NEW YORK LAW SCHOOL

NYLS Journal of Human Rights

Volume 17 | Issue 1 Article 9

2000

Remarks of Dolores S. Smith

Dolores S. Smith

Remarks of Dolores S. Smith

Dolores S. Smith[1]

Title V of the Gramm-Leach-Bliley Act (GLBA) gives consumers new rights, both to learn about and to control the sharing of personal information by their financial institutions.[2] Title V directs the Board and other Federal agencies to issue implementing regulations, and to make these regulations as consistent as possible.[3] In keeping with this mandate, the Board and the other Federal banking agencies jointly issued final regulations on June 1, 2000.[4]

To provide context for our discussion of consumer financial privacy, I will give some background about the topic. Then, turning specifically to the GLBA and the banking agencies' regulations, I will highlight several issues regarding consumer financial privacy that the legislation raised and the regulations resolved.

I. BACKGROUND

One might well ask: Why are consumer privacy protections included in a financial modernization law? One explanation is that in recent years concerns about consumer financial privacy have become increasingly prominent in the media, among members of the public, the financial industry, and the Congress.[5] For example, privacy figures increasing on the editorial and "op-ed" pages of newspapers as an important public policy issue.[6] Recent surveys show that identity

---

[1] Ms. Smith's remarks, delivered March 28, 2000, have been updated to take account of subsequent events, through the issuance of final regulations under the consumer financial privacy provisions of the Gramm-Leach-Bliley Act.

[2] *See* Title V of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801.

[3] *See* 15 U.S.C. § 6804.

[4] *See* Banks and Banking, 12 C.F.R. § 216 (2001).

[5] *See, e.g.,* Joseph B. Cahill, *Banks Release of Client Data is Examined,* WALL ST. J., Sept. 27, 1999.

[6] *See* Paul Gigot, *Editorial, Privately Held Concerns*, WALL ST. J., Sept. 27, 1999.

theft associated with the disclosure of personal information is among consumers' leading concerns.[7]

The increasing prominence of privacy concerns, in turn, is related to a number of factors. I will mention some of them. One is the European Union ("EU") directive on privacy.[8] The directive was adopted in 1995 and was followed by negotiations, highly publicized in some sectors, between U.S. officials and EU representatives. At issue was whether U.S. laws provide privacy protections sufficiently comparable to those established by the EU. At stake was the need to ensure that U.S. firms are not placed at a competitive disadvantage by being barred from receiving consumer information from member countries of the EU. U.S. and EU officials agreed on "Safe Harbor Principles" that would permit compliant U.S. firms to do business in Europe without being barred from receiving consumer information.

A second factor is consumers' growing use of the Internet. This use has been accompanied by industry efforts to collect data about consumers and about their Internet activities. There is a corresponding rise in consumers' concerns about the confidentiality of financial data that they provide and that are captured and transmitted on-line; and growing interest on the part of Federal agencies about the practices that financial institutions follow with respect to customer privacy.[9] In 1999, the four bank and thrift regulators surveyed the privacy disclosures posted at the Web sites of the institutions they regulate. Earlier this year, the Federal Trade Commission surveyed on-line privacy disclosures more generally.[10]

---

[7] *See American Opinion (A Special Report): Bright Past Kindles America's Hope,* WALL ST. J., Sept. 16, 1999 (publishing results of a Wall Street Journal/NBC Poll that Americans cite loss of personal privacy as their utmost concern about the future, ahead of overpopulation, terrorism, and global warming).

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 of Oct. 1995 (OJ 1995 L 281/31) (governing the protection of individuals with regard to the processing of personal data and the free movement of such data).

[9] Amber Veverka, *Federal Agencies Schedule Public Comment on Banking-Privacy Law*, KNIGHT RIDDER/TRIB. BUS. NEWS, Jan. 22, 2000 (explaining legislators' renewed interest in privacy protection).

[10] *See Privacy Online: Fair Information Practices in the Electronic Marketplace: Hearings before Fed. Trade Comm.*, 106th Cong. (2000) (statement of Robert Pitofsky, Chairman of the Fed. Trade Comm.).

Third, in 1999 Minnesota's Attorney General sued U.S. Bancorp, alleging that its information sharing practices violated state and federal law.[11] This high-profile lawsuit spotlighted financial disclosure practices on the part of banks that were a surprise to many of us. Until then a general assumption was that our financial records, were, for the most part, kept confidential by banks.[12] Instead, we learned that U.S. Bank, and others, were routinely selling consumer data to telemarketers and other third parties. More recently, the Attorney General of New York expressed similar privacy-related concerns to the Chase Manhattan Corporation.[13] Mr. Mindell, on our panel today, represented the Attorney General of New York regarding this matter.[14] I look forward to hearing from him about it.

Fourth, financial modernization and consumer privacy are two sides of the same coin. The GLBA enables financial institutions to diversify their activities. To attain the maximum benefit from this diversification, institutions want to expand their collection, analysis, and use of consumer data.[15] Indeed, one of the main incentives for financial and non-financial firms to affiliate is to pool their consumer data to gain economies of scale from investments in information

---

[11] *See generally,* David Ramp, *Minnesota Settles With U.S. Bancorp,* TELEMARKETING FRAUD BULLETIN, Aug. 1999 at 1; *see also* Michael Sisk, *Data Management: Consumer Privacy Moves to the Forefront,* FUTURE BANKER, Sept. 6, 1999, at 42 (citing the complaint alleging violations of the Fair Credit Report Act and fraudulent and deceptive practices).

[12] *See* Ron Insana, *Many People Are Not Aware that Banks Sometimes Give Out Personal Financial Information to Companies,* CNBC TRANSCRIPTS, Aug. 4, 1999 (identifying seventy-nine-year-old Albert Newman, bank consumer, who was unaware of his bank's practice).

[13] Winnie Hu, *Chase Bank Agrees to Stop Sharing Data,* N.Y. TIMES, Jan. 26, 2000 at B1; *see also* Press Release, Office of the N.Y. State Attorney General Eliot Spitzer, Spitzer Secures Privacy Agreement with Nat'l Bank (Jan. 25, 2000) *available at* http://www.oag.state.ny.us (describing the *Chase Manhattan* case).

[14] Press Release, Office of the N.Y. State Attorney General Eliot Spitzer, Spitzer Secures Privacy Deal with National Bank (Jan. 25, 2000) *available at* http://www.oag.state.ny.us.

[15] *See The Privacy Revolution* FIN. SERVICES ALERT (Goodwin, Procter & Hoar, LLP, US).

technology, and to cross-market products more effectively.[16] These developments, naturally, sharpen consumers' concerns about the privacy of their financial data.

Lastly, financial privacy is an issue that legislators find themselves responding to, not just as Members of Congress, but also, as consumers. For example, last year, as the House Committee on Banking and Financial Services was marking up H.R. 10, a predecessor to the GLBA, a privacy amendment was introduced, permitting customers to opt out of certain information sharing.[17] In debating the amendment, many Committee members realized, perhaps for the first time, that their own financial data were largely unprotected by federal law.[18] Although the amendment was not adopted at the time, it raised Members' consciousness, and privacy protections became a necessary adjunct to financial reform.[19] Ultimately, consumer privacy protections became an important point of negotiation among Members of Congress as the banking reform legislation advanced.

II. LEGISLATION

The statutory provisions contained in the GLBA relate to a number of different aspects of consumer financial privacy. Besides giving consumers new rights to learn about and control data-sharing in their relationships with financial institutions, the Act directs the Federal banking agencies to set standards for the security, confidentiality, and integrity of customer data held by financial

---

[16] *See* Robert Dodge, *Congress Considers How Companies Are Using Your Data*, CHARLESTON GAZETTE, June 8, 1999 at 6D (citing how companies may form conglomerates to use consumer data).

[17] 145 CONG. REC. H 5305 (March 10, 1999).

[18] *See id.*

[19] *See* Bryan Amendment No. 316 (proposed 1999) (amending Title VII-Financial Information Privacy to permit customers to opt out of sharing of confidential information).

institutions.[20] It seeks to combat "pretext calling," which is the practice of fraudulently obtaining customer information from a financial institution (or even from the customer).[21] It reinstates the banking agencies' authority to enforce the Fair Credit Reporting Act (FCRA), which governs the disclosure of information to, and by, consumer reporting agencies.[22] The Act also calls for the Department of the Treasury (in conjunction with other agencies, including the Board) to study the sharing of consumer data among affiliated financial institutions.[23]

At this point, let me interject a reminder: The privacy provisions we are discussing restrict only the sharing of information with nonaffiliated third parties. In 1996, the Congress amended the FCRA to provide, that an institution can share consumer reports with its affiliates without incurring the responsibilities of a consumer reporting agency (which could be onerous), so long as the institution gives the consumer the opportunity to opt out of the institution's intended sharing of information.[24] This state of affairs continues under the GLBA. And neither the FCRA nor the privacy provisions of the GLBA give consumers an opt-out right with respect to an institution's sharing of "transaction or experience information" with its affiliates. An example of "transaction or experience information" is the payment record on a consumer's credit account with the institution that is sharing the information.[25]

---

[20] *See* Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6801 (a), (b) (West Supp. 2000) (directing financial institutions to set standards regarding privacy and security of customer personal information).

[21] *See id* at § 6821 (making it a violation to fraudulently obtain or disclose information held by a financial institution, relating to another person).

[22] *See* Fair Credit Reporting Act of 1970 (FCRA) 15 U.S.C.A. § 1681 (a) (West 1999).

[23] *See* 15 U.S.C.A. at § 6808 (a) (2000) (studying the purposes, risks and benefits of information sharing among financial affiliates).

[24] *See* 15 U.S.C.A. at § 6802 (b) (2000).

[25] *Id.*

III. REGULATIONS

In turning to the specifics of the regulations, let me say that because the Act is very complex in some areas, so are the regulations. Accordingly, what follows is, in some respects, a simplification of the regulations.

The regulations establish several basic duties.[26] First, a financial institution must refrain, under certain circumstances, from disclosing "nonpublic personal information" about a consumer to a nonaffiliated third party, unless the financial institution has given the consumer specified notices about its privacy policies and about the consumer's right to opt out, together with a reasonable opportunity to opt out, and the consumer has not opted out.[27] Second, a financial institution *receiving* nonpublic personal information from a nonaffiliated third party may re-disclose, or re-use it, only in certain ways.[28] Third, subject to some limited exceptions, a financial institution must not disclose credit card and certain other account numbers to nonaffiliated third parties for use in telemarketing, direct-mail marketing, or marketing by e-mail. Lastly, again subject to limited exceptions, a financial institution must notify a customer about the institution's privacy policies no later than when the institution establishes the customer relationship, and no less than annually while the relationship continues.[29]

The agencies addressed many issues in crafting the regulations that set forth these duties. I will highlight five issues.

First, how much of the data obtained by a financial institution is subject to consumer choice and control? This broad issue involved several sub-issues. One was: does the Act give consumers notice-and-opt out rights only over data that are thought to be "intrinsically financial," or also over other data obtained by a financial institution in connection with providing a financial product or service? The

---

[26] *See* §§ 6802–6803 (2000) (establishing opt-out right and disclosure obligations).

[27] *See* § 6802 (a) (2000).

[28] *See id.* at (c) (placing limits on the reuse of information).

[29] *Id.* (discussing the privacy policies of Title V of the Gramm-Leach-Bliley Act); *see also* Ted Dreyer, *Privacy Matters*, NAT'L L. J., vol. 22, no. 48, B6 (July 2000).

regulations interpret the Act as protecting not only data about matters involving money, but also as protecting other information obtained by the financial institution in the course of providing a financial product or service.[30]

Second, under the statute, the consumer's rights generally do not extend to information that is "publicly available." But, what does that term mean? The agencies concluded that it means information that the institution has a reasonable basis to believe is lawfully available to the general public.[31] The regulations specify three sources of this information: government records, widely distributed media, and disclosures to the general public that are mandated by law.[32] Let us take an example involving a widely distributed medium: the telephone book. Given the existence of unlisted numbers, an institution could treat a consumer's telephone number as publicly available information if the institution has located the telephone number in the telephone book, or if the consumer has informed the institution that the telephone number is not unlisted. But an institution could not reasonably believe that all telephone numbers are available to the public.

A third sub-issue was whether the Act gives consumers the rights over only the data they provide once an account has been opened or a loan extended. The regulations take a broader approach, so that consumers' rights also apply to information provided in an application.

And a fourth sub-issue was: does the Act give consumers rights over the presence of their names on a customer list disclosed by a financial institution? The regulations generally answer "yes," meaning that most lists of customer names may be disclosed only if the customers whose names are included receive notice and the right to opt out.[33]

---

[30] Michael Nelson, *First Annual Institute on Privacy Law: Strategies for Legal Compliance in a High Tech and Changing Regulatory Environment*, 607 PLI/PAT 231, 343 (2000).

[31] *Id.* at 340; *See also* 12 C.F.R. § 3 (p).

[32] 12 C.F.R. § 216.3 (p).

[33] *Id.* at § 216.3 (n).

A second major issue was: who must receive notice? The Act makes clear that financial institutions must provide notice to consumers who enter into (or who are in) continuing relationships with the institutions. What about other consumers, such as individuals who engage in isolated transactions with a financial institution? For example, is an individual who buys a teller's check from a bank entitled to a privacy notice, regardless of whether the bank discloses data about the consumer, and regardless of whether the bank and the individual have a continuing relationship? The regulations say that, in such cases, the individual is not entitled to a privacy notice.[34]

Third, when are financial institutions required to provide a consumer with a privacy notice? The regulations balance the interests of consumers and financial institutions in this regard.[35] The regulations generally require institutions to provide notices before disclosing data or establishing a continuing relationship. Institutions must provide notices long enough before disclosing data, to afford consumers a reasonable opportunity to opt out.[36] But institutions need not provide privacy notices far in advance of establishing a customer relationship. For example, they need not attach privacy notices to their credit card "take one" applications made available at retail stores and other locations. Moreover, in some limited circumstances, such as when institutions acquire deposit accounts without the accountholders' approval, they may provide privacy notices after the customer relationship has been established.[37]

Fourth, what should be the content of privacy notices? The agencies had to decide whether privacy notices should be very cursory, very detailed, or something in between. The regulations take a middle course, requiring that consumers receive needed information while mitigating information overload. For example, the statute generally requires that an institution's privacy notice identify the categories of persons to whom the institution discloses nonpublic

---

[34] *Id.* at § 216.4 (b).
[35] *Id.* at § 216.4 (a).
[36] *Id.*
[37] 12 C.F.R. § 216.4 (e).

personal information. The regulations reflect this requirement without, however, mandating that the categorization be excessively detailed.[38] An institution need only identify three categories of recipients, and provide a few examples of each category.

Fifth, how many different ways of opting out must a financial institution provide, and how user-friendly must they be? Again, the agencies struck a balance, permitting financial institutions to provide single means of opting out, so long as it is reasonable for the consumer to whom it is provided.[39] The regulations offer examples of what is deemed reasonable, including check-off boxes in prominent locations on application forms accompanying a notice of the right to opt out. The regulations also provide examples of means not considered reasonable; for example, an institution could not require a consumer to compose and send a letter to an institution setting forth the consumer's decision to opt out.[40]

Besides issuing the regulations that I have been discussing, the Federal Reserve Board and other agencies have many additional privacy-related responsibilities: implementing those regulations, issuing regulations under the FCRA, setting standards for the protection of consumer data, combating pretext calling, and so on.[41] Our fulfillment of these responsibilities will benefit from your questions and comments. We look forward to receiving them.

---

[38] 12 C.F.R. § 216.6.

[39] *Id.* at § 216.7.

[40] *Id.*

[41] *See* Title V of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801.