 16 C.F.R. Part 314 (2002). The Final Rule requires "each financial institution to develop a written information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue." *Id.*

173 145 CONG. REC. S13, 883, 894 (daily ed. Nov. 4, 1999) (statement of Sen. Richard Shelby).

174 *Id.*; ELECTRONIC PRIVACY INFORMATION CENTER, THE GRAMM-LEACH-BLILEY ACT, *at* http://www.epic.org/privacy/glba.html (last modified Dec. 2, 2002) [hereinafter ELECTRONIC PRIVACY INFORMATION CENTER].

175 Symposium: *The Future of Law and Financial Services: Panel II: The Policy Aspect, Consumer Data Privacy*, 6 FORDHAM J. CORP. & FIN. L. 69, 77-78 (2001).

176 PROTECTING FINANCIAL PRIVACY, *supra* note 147.

177 Givens, *supra* note 4.

178 *Id.*

179 Budnitz, *supra* note 165, at 888.

180 *See id.*

181 *Id.*

182 *See* 145 CONG. REC. E2363, E2364 (Daily Ed. Nov. 11, 1999) (statement of Rep. Melvin Watt) (contending that opt-out provision does not protect privacy of consumers); 145 CONG. REC. S13, 783, 789 (Daily Ed. Nov. 3, 1999) (statement of Sen. Paul Sarbanes) (contending that without a consent provision, the privacy protections are weak).

sonal information. With the opt-out system, information may be shared until the consumer tells the institution to keep their information confidential. Failure to exercise the right to opt-out is passive; the consumer may not have seen the privacy notice that included the opt-out disclosure, or the consumer may simply have forgotten to make the necessary phone call or mail the necessary letter.[183]

Privacy advocates favor an opt-in system as opposed to the opt-out procedure. Under an opt-in system, information remains private unless the consumer consents to the information being shared.[184] An opt-in requires an affirmative act. This is much stronger proof of the consumer's actual intent. An opt-in system would offer the consumer an opportunity to give meaningful consent.[185] Most consumers do not reasonably expect that the information provided to obtain a bank account or a loan is going to be collected and shared.[186] The opt-in system would simply require the financial institution to obtain consent before sharing this information. If the institution has a valid, worthwhile purpose, the institution must explain the benefits of giving consent, which should not be difficult to obtain if there is a definite benefit.[187] An opt-in system would also help to avoid wasteful marketing to uninterested customers.[188] The opt-in identifies the consumers who are favorably disposed to marketing because they have exercised their right to be placed in a database to receive such information.[189] Institutions would then have more accurate information to make their marketing more efficient.[190]

One Internet-based marketing company, NetCreations, Inc., has concluded that making use of the opt-in approach, with an opportunity to opt-out when the consumer receives a marketing message, is most effective.[191] Giving the individual control is the best way to market materials and maintains the customer's goodwill.[192]

Under the current system, the burden of protecting the privacy of nonpublic personal information rests on the consumer.[193] Unless the consumer specifically informs every organization she does business with that she does not want them to share information, the organization is permitted to do so.[194]

3. *The Definition of a Financial Institution is Unclear*

While the GLB Act defines a financial institution broadly, including businesses not traditionally considered related to the banking industry,[195] the definition may be underinclusive given the "overlapping nature of e-commerce, which often involves financial institutions and other businesses."[196] The GLB Act imposes no duties upon Web businesses that are not financial institutions as defined by the Act, or those that do not share information with financial institutions. Web sell-

183 Quinn, *Opt Out Rights*, *supra* note 3.

184 Hatch, *supra* note 12, at 1494.

185 William Safire, *Stop Cookie-Pushers*, N.Y. TIMES, June 15, 2000, at A27.

186 *See* Quinn, *Money Safer Than Your Privacy*, *supra* note 2.

187 Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, MINN. L. REV., 1219, 1243-44 (2002) [hereinafter Janger & Schwartz].

188 *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2406-08 (1996) [hereinafter Murphy].

189 *See id.* at 2406.

190 *See id.*

191 *Internet Marketers Vote in Favor of Opt-In Email: NetCreations Inc. Sponsors Key Internet Marketing Surveys*, BUS. WIRE, Mar. 9, 2000.

192 *Id.*; *see* Carol Patton, *Weaving Your E-Mail Marketing Web: Mass Mailing Done Right Can be Golden, But Done Wrong, It's Just Spam*, CRAIN'S DETROIT BUS., June 12, 2000, at E1.

193 ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 174.

194 Blackmon, *supra* note 96.

195 The American Bar Association ("ABA") challenged a decision of the FTC that lawyers and law firms may, in many instances, be financial institutions within the meaning of the GLB Act and therefore required to comply with the privacy policy notices provision. *See* Scott Daniels, *Read This Please! (At Least Some Of It)*, 15 UTAH BAR J., 6 (June/July 2002). The ABA tried to argue that an exemption was appropriate for lawyers and law firms because Congress did not intend to regulate the legal profession through the GLB Act and that existing rules of professional responsibility provide greater protection to consumers than the GLB Act would when applied to lawyers and law firms. *See* Letter from Martha W. Barnett, President of the American Bar Association, to Timothy J. Muris, Chairman of the Federal Trade Commission, *at* http://www.ftc.gov/os/2002/04/ababarnett010710.pdf (July 10, 2001). The FTC, however, denied these requests stating, "The Act does not provide the Commission with express authority to grant exemptions from the other provisions of the GLB Act, including the initial and annual notice provisions." *See* Letter from J. Howard Beales, Director of the Bureau of Consumer Protection of the FTC, to Robert E. Hirshon and Robert D. Evans, Governmental Affairs Office of the American Bar Association (Apr. 8, 2002) *at* http://www.ftc.gov/os/2002/04/hirshon-beales020408.pdf.

196 Budnitz, *supra* note 165, at 870.

ers are not considered financial institutions unless the seller itself has issued a credit card to the consumer.[197] However, the consumer most likely has expectations that information relating to the purchase is confidential whether or not the purchase is from a financial institution or a Web seller.[198]

4. The Privacy Notices are Inadequate

The GLB Act requires that the privacy notices sent to customers and the disclosure of opt-out provisions must be made "clearly and conspicuously."[199] However, the privacy notices that have been received have been difficult to understand and written in a manner that made it difficult to exercise the option to opt-out.[200] A study of the readability of the privacy notices was conducted by Mark Hochhauser for the Privacy Rights Clearinghouse.[201] This study found that the privacy notices were written at a third year college level or above.[202] The accepted standard recommended for documents that are intended for the general public is an eighth grade reading level.[203]

In addition to being difficult to understand, they are written in a manner that makes it difficult to understand how to opt-out.[204] Explanations of how to opt out generally appear at the end of the notices, so it is necessary to read through all of the fine print before learning how to opt out.[205] In order to gain attention, the privacy notices should provide the information on how to opt out at the beginning of the notice in print that is intended to draw a consumer's attention.[206]

5. Enforcement Mechanisms are Inadequate

The Act also does nothing to curtail the collection of consumer information. "[A] slew of companies advertising on the Internet and in the backs of newspapers and legal publications continue to offer financial information about virtually anyone for a marginal fee."[207] The accumulation and sale of personal information continues even after the GLB Act, which makes obtaining personal information under false pretenses and the theft of financial information subject to fines and imprisonment.[208] Part of the problem is the lack of enforcement mechanisms. The FTC lacks resources to adequately pursue such information brokers.[209] In November of 1999, the FTC established an identity theft hotline and, in the first month of its implementation logged approximately 445 phone calls per week.[210] In December of 2001, the weekly average of calls answered was approximately 3,000 per week.[211] Despite the large volume of consumer complaints, the FTC has been slow to pursue alleged information brokers. From the time of the hotline's inception to September of 2000, the commission had only brought one case against an alleged information broker[212] and in March of 2002, settled charges against three different information brokers.[213] This may be partially due to the fact that government agencies are subject to congressional lobbyists pressures, which influence the priority placed upon enforcing the privacy provisions of the GLB Act.[214]

Pursuant to Section 523 of the GLB Act, financial institutions need to establish security procedures to safeguard consumer information, such as

197 Ledig, *supra* note 129, pt. 2.1.1.

198 *See id.* at 871.

199 15 U.S.C. §8602(b)(1)(A).

200 Janger & Schwartz, *supra* note 187, at 1230-31.

201 Mark Hochhauser, Lost in the Fine Print: Readability of Financial Privacy Notices, *at* http://www.privacyrights.org/ar/GLB-Reading.hym (July 2001).

202 *Id.*

203 *Id.*

204 COMMENTS IN THE MATTER OF FINANCIAL SERVICES MODERNIZATION ACT OR GRAMM-LEACH-BLILEY ACT, ELECTRONIC PRIVACY INFORMATION CENTER, THE PRIVACY RIGHTS CLEARINGHOUSE, US PIRG, AND CONSUMERS UNION, Study on Information-Sharing Practices Among Financial Institutions and Their Affiliates, 18, May 1, 2002; Janger & Schwartz, *supra* note 187, at 1231-21.

205 Janger & Schwartz, *supra* note 187, at 1231-32.

206 *Id.* at 1258.

207 Brian Krebs, *Financial Privacy Elusive in Wake of New Privacy Laws*, NEWSBYTES, Sept. 13, 2000 [hereinafter Krebs].

208 15 U.S.C. §6823.

209 Budnitz, *supra* note 165, at 881-82.

210 Richard M. Stana, *Identity Theft: Prevalence and Cost Appear to be Growing*, United States General Accounting Office 4 (GA-02-363) (2002).

211 *Id.*

212 Krebs, *supra* note 207.

213 FTC, INFORMATION BROKERS SETTLE FTC CHARGES, Mar. 8, 2002, *at* http://www.ftc.gov/opa/2002/03/pretextingsettlements.htm (last visited Feb. 1, 2003). The complaints named Information Search, Inc. of Baltimore, Md., Smart Data Systems of Staten Island, N.Y., and Discreet Data Systems of Humble, Tex. as defendants. *Id.* Smart Data Systems and Discreet Data Systems settled for $2,000 each. A $15,000 payment was suspended against Information Search based upon financial statements. *Id.*

214 *See* Budnitz, *supra* note 165, at 881-82.

verification, fraud prevention, and information security.[215] While the bank and thrift regulatory agencies have issued the joint guidelines for safeguarding confidential consumer information,[216] there are no required methods to ensure adherence to these policies.[217] The guidelines list security measures for financial institutions to consider implementing, such as:

> (1) identify and assess the risks that may threaten customer information; (2) develop a written plan containing policies and procedures to manage and control these risks; (3) implement and test the plan; and (4) adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.[218]

However, a financial institution only needs to implement the security measures it determines to be appropriate.[219]

Verification procedures must be established to ensure the accuracy of the information given to a financial institution when new accounts are opened. For example, institutions could call the customer to confirm her desire to open an account or apply for a credit card. Institutions could also verify information by contacting the employer listed on the application.[220]

To prevent the occurrences of fraudulent address changes, financial institutions should send a confirmation of the address change request to the new address as well as the previous address on the institution's record. In addition, when a customer is seeking to open a new account, the financial institution should take steps to make sure the information given has not been associated with fraudulent activity. To do this, the financial institutions should check the credit reports for a fraud alert.[221]

To ensure adherence to these policies, the financial institutions should have written procedures on how to open an account and regular training to make sure that employees follow the procedures.[222] Part of the established procedures should limit the circumstances under which a consumer's information is revealed over the telephone and encourage the institution's employees to report attempts to open accounts using another individual's information.[223]

IV. FIRST AMENDMENT ARGUMENTS

At least twenty-five states have considered enacting greater privacy protections than those provided by the GLB Act.[224] At the time the GLB Act was being considered by Congress, there were a number of other bills before Congress, which would have provided increased protection for privacy.[225] However, when there is a claim that an individual's privacy is being invaded and the action invading that privacy involves speech, writing, or other communicative media, there is a tension with First Amendment rights.[226] An evaluation of the First Amendment may explain why Congress was hesitant to further control the collection and dissemination of personal information. However, as these next sections will demonstrate, the First Amendment is not a bar to heightened protection of consumer's personal information.

A. Background

The First Amendment of the United States Constitution states, "Congress shall make no law respecting an establishment of religion, or

---

215 Richard Spillenkothen, *Identity Theft and Pretext Calling*, Supervisory Letter SR 01-11 (SUP), Board of Governors of the Federal Reserve System, *at* http://www.federalreserve.gov/boarddocs/SRLetters/2001/sr0111.htm, April 26, 2001, (last visited Feb. 1, 2003) [hereinafter Spillenkothen]; *see also*, John Ginovsky, *Pretext Calls: Is Your Staff Equipped to Handle Them Properly*, ABA Bankers News, *at* http://www.privacytoday.com/bankersnews2.htm (June 12, 2001).

216 Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616 (Feb. 1, 2001) [hereinafter Interagency Guidelines].

217 BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, FEDERAL DEPOSIT INSURANCE CORPORATION, OFFICE OF THE COMPTROLLER OF THE CURRENCY & OFFICE OF THRIFT SUPERVISION, Joint Release, *Agencies Adopt Guidelines for Customer Information Safety* (Jan. 17, 2001).

218 *Id.*

219 *Id.*

220 Spillenkothen, *supra* note 215.

221 *Id.*

222 *Id.*; FEDERAL TRADE COMMISSION, FINANCIAL INSTITUTIONS AND CUSTOMER DATA: COMPLYING WITH THE SAFEGUARDS RULE, *at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm (Sept. 2002).

223 *Id.*

224 Budnitz, *supra* note 165, at 883.

225 *Id.* at 884-89. In addition to other privacy bills in Congress, roughly half of the states introduced privacy bills that would grant stronger privacy protection than the GLB Act. As of now, however, all of these bills have failed to be approved by the state legislators because of strong opposition by the financial services industry. *See* Givens, *supra* note 4.

226 Scott Shorr, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1795 (1995).

prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[227] The Supreme Court has long recognized "that not all speech is of equal importance. It is speech on matters of public concern that is at the heart of the First Amendment's protection."[228] Essentially, First Amendment protections are extended to communications that involve public discourse to enable the conveyance of information necessary for decision making.[229]

Most financial institutions would argue that the collection, use, and dissemination of information about their consumers is protected by the Constitution as commercial speech, and therefore may not be subjected to restrictions.[230] To support this position, financial institutions would most likely rely on the Supreme Court's statement, "the free flow of commercial information is indispensable . . . to the proper allocation of resources in a free enterprise system [and] to the formation of intelligent opinions as to how that system ought to be regulated or altered."[231]

In addition, to further support the proposition that the sharing of financial information about a consumer is commercial speech, financial institutions could rely on *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*[232] In *Dun & Bradstreet*, the Supreme Court examined credit reports issued by credit reporting agencies. The Court stated that a credit report "provided subscribers with financial and related information about businesses."[233] Therefore, consumer reports are only of interest to the individual and the specific business audience.[234] It was not necessary to provide the credit reports with full First Amendment protection because the information was not needed to promote the free flow of information on matters of public concern.[235] The credit reports implicated concerns that argued in favor of the constitutional protection that commercial speech receives.[236]

B. Commercial Speech Doctrine

The Supreme Court has had some difficulty coming up with a precise definition of commercial speech.[237] According to Robert Post, a professor of law at the University of California, Berkeley, "[t]he court [in Thomas v. Collins][238] explicitly concludes that no simple fact, like the presence of a business interest or compensation, can distinguish commercial from political speech."[239] The Court must therefore determine the nature of the speech and whether it should be included within public discourse.[240] The contemporary Court has preferred a common-sense approach in deciding where the line should be drawn distinguishing between commercial speech and public discourse.[241]

The commercial speech doctrine first appeared in *Valentine v. Chrestensen*,[242] where the Court held that the First Amendment leaves states free to restrict "purely commercial advertising."[243] The Court retreated from this position and gave commercial speech a larger degree of protection in *Pittsburgh Press Co. v. Pittsburgh Commission on Human Relations*.[244] In *Pittsburgh Press*, the Court stated that subsequent courts have held, "speech is not rendered commercial by the mere fact that it relates to an advertisement."[245] The advertisement in question was not granted any First

---

227 U.S. CONST. amend. I.

228 Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758-59 (1985).

229 Robert Post, *The Constitutional Status of Commercial Speech*, 48 UCLA L. REV. 1, 4 (2000) [hereinafter Post].

230 *See* Jorstad, *supra* note 6, at 1513.

231 Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 765 (1976).

232 472 U.S. 749 (1985).

233 *Id.* at 751.

234 *Id.* at 762.

235 *Id.* at 762-63.

236 *Id.*; *see, e.g.*, Motor and Equip. Mfrs. Ass'n v. EPA, 627 F.2d 1095 (D.C. Cir. 1979) (regulation restricting automobile manufacturers from disseminating maintenance notices was seen as a restriction on commercial speech but was held as passing constitutional muster because the regulation of speech had a reasonable basis in a substantial government interest); U.S. West v. FCC, 182 F.3d 1224 (10th Cir. 1999) (disseminating information by telecommunications carriers about their customers is commercial speech that required protection because the FCC regulation at issue violated the First Amendment).

237 Joshua A. Marcus, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 258 (1998) [hereinafter Marcus].

238 323 U.S. 516 (1945).

239 Post, *supra* note 229, at 18.

240 *Id.* at 20.

241 *See, e.g.*, Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 455-56 (1978); Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y., 447 U.S. 557, 562 (1980); *Virginia State Bd. of Pharmacy*, 425 U.S. at 771 n.24.

242 316 U.S. 52 (1942).

243 *Id.* at 54.

244 413 U.S. 376 (1973).

245 *Id.* at 384.

Amendment protection however, because the advertisement was for an illegal commercial activity.[246]

After its holding in *Valentine*, the Court continued to narrow its stance in *Bigelow v. Virginia*.[247] *Bigelow* involved a Virginia newspaper advertisement that described the legality and availability of abortions in New York.[248] The Court held that "speech is not stripped of First Amendment protection merely because it is published in that form [paid commercial advertisement]."[249] The mere presence of a commercial aspect did not eliminate all First Amendment protection.[250]

In 1980, the Supreme Court held in *Central Hudson Gas & Electric Corp. v. Public Service Commission*[251] that "the Constitution . . . accords a lesser protection to commercial speech than to other constitutionally guaranteed expression.[252] The protection available for a particular commercial expression turns on the nature both of the expression and of the governmental interests served by its regulation."[253] *Central Hudson* established a four-part test to evaluate the constitutionality of government regulations on commercial speech.[254] Under the *Central Hudson* test, a court must first decide whether the speech is protected by the First Amendment.[255] The speech must concern a lawful activity, and it must not be misleading.[256] Second, the Court must decide whether the government has a substantial interest in regulating the speech.[257] Third, if the court finds that the government interest is substantial and concerns a lawful activity, the court must decide whether the regulation materially advances the government interest.[258] Finally, the court must decide whether the regulation "is not more extensive than is necessary to serve that interest."[259]

Given that the information sharing covered by the GLB Act is commercial speech, *Central Hudson* would apply. In order to determine whether Congress would be able to amend the GLB Act to create greater privacy protections, a court would be required to determine the type of information that is being collected and disseminated by the financial institutions. The most common information disclosed to a financial institution is an individual's name, address, telephone number, and Social Security number. The following section will evaluate whether requiring financial institutions to obtain affirmative consent from a consumer before sharing information with an affiliate would pass constitutional muster.

C. *Central Hudson* Analysis

The first inquiry under *Central Hudson* is whether the speech is lawful and is not misleading.[260] Neither the financial institution, nor the consumer, would likely argue that the names, addresses, telephone numbers, and Social Security numbers currently shared among affiliates is false or misleading information.

The second inquiry is whether the government has a substantial government interest in regulating the speech.[261] The government's interest in restricting the dissemination of a consumer's name, address, telephone number, and Social Security number without consent to affiliates of a financial institution, is to protect the privacy, confidentiality, and security of this information from becoming subject to misuse, such as identity theft.[262] Courts have recognized that the protection of consumer privacy is a substantial government interest.[263]

In response, financial institutions would argue that protecting consumer privacy does not rise to the level of a substantial government interest by relying on *U.S. West, Inc. v. Federal Communications*

246 *Id.* at 388.

247 421 U.S. 809 (1975) (holding unconstitutional a law which made it a misdemeanor to publish abortion advertisements).

248 *Id.* at 812.

249 *Id.* at 818 (citing Pittsburgh Press Co. v. Human Rel. Comm'n, 413 U.S. 376, 384 (1973); New York Times Co. v. Sullivan, 376 U.S. 254, 266 (1964)).

250 *Id.*

251 447 U.S. 557 (1980) (considering whether the New York State Public Service Commission could prevent electric companies from taking part in promotional advertising).

252 *Id.* at 563 (quoting *Ohralik* 436 U.S. at 456, 457).

253 *Id.*

254 *Id.* at 566; Marcus, *supra* note 236, at 264-65 (providing historical development of the commercial speech doctrine).

255 *Central Hudson*, 447 U.S. at 566.

256 *Id.* The state may not regulate speech that does not pose a danger to the asserted government interest. *Id.* at 565.

257 *Id.* at 566.

258 *Id.*

259 *Id.*

260 *Id.*

261 *Id.*

262 *See* OCC Advisory Letter, *supra* note 64.

263 *See, e.g.*, Florida Bar v. Went For It, Inc., 515 U.S. 618, 625 (1995) (protecting consumers from unwanted solicitation); Edenfield v. Fane, 507 U.S. 761, 769 (1993) (protecting consumers from unwanted solicitation).

Commission.[264] In *U.S. West,* an FCC order required telecommunications carriers to obtain customer approval before using or disclosing phone records.[265] The court was noticeably concerned because the FCC had not stated the specific privacy harm that it sought to protect against.[266] While analyzing nonpublic personal information, Congress and consumers have a specific harm to combat under the GLB Act, the violation of a stated purpose of the Act, the "continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[267]

Financial institutions may also argue that the costs of restricting the sharing of information among affiliates would outweigh the government interest. Richard Kovacevich, the President and Chief Executive Officer of Wells Fargo & Co., a diversified financial services company, states that, "[t]he more privacy we have, the slower we will be in responding to customers' requests for credit and the less able we will be to identify products that best suit our customers' needs."[268] Thus, financial institutions would argue that restricting the use and transfer of information contradicts the purpose of the Act, which is to allow financial institutions to provide efficient service.[269] However, *Trans Union Corp. v. FTC*[270] has already determined that the protection of the privacy of consumer credit history is a substantial government interest.[271]

The third inquiry under *Central Hudson* is whether the regulation would materially advance the government interest.[272] To require affirmative consent from a consumer before disseminating nonpublic personal information among affiliates does not deny a financial institution use of the nonpublic personal information. Consent would simply require the financial institution to obtain the consumer's permission before sharing the nonpublic personal information. If the institution has a valid purpose for wanting to share the information with an affiliate, then the consent should not be difficult to obtain.[273] The stated purpose of the Act is to respect the privacy of customers and the confidentiality of the customers' nonpublic personal information.[274] Regulations that restrict the use and dissemination of nonpublic personal information would clearly support this interest.[275]

The final inquiry is whether an opt-in regulation is no more extensive than necessary to accomplish the purpose.[276] Under this inquiry, the regulations must demonstrate "a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition, but one whose scope is in proportion to the interest served."[277] Currently, the Act only requires notice and an opportunity to opt-out of information disclosure to nonaffiliated third parties.[278] The further restriction on sharing nonpublic personal information among affiliates would simply allow consumers to retain control over their own information. Information given to an institution for one purpose should not be disseminated to affiliated or nonaffiliated third parties without the consent of the consumer. Therefore, further re-

---

264 182 F.3d 1224 (10th Cir. 1999); *see generally* Andrew Dymek, *A Clash Between Commercial Speech and Individual Privacy: U.S. West v. FCC,* 2000 UTAH L. REV. 603 (2000) (providing a detailed analysis of U.S. West v. FCC and issues relating to First Amendment and privacy conflicts).

265 *U.S. West,* 182 F.3d at 1228.

266 *Id.* at 1235. The court stated that it could infer the privacy harm §222 sought to protect against. The Court held that the government asserted a substantial state interest because it sought to protect people from the disclosure of sensitive and potentially embarrassing personal information. *Id.* at 1235-36.

267 15 U.S.C. §6801(a).

268 Richard M. Kovacevich, *Privacy and the Promise of Financial Modernization,* THE REGION, Special Issue 2000, *at* http://minneapolisfed.org/pubs/region/00-03/kovacevich.html (last visited Jan. 10, 2002). Wells Fargo & Co. provides banking, estate planning, insurance, investment, and mortgage and consumer financing. *See* Wells Fargo, WELLS FARGO TODAY, Fourth Quarter 2001, *at* http://www.wellsfargo.com/about/today1.jhtml (last visited Mar. 13, 2002).

269 U.S. PUBLIC INTEREST RESEARCH GROUP ("PIRG"), WHAT IS THE GRAMM-LEACH-BLILEY FINANCIAL SERVICES MODERNIZATION ACT OF 1999 AND HOW DOES INFORMATION SHARING AFFECT YOUR PRIVACY?, *at* http://www.pirg.org/consumer/privacy/glb.htm (last visited Feb. 1, 2003).

270 245 F. 3d 809 (D.C. Cir. 2001) (finding that restriction on the speech of a credit reporting agency due to an FTC ban on the sale of target marketing lists did not violate First Amendment rights because the government had substantial interest in protecting the privacy of credit information).

271 *Id.* at 818.

272 *Central Hudson,* 447 U.S. at 566.

273 *See* Murphy, *supra* note 187, at 2406.

274 15 U.S.C. §6801.

275 U.S. v. Edge Broadcasting Co., 509 U.S. 418, 428 (1993) (holding that factual evidence is not necessary to establish that regulations will materially advance the government interest where the relation is obvious).

276 *Central Hudson,* 446 U.S. at 566.

277 Greater New Orleans Broadcasting v. U.S., 527 U.S. 173, 188 (1999) (quoting Board of Trustees v. Fox, 492 U.S. 469, 480 (1989)).

278 15 U.S.C. §6802.

strictions on the dissemination of nonpublic personal information without the consent of the consumer would comply with the requirements of the First Amendment's commercial speech doctrine.

VI. CONCLUSION

The current privacy protections implemented by the Gramm-Leach-Bliley Act are an important first step in giving notice to the consumer of how her financial information is being treated by the financial institution. However, there is still too much latitude for the use of that information without the consumer's consent. The use and dissemination of information about a consumer, without her consent, poses a serious threat to the privacy of her bank account, credit card, and insurance policy. Restricting the dissemination of this information, which many financial institutions consider commercial speech, to affiliated parties may be accomplished with no damage to the First Amendment because commercial speech is not entitled to full First Amendment protection as indicated by *Central Hudson*. Due to the increased concern over the commercial use of personal information and the fact that there is no damage to the First Amendment in restricting this speech, legislators should amend the Gramm-Leach-Bliley Act to restrict information sharing among affiliates of financial institutions without the consent of the consumer.