NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW AND COMMERCIAL REGULATION

Volume 29 | Number 4 Article 3

Summer 2004

The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy

Oliver Ireland

Rachel Howell

The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy

Cover Page Footnote
International Law; Commercial Law; Law

The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy

Oliver Ireland[*] *and Rachel Howell*[**]

I. Introduction

Surveys of public opinion tend to show a strong concern for privacy, particularly with respect to financial information.[1] Consumers fear that information about them may be misused by the government or the private sector.[2] But, as recent events have made clear, that concern for privacy may be readily subordinated to other concerns, such as the fight against terrorism and fraud in the form of the growing crime of identity theft.[3]

II. Privacy Overview: The Concept of Privacy

Although we often view privacy as a cornerstone of personal freedom, legal recognition of a right to privacy in the United States is uneven and demonstrates a willingness to subordinate privacy interests to other policy interests.[4] For example, there is no

---

[*] Oliver Ireland is a partner in the Washington, D.C. office of Morrison & Foerster LLP, where his practice focuses on financial services and privacy. Prior to joining Morrison & Foerster LLP, Mr. Ireland was Associate General Counsel of the Board of Governors of the Federal Reserve System.

[**] Rachel Howell is an associate in the Washington, D.C. office of Morrison & Foerster LLP, where her practice focuses on financial services and privacy.

[1] *See, e.g.*, Electronic Privacy Information Center, *Public Opinion on Privacy*, *at* http://www.epic.org/privacy/survey (last updated June 25, 2003) (detailing the results of a number of public opinion surveys related to various aspects of privacy).

[2] *Id.*

[3] *See* Anita L. Allen, *Privacy Isn't Everything: Accountability as a Personal and Social Good*, 2003 Daniel J. Meador Lecture (Feb. 4, 2003), *in* 54 ALA. L. REV. 1375, 1375-76 (2003).

[4] *See, e.g.*, Jeffery A. Lowe, *Big Brother Will Be Watching: LifeLog Project Up Administration's Sleeve Threatens Privacy Rights of Every American*, L.A. DAILY J., July 31, 2003, at 6 (discussing the possible ramifications of the Bush administration's new LifeLog computer surveillance system on individual privacy).

express "right to privacy" set forth in the Constitution.[5] Nevertheless, in the 1965 landmark case *Griswold v. Connecticut*,[6] the U.S. Supreme Court struck down a Connecticut law banning birth control, basing its decision on a zone of privacy created by several constitutional rights.[7] In writing the opinion of the Court, Justice William O. Douglas wrote, "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy."[8] *Griswold* has been cited since its issuance as one of the foundations of an individual's "right to privacy." Yet, Justice Potter Stewart, in his *Griswold* dissent, stated, "with all deference, I can find no such general right of privacy in the Bill of Rights, in any other part of the Constitution, or in any case ever before decided by this Court."[9] As surely as the Supreme Court justices could not agree on a right to privacy at such a critical time,[10] the debate continues as to where and when the right to privacy exists or is muted by a competing interest.[11]

Similarly, legislative and regulatory treatment of privacy interests has been erratic.[12] As this article will demonstrate, despite

---

5 U.S. CONST; *see also* David J. Garrow, *Privacy and the American Constitution*, 68 SOC. RES. 55, 55 (2001) (discussing the absence of an express right to privacy in the U.S. Constitution).

6 Griswold v. Connecticut, 381 U.S. 479 (1965) (striking down a state law banning the sale of contraceptives based on a right to privacy). In addition, the recently enacted California Financial Information Privacy Act provides more stringent privacy protections than the federal Gramm-Leach-Bliley Act (GLBA). *See* California Financial Information Privacy Act, CAL. FIN. CODE § 4050 et. seq. (1999).

7 *Griswold*, 381 U.S at 485-86 (reversing the opinion of the Supreme Court of Errors of Connecticut).

8 *Id.* at 484. The Court also notes that neither the right of people to associate nor the right to educate a child in a school of the parent's choice are mentioned in the Constitution or the Bill of Rights, but the First Amendment has nevertheless been construed to include such rights. *See id.* at 482.

9 *Id.* at 530 (Black, J., dissenting).

10 *Id.* at 479-531 (comparing the brief majority opinion with the dissenting opinions).

11 *See, e.g.*, Lowe, *supra* note 4, at 6 (discussing the likely subordination of individual privacy interests in the face of the Bush administration's War on Terror).

12 *See* Deron H. Brown, Book Note, 22 T. JEFFERSON L. REV. 251, 255 (2000) (reviewing FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997)).

an apparent growing concern over financial privacy in particular, it is difficult to identify a clear public policy trend with respect to the privacy of consumer financial information.

Unlike some other countries,[13] the United States does not have a comprehensive general privacy statute, but rather focused privacy laws at both the state and federal levels.[14] For example, Congress has enacted federal laws related to healthcare privacy, such as the Health Insurance Portability and Accountability Act of 1996,[15] and consumer financial privacy, such as Title V of the Gramm-Leach-Bliley Act (GLBA).[16] One of the potential spheres of privacy with which Americans have been most concerned in recent years, and thus Congress has been the most active, is the area of financial privacy. This concern may rest on the fact that financial records have an increasing potential to reveal the most information about an individual, among many other things. They may show: to whom political contributions were made; to where one has traveled; investments; items purchased; and social causes and organizations supported.

The rise in concern about financial privacy has correlated strongly with the development of improved data processing and communications technologies. The first federal legislation to address the privacy of consumer financial information was the Fair Credit Reporting Act (FCRA)[17] in 1970.

The FCRA was intended to address consumer perception of

---

13 *See, e.g.*, Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 1, 1995 O.J. (L281) 31, 38 (establishing sweeping privacy requirements for the European Union member states).

14 *See* Gregory T. Nojeim, *Financial Privacy*, 17 N.Y.L. SCH. J. HUM. RTS. 81, 90 (2000). For a comparison of specific federal legislation with state legislation, see Gramm-Leach-Bliley Financial Services Modernization Act, 15 U.S.C. §§ 6801-6809 (2000); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26 U.S.C., 29 U.S.C., 42 U.S.C.); California Financial Information Privacy Act, *supra* note 6; Privacy of Consumer Financial and Healthy Information Regulation, VT. CODE R. 21 020 053 (2002).

15 Health Insurance Portability and Accountability Act of 1996, *supra* note 14.

16 The Financial Modernization Act, Pub. L .No. 106-102, 15 U.S.C. §§ 6801-6809.

17 The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1970).

abusive practices and lack of responsiveness on the part of some credit bureaus and other entities that collect and disseminate credit and other personal information. The FCRA created standards for the collection and maintenance of credit and other consumer information by consumer reporting agencies. The FCRA also limits the dissemination of consumer reports to certain "permissible purposes"[18]and otherwise prohibits disclosure of consumer report information by consumer reporting agencies.

A. The Privacy Act of 1974

Shortly after the enactment of the FCRA, in 1972 then secretary of Health, Education, and Welfare, Elliot L. Richardson, established the Secretary's Advisory Committee on Automated Personal Data Systems. The formation of this committee was in response to growing concerns about the harm that could result from the unfettered use of computer and telecommunications technology to collect, store and use data about individual citizens. The Committee was asked to analyze and make recommendations about: (1) harmful consequences resulting from using automated personal data systems; (2) safeguards that might protect against potentially harmful consequences; (3) measures that might afford redress for any harmful consequences; and (4) policy and practice relating to the issuance and use of Social Security numbers.[19] The resulting report, *Records, Computers and the Rights of Citizens* ("HEW Report") is set forth in the Code of Fair Information Practice, which outlines five fair information privacy principles that were integrated into the Privacy Act. These principles are still relied upon as a basis for privacy and information policy and provided the intellectual foundation[20] for the Federal Privacy Act of 1974 ("Privacy Act").[21]

The Privacy Act regulates information systems maintained by the federal government. The Privacy Act also created the Privacy

---

18 See *id.* § 1681b.

19 Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems, "Records, Computers and Rights of Citizens" Report (1973), *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm (last visited Feb. 22, 2004).

20 *See* ARTHUR A. BUSHKIN & SAMUEL I. SCHAEN, THE PRIVACY ACT OF 1974: A REFERENCE MANUAL FOR COMPLIANCE (System Development Corporation 1975).

21 5 U.S.C. § 552a (1974).

Protection Study Commission, which was charged with investigating and studying privacy protection throughout the United States and making recommendations for future legislation.[22] As a result, the Privacy Protection Commission issued a report entitled *Personal Privacy in the Information Society*.[23]

B. The Right to Financial Privacy Act of 1978

At about the same time, concerns over privacy increased as the federal courts issued several decisions that called into question the privacy of financial records. For example, in *California Bankers Association v. Schultz*,[24] the U.S Supreme Court upheld the Bank Secrecy Act[25] against challenges by the American Civil Liberties Union and the California Bankers Association that its recordkeeping requirements infringed upon a constitutional right to privacy. The Bank Secrecy Act requires financial institutions to keep records of certain financial transactions including making and retaining microfilm copies of all checks over a certain dollar amount.[26] Due to the impracticality of sorting checks for copying by the dollar amount, many banks were copying all checks. Just two years later in *United States v. Miller*,[27] the Supreme Court held that a bank customer does not have a constitutionally protected right of privacy in bank account records; thus, a bank customer lacks standing to challenge, on Fourth Amendment grounds, a bank's disclosure to federal authorities. On the same day as *Miller*, the Supreme Court decided *Fisher v. United States*,[28] which held that an individual has no Fifth Amendment right against compelled self-incrimination that would entitle him to prevent his attorney from producing financial records made by the

---

22 *See id.* at §§ 1905-1909.

23 Privacy Protection Study Commission, Personal Privacy in an Information Society Report (1977), *available at* http://www.epic.org/privacy/ppsc1977report (last visited Mar. 22, 2004).

24 416 U.S. 21 (1974).

25 The Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 11/4 (1970) (codified and amended at 12 U.S.C. §§ 1730d, 1829b, 1951-1959; 31 U.S.C. §§ 5311-5355).

26 12 U.S.C. § 1829b(d).

27 425 U.S. 435 (1976).

28 425 U.S. 391 (1976).

individual's accountant when summoned by the I.R.S. In so holding, the Court reasoned that where records are developed by a third party as a result of an ordinary business relationship, the subject has no constitutionally protected right of privacy in those records.

Congress responded to the Court with what would become the Right to Financial Privacy Act of 1978 (RFPA).[29] Legislative history indicates that the bill that was to become the RFPA was "a congressional response to the Supreme Court decision in *United States v. Miller*."[30] The Act protects customer records maintained by certain financial institutions from improper disclosure to officials or agencies of the federal government.[31] RFPA prohibits a financial institution from disclosing records it holds to the federal government without notification to the customer whose records are being requested and requires a waiting period whereby the customer has the opportunity to challenge the request through legal action.[32] RFPA is limited to disclosures to the federal government, and does not reach requests for customer information made by state or local governments or private parties.[33] RFPA also mandates that the government, among other requirements, provide a covered financial institution a certificate of compliance with RFPA before requested customer information may be released.[34]

There was little opposition to the legislation that would become RFPA. The only significant opposition came from federal law enforcement officials who were concerned that it would impede federal authorities' investigations and prosecutions of crimes, particularly white collar and organized crime.[35]

---

29 Pub. L. No. 95-630, Tit. XI, 92 Stat. 3641, §§ 3697-3710 (1978), codified as amended at 12 U.S.C. §§ 3401-3422 (2004).

30 95th Cong. 2d session, House Report No. 95-1383 (p. 34) (July 20, 1978); *see also* Cong. Rec. Oct. 14, 1978 S.37,570 (remarks of M. Abourezk). "In the celebrated Miller case, the Supreme Court held that the fourth amendment prohibitions against search and seizure did not protect bank records which were part of the daily business of the bank . . . . The Court did not however, rule out a legislative remedy to this very large hole in the constitutional privacy protections of individuals." *Id.*

31 *See* 12 U.S.C. § 3402.

32 *See* 12 U.S.C. § 3410.

33 *See* 12 U.S.C. § 3401.

34 *See* 12 U.S.C. § 3403(b).

35 *See* 124 Cong. Rec. H33,836-37 (daily ed. Oct. 5, 1978) (remarks of Rep.

C. 1996 Amendments to the FCRA

In 1996, the FCRA was amended to clarify various aspects of the obligations of consumer reporting agencies and the uses of consumer reports. Most significantly from a privacy standpoint, the 1996 amendments expanded the ability for related entities to share consumer reports among affiliates if it is clearly and conspicuously disclosed to the consumer that the information may be shared among affiliates and the consumer is given the opportunity to opt out of affiliate sharing prior to such disclosure.

D. Know Your Customer Rule

While the issue of privacy of individual financial information had been relatively quiet since the enactment of RFPA, a growing concern over money laundering led federal bank regulatory agencies in 1998 to take a step that was widely perceived by the public as an attack on the privacy of financial information.

On December 7, 1998, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and the Office of Thrift Supervision (the "Banking Agencies") published for public comment the proposed "Know Your Customer Rule."[36] The Know Your Customer Rule was intended to implement 12 U.S.C. 1818(s).[37] This statute requires the Banking Agencies to prescribe regulations requiring depository institutions to establish and maintain procedures reasonably designed to ensure and monitor compliance with the Bank Secrecy Act.[38] The Know Your Customer Rule was designed to thwart illicit financial activities that pose a serious threat to the integrity of financial institutions, such as money laundering and fraud.[39] The Know Your Customer Rule was premised on the notion that when financial institutions identify their customers and determine what transactions are normal and expected for these customers, they can monitor transactions to identify unusual or suspicious account activity.[40]

Cavanaugh).

36 63 Fed. Reg. 67,536 (proposed Dec. 7, 1998) (withdrawn Mar. 23, 1999).

37 *See id.*

38 31 U.S.C. § 5311 et seq.

39 *See* 63 Fed. Reg. 67,536.

40 *See id.*

By identifying and reporting unusual or suspicious transactions, financial institutions could protect their integrity and assist the Banking Agencies and law enforcement authorities in stifling illicit activities.[41]

As proposed, the Know Your Customer Rule would have required each bank to develop a program to determine the identity of its customers; determine its customers' sources of funds; determine, understand, and monitor the normal expected transactions of its customers; and report any transaction of its customer that appeared suspicious in accordance with the existing suspicious activity report requirements.[42] When the public comment period for the regulation ended on March 8, 1999, the Banking Agencies had received an unprecedented number of comments (totaling over 250,000 to the FDIC alone[43]) on the proposed rule from the public, banking organizations, industry associations, and members of Congress. Of those comments received, most of the comments voiced concern over the privacy of information that would be collected and held by financial institutions and many expressed concern about the added burden on banks.[44] As the opposition letter filed by the American Bankers' Association stated:

The terminology used in this proposal clearly raises great concern about privacy. Media reports have focused especially on the profiling and monitoring wording, and privacy advocates have expressed outrage that their local banker will be required to analyze all customers' transactions. This growing public view has so tainted the discussion of this regulation that assurances of deletion of the profiling term will not be sufficient, we believe, to

---

41 *See id.*

42 In its present version, 12 C.F.R. § 21.11 requires national banks to report known or suspected criminal offenses, at specified thresholds, or transactions aggregating $5,000 or more if bank officers suspect the transactions involve money laundering or violation of the Bank Secrecy Act.

43 *See Hearing before the Subcomm. on Commercial and Administrative Law* (Mar. 4, 1999), *available at* http://www.house.gov/judiciary/106-39.htm (statement of Rep. Barr, Member, House Subcomm. on Commercial and Administrative Law).

44 Joint Statement, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision, *Proposed "Know Your Customer" Rule* (Mar. 23, 1999), *available at* http://www.federalreserve.gov/boarddocs/press/boardacts/1999/19990323/statement.HTM.

calm the public. This concern goes beyond the propriety of a [Know Your Customer] proposal.[45]

Indeed, opposition was so strong that a bill was introduced in the 106th Congress (HR10) to provide for the hault of the Know Your Customer Rule.[46] As then Representative Bob Barr (R-GA), one of the chief proponents of the bill noted:

Essentially, these regulations propose requiring banks to compile detailed information on the financial transactions of their customers without any regard to whether those customers are suspected of criminal wrongdoing. This information then becomes your personal profile. If that profile simply indicates a recent transaction is out of character, your bank is forced to report your finances to the government.[47]

Barr continues "It is highly unlikely, even ludicrous, to assume that profiling the salary deposits, ATM fees, and mortgage payments of millions of Americans will have a significant impact on the activities of criminals."[48] These regulations assume that millions of law-abiding Americans are potential criminals, simply because they have a checking account. Existing law already provides more than adequate authority to fight money laundering.[49]

In the Joint Press Release announcing the withdrawal of the Know Your Customer Rule, Comptroller Hawke is quoted as testifying before the House Judiciary Committee, Subcommittee on Commercial and Administrative law that, "I firmly believe that any marginal advantages for law enforcement in this proposal [Know Your Customer Rule] are strongly outweighed by its

---

45 Letter from Edward L. Yingling on behalf of the American Bankers' Association to Banking Agencies (Jan. 28, 1999), *available at* http://www.aba.com/aba/static/KYC_Commentltr.html (calling for the withdrawal of the proposed "Know Your Customer" Rule) (on file with the North Carolina Journal of International Law and Commercial Regulation).

46 H.R. 10 100th Cong. § 191 (1999).

47 *Oversight Hearing on "The 'Know Your Customer' Rules: Privacy in the Hands of Federal Regulators" Before the House Com. and Admin. L. Subcomm.*, 106th Cong. (1999) (testimony of U.S. Rep. Bob Barr), *available at* http://www.house.gov/judiciary/106-39.htm (on file with the North Carolina Journal of International Law and Commercial Regulation).

48 *Id.*

49 *Id.*

potential for inflicting lasting damage on our banking system."[50]

Even after the withdrawal of the proposed Know Your Customer Rule, animosity still lingered. For example, the American Civil Liberties Union launched a "Know Your Banker" campaign which encouraged consumers to write a letter to their banker requesting information about the bank's policies regarding the privacy of consumer financial information.[51]

E. GLBA

The concern for financial privacy evidenced by the public response to the Know Your Customer Rule appeared to continue with adoption of the GLBA. The GLBA, which was signed into law on November 12, 1999, contains the most comprehensive federal financial privacy provisions ever enacted, requiring a financial institution to protect the security, integrity, and confidentiality of customer information. The privacy provisions are found in Title V of the GLBA, which is broken down into two subtitles: Subtitle A creates new substantive obligations relating to the disclosure of customer information by financial institutions to nonaffiliated third parties;[52] Subtitle B establishes new federal prohibitions relating to the fraudulent acquisition of customer information from a financial institution.[53] The GLBA affects an extremely wide range of organizations. It applies to "financial institutions" which means any entity "the business of which is engaging in financial activities" as described in section 4(k) of the Bank Holding Company Act of 1956[54] which includes, among others, banking institutions, insurance companies, and securities firms.

---

50 Press Release, Office of the Comptroller of the Currency, Comptroller Says "Know-Your-Customer" Rule Should be Rejected, OCC Release No. 99-17 (Mar. 4, 1999), *available at* http://www.occ.treas.gov/ftp/release/99%2D17.txt (on file with the North Carolina Journal of International Law and Commercial Regulation).

51 Press Release, American Civil Liberties Union of San Diego and Imperial Counties, ACLU Denounces Bank Spying; Urges Customers to "Know Your Banker," (may 10, 1999), *available at* http://www.aclusandiego.org/KNOWYOURBANKER.htm (on file with the North Carolina Journal of International Law and Commercial Regulation).

52 *See* 15 U.S.C. §§ 6801-6809 (1999).

53 *See* 15 U.S.C. §§ 6821-6827 (1999).

54 *See* 12 U.S.C. §§ 1841-1850 (1956).

The GLBA only limits the disclosure of "nonpublic personal information" which is defined as personally identifiable information about a consumer or consumers and any list or grouping of consumers created by using personally identifiable information.[55] Nonpublic personal information does not include publicly available information.[56]

The GLBA generally prohibits the disclosure of nonpublic personal information about a consumer to nonaffiliated third parties unless notice and opt-out is delivered to that consumer.[57] Notices must be provided to consumers initially and annually thereafter to those consumers with whom a continued relationship exists (customers).[58] Notices must include the categories of nonpublic personal information that a financial institution collects and the categories that it discloses.[59] Notices must also identify what categories of nonpublic personal information are disclosed to affiliated and to nonaffiliated third parties.[60] When a notice is required, consumers must also be given the opportunity to opt-out of the disclosures unless such disclosures are made within one of the exceptions.[61]

Although considered by some as a significant advance in privacy protection, the GLBA has been criticized for permitting affiliate sharing and relying on an opt-in, instead of an opt-out for non-affiliate sharing. Perhaps more significantly to the GLBA opt-out is subject to a long list of exceptions.[62] For example, no notice is required for disclosures that are necessary to a transaction requested or authorized by a consumer.[63] No notice is required for disclosures related to the servicing or processing of a financial product requested or authorized by a consumer.[64] No notice is required for disclosures made in connection with the maintenance

---

55 15 U.S.C. § 6809(4) (1999).

56 15 U.S.C. § 6809(4)(B) (1999).

57 15 U.S.C. § 6803 (1999).

58 *Id.*

59 *Id.*

60 *Id.*

61 *Id.*

62 15 U.S.C. § 6802 (1999).

63 15 U.S.C. § 6902(e)(1) (1999).

64 *Id.*

or service of a consumer account and disclosures may always be made with a consumer's consent.[65] In addition, financial institutions need not provide opt-out for disclosures to nonaffiliated third parties made in order to perform services for or functions on behalf of the financial institution, or market the financial institution's own products or services or the products or services of the third party under a joint-marketing agreement.[66] The net effect of the GLBA is that it serves primarily as a limitation on the disclosure of information for marketing purposes.

F. USA PATRIOT Act

Before the dust had settled from the attacks on New York City and Washington, D.C. on September 11, 2001 ("September 11th"), the public's outrage at the proposed Know Your Customer Rule by the Banking Agencies and the concern that fostered the GLBA requirements addressed more pressing concerns. In the wake of the attacks of September 11th, privacy advocates took a back seat to the desire to use the financial system to detect and thwart terrorism. As stated by the Congressional Office of Technology Assessment, "It takes money for weapons and explosives. It takes money to get terrorists to their targets, and then into hiding."[67]

Congress quickly responded by enacting the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act")[68]—passed in the wake of the September 11th terrorist attacks. The stated purpose of the USA PARIOT Act is to enable law enforcement officials to track down and punish those responsible for the attacks and to protect against any similar attacks.[69] The USA PATRIOT Act grants federal officials greater powers to trace and intercept terrorists' communications both for

---

65 15 U.S.C. § 6802(e)(1)(B) (1999).

66 15 U.S.C. § 6802(b)(1)(C)(2) (1999).

67 UNITED STATES CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION TECHNOLOGIES FOR CONTROL OF MONEY LAUNDERING 121, OTA-ITC-630 (Washington, D.C: U.S. Government Printing Office, Sept. 1995).

68 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

69 *See id.*

law enforcement and foreign intelligence purposes.[70] The USA PATRIOT Act also expanded the authority of the Federal Bureau of Investigation and law enforcement to gain access to business records, medical records, educational records, and library records, including stored electronic data and communications.[71] With respect to financial information, the USA PATRIOT Act requires financial institutions to take additional steps to Know Their Customer by verifying their identity and provides the government with more effective means to access that information.[72]

Treasury rules to implement Section 314 of the USA PATRIOT Act allow a federal law enforcement agency investigating terrorist activity or money laundering to request that the Financial Crimes Enforcement Network ("FinCEN"), on the agency's behalf, provide certain financial information from a financial institution or group of financial institutions.[73] FinCEN, on behalf of the agency, may require a financial institution to search its records to ascertain whether the financial institution maintains or has maintained accounts for, or conducted transactions with, the individual or entity specified.[74] The rule sets a floor for such inquiries whereby the requesting agency need only certify that each individual or entity that is the subject of the request is "engaged in, or is reasonably suspected based on credible evidence of engaging in, terrorist activity."[75] The certification also must contain certain identification information.[76] The information that must be reported back by the financial institution, if a match is found in the financial institution's records, is limited to the name or account number of each individual or entity for which a match is found, a social security number and date of birth, or other similar identifying information that was provided by the subject of the information when the account was

---

70 CHARLES DOYLE, THE USA PATRIOT ACT: A LEGAL ANALYSIS, CRS Report for Congress, Order Code RL 31377, at 1-2 (2002).

71 *Id.* at 1-2, 68.

72 *Id.* at 1-2.

73 Financial Record-Keeping and Reporting of Currency and Foreign Transactions, 31 C.F.R. § 103.100 (2004).

74 *Id.* § 103.100(b)(1) (2004).

75 *Id.*

76 *Id.*

opened or the transaction conducted.[77] The rule further provides that the RFPA shall not stand as an obstacle to responding to these requests.[78] Although the information to be provided in response to these requests is limited to the Section 314 rules, it effectively reinstates the *Miller* rule with respect to this information.

In addition, Section 326 of the USA PATRIOT Act added a new subsection to 31 U.S.C. § 5318 of the Bank Secrecy Act. This subsection requires that the regulations setting forth the minimum standards for financial institutions[79] and their customers regarding the identity of the customer that apply in connection with the opening of an account at a financial institution.[80] Joint Treasury and federal banking agency rules to implement Section 326 of the USA PATRIOT Act require financial institutions to adopt reasonable procedures to "verify the identity of any person seeking to open an account to the extent reasonable and practicable, to maintain records of the information used to verify the person's identity, and to determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency."[81]

"Under the Section 326 rules, a bank must implement a written customer identification program ("CIP") appropriate for the size and type of business"[82]of the bank. "The CIP must include risk-based procedures to allow the bank to form a reasonable belief that it knows the true identity of each of its customers."[83] Such

---

77 *Id.* § 103.100(b)(2)(ii) (2004).

78 *Id.* § 103.100(b)(2)(iv)(B)(3) (2004).

79 The Bank Secrecy Act broadly defines "financial institution" and includes a variety of entities including: commercial banks; agencies and branches of foreign banks in the United States; thrifts; credit unions; private banks; trust companies; investment companies; brokers and dealers in securities; futures commission merchants; insurance companies; travel agents; pawnbrokers; dealers in precious metals; check cashers; casinos; and telegraph companies. *See* Bank Secrecy Act, 31 U.S.C. § 5312(a)(2) and (c)(1)(A) (2001).

80 68 Fed. Reg. 25090 (May 9, 2003).

81 *Id.*

82 Financial Recordkeeping and Recording of Currency and Foreign Transactions, 68 Fed. Reg. 25109 (May 9, 2003) (to be codified at 31 C.F.R. pt. 121(b)(1)).

83 Financial Recordkeeping and Recording of Currency and Foreign Transactions, 68 Fed. Reg. 25109 (May 9, 2003) (to be codified at 31 C.F.R. pt. 121(b)(2)).

"procedures must be based on the bank's assessment of" the risks related to the bank's business, including the types of accounts the bank maintains, "methods of opening accounts" used by the bank, "types of identifying information available, and the bank's size, location, and customer base."[84]

At a minimum the following information is required from the customer prior to opening an account: (1) name, (2) date of birth, (3) address, which shall be the residential or business street address of the individual, or an APO or FPO for an individual without a residential or business street address, or the residential or business street address of the next of kin or other contact; or for a person other than an individual, a principal place of business, local office or other physical location; and (4) an identification number which shall be for a U.S. person a taxpayer identification number, passport number and country of issuance, alien identification number or number and country of issuance of any other government-issued document that shows nationality or residence and bearing a photograph or similar safeguard.[85]

While the FDIC alone received more than 250,000 negative comments on the Know Your Customer Rule, Treasury and the banking agencies collectively received approximately five hundred comment letters in response to the USA PATRIOT Act proposed rule.[86] The comments on the proposed rule were largely from industry members and associations and did not express the general outrage that sprung from the Proposed Know Your Customer Rule.[87] Only a small number of comments were received from individuals, and of those, only some criticized the rule as an infringement upon individual liberty and privacy.[88]

G. The FACT Act

On December 4, 2003, President George W. Bush signed into law the Fair and Accurate Credit Transactions Act of 2003

---

84 *Id.*

85 Financial Recordkeeping and Recording of Currency and Foreign Transactions, 68 Fed. Reg. 25109 (May 9, 2003) (to be codified at 31 C.F.R. pt. 121(b)(2)(i)(A)).

86 63 Fed. Reg. 25091.

87 *Id.*

88 *Id.*

("FACT Act").[89] The FACT Act permanently reauthorized the national uniformity provisions of the FCRA.[90] Other provisions of the FACT Act were designed to assist both consumers and financial institutions in the fight against identity theft.[91] The FACT Act was based on a recognition by Congress that the growth in technology and the free flow of information was accompanied by the burgeoning crime of identity theft. A number of the identity theft provisions rely on the same type of customer identification processes required under Section 326 of the USA PATRIOT Act. For example, the FACT Act adds a new section 605A to the FCRA, establishing three instances where consumers or military personnel can direct a nationwide consumer reporting agency, as defined under section 603(p) of the FCRA,[92] to include a fraud alert or an active duty alert in each consumer report furnished on those consumers.[93] The fraud alerts, provided for by the FACT Act, are designed to clearly and conspicuously notify users of consumer reports that the consumer may have been a victim of identity theft or other fraud, or that the consumer is on active duty in the military. Therefore, users are warned to verify the identity of the consumer before establishing a new credit plan or loan obligation or issuing an additional card when requested by a consumer with an alert in his or her file.[94] The legislative history of this provision reflects that fraud alerts were designed specifically to limit opportunities for criminals to harm consumers in situations involving the use of a credit report and that the provision was intended only to apply when a credit report is being pulled to provide new credit or extend existing credit limits, requested by consumers.[95] The FACT Act requires a consumer

---

89 Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 117 Stat. 1952 (2003).

90 Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114 (1970) (codified at 15 U.S.C. § 1681).

91 Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 117 Stat. 1952 (2003).

92 15 U.S.C.A. § 1681a(p) (2003).

93 Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 117 Stat. 1952 § 112(a), (2003) (codified as amended at 15 U.S.C.A. § 1681c-1(a)(1)(A)).

94 *Id.* (codified as amended at 15 U.S.C.A. § 1681c-1(h)(1)(A).

95 S. REP. NO. 108-166, at 11 (2003).

reporting agency to place a fraud alert[96] on a consumer's credit file consistent with the requirements of the FACT Act, when one is requested by the consumer.[97] This fraud alert provides all prospective users of a consumer report on the consumer with a warning that the consumer does not authorize the establishment of any new credit plan or other new credit obligation in the consumer's name, unless the user verifies the identity of the person making the request in an appropriate manner.[98]

The legislative history notes that what constitutes reasonable verification standards intentionally was not described in detail, with the expectation that users will consider various mechanisms, including the verification requirements of section 326 of the USA PATRIOT Act.[99]

Further, the FACT Act requires the Banking Agencies, the National Credit Union Administration ("NCUA") and the FTC to jointly establish procedures for the identification of possible instances of identity theft – *i.e.*, "red flag" guidelines and regulations.[100] The legislative history for this provision elucidates that this requirement was expected to result in the development of broad guidelines, thus resulting in policies and procedures that vary from institution to institution.[101] The legislative history further explains that many institutions already have such policies and procedures in place as a result of the new account verification requirements of Section 326 of the USA PATRIOT Act[102] and the FACT Act requires that the policies and procedures established under the "red flag" guidelines shall not be inconsistent with the policies and procedures required by Section 326 of the USA PATRIOT Act.[103]

---

96 A fraud alert is defined as a statement in a consumer's file that the consumer may be a victim of identity theft or other fraud. 15 U.S.C.A. § 1681c-1(a)(1) (2003).

97 FACT Act, Pub. L. No. 108-159 § 112(a), 117 Stat. 1953 (2004) (to be codified at 15 U.S.C. §§1681c-1(a)-(b)).

98 FACT Act, Pub. L. No. 108-159 § 112(a), 117 Stat. 1953 (2004) (to be codified at 15 U.S.C. § 1681c-1(h)(1)(B)(i)).

99 H.R. REP. NO. 108-263, at 40-41 (2003).

100 FACT Act, Pub. L. No. 108-159 § 114, 117 Stat. 1953 (2004) (to be codified at 15 U.S.C. § 1681m(e)(1)(A)-(B)).

101 S. REP. NO. 108-66, at 13 (2003).

102 *Id.*

103 FACT Act, Pub. L. No. 108-159 § 114, 117 Stat. 1953 (2004) (to be codified at

While the FACT Act encourages financial institutions to know their customers, it also addresses the perceived gap left by the GLBA rules with respect to the affiliate sharing of information but does so in a unique way by focusing on the use of the information rather than its disclosure. The FACT Act adds a new section 624 to the FCRA which provides that an institution that receives either experience information or consumer report information on a consumer from an affiliate may not use such information for marketing solicitation to the consumer about the institution's products or services, unless the institution clearly and conspicuously discloses to the consumer that information received from affiliates may be used for marketing purposes and the consumer is given an opportunity and method to opt out of receiving such marketing solicitations.[104] The legislation clarifies that this section does not limit the ability of affiliates to share information, nor does it limit their ability to establish and maintain a database of information shared by affiliates; rather, it only requires notice of such sharing before the information is used to send marketing solicitations.[105] Affiliates, however, are allowed to share information without limitation, so long as it is not used for marketing solicitations without first providing notice and opt-out.[106] Under this new section, the opt-out notice may be provided to the consumer together with disclosures required by any other provision of law, such as those required by GLBA.[107]

III. Conclusion

A fundamental right to privacy of financial information does not exist in U.S. law. Where U.S. citizens are willing to have defined the edges of their right to privacy defined, it is shaped not by a fundamental right to privacy itself but by the strength of those forces bearing down upon it. The proposed Know Your Customer Rule was conceived at a time where the American people felt comfortable in their homes; yet September 11th eroded that

---

15 U.S.C. § 1681(m)(e)(3)).

104 FACT Act, Pub. L. No. 108-159 § 214(a), 117 Stat. 1953 (2004) (to be codified as amended at 15 U.S.C. § 1681s-3(a)(1)).

105 149 CONG. REC. 176, at E2512 (Dec. 9, 2003).

106 *Id.*

107 15 U.S.C. §§ 6802-03 (2003).

confidence. As a result, people's immediate concerns shifted from fearing the state as a predator to wanting the state as protector. Indeed, while the implementing regulations for the USA PATRIOT Act were in many ways similar to the requirements of the proposed Know Your Customer Rule, the USA PATRIOT Act rule did not draw any significant opposition on privacy grounds.

The U.S framework for financial privacy is, and will be, responsive to the external forces of the time. The United States values the free flow of information, and the rewards that come from it. For example, credit reporting enables people to pay rates on credit that more accurately reflect the individual's credit risk, rather than absorbing the cost to the financial institution of offering credit to those who pose a greater credit risk. A recent trend in consumer privacy can be seen in the FACT Act provision that limits the uses of consumer information, rather than the transfer of this information. This notion of limiting the use of the information, rather than the flow, may signal a new approach to privacy in a world that cannot deny the perpetual advancement of information technology.