

**Uneasy Access: Privacy Problems in the Financial Services Modernization Act**  
Grayson Barber  
April 11, 2000

**Overview**

The Financial Services Modernization Act, 12 U.S.C. 93a, 15 U.S.C. §6801 et seq., informally known as “Gramm-Leach-Bliley” after its sponsors, permits financial institutions like banks, brokerages and insurance companies, to merge with each other and to share information about their customers. The statute has generated concern among privacy advocates because it permits financial institutions to share “nonpublic personal information” freely with their affiliates, and to sell private data about their customers with only the barest constraints.

Leading the parade of horrors is the prospect of a bank making lending decisions based on the health data it gets from its affiliated insurance company, withholding mortgage loans from cancer patients, for example.<sup>1</sup> Another prospect is the insurance company that declines to sell insurance unless its prospective customers consent to having all their credit card transactions reviewed. A third is that individual citizens will find themselves in the crosshairs, as intimate details about them become widely known.

The statute defines “nonpublic personal information” to mean “personally identifiable financial information,” a term that is *not* defined. The proposed rules indicate that it would include any data obtained by a financial institution “in connection with providing financial products and services.” This means that if a consumer provides medical information in order to purchase life insurance, the health records become “financial information” because they are used to purchase a financial product. Account

---

<sup>1</sup> See the discussion of state privacy protections, infra.

balances and credit card transactions would also be considered “personally identifiable financial information.” See proposed rule at §40.3(n).<sup>2</sup>

The Financial Services Modernization Act permits companies to develop and share rich sources of information about consumers, the easier to generate revenues and fend off undesirables. The new statute provides the advantages not only of one-stop shopping and improved fraud detection, it also permits financial institutions to track their customers’ personal interests and preferences - creating a mother lode of valuable private information.

### **Individuals Lose Bargaining Power**

With scant opportunity to control the dissemination of their personal information, individuals lose the opportunity to make meaningful choices. The market would adequately inspire financial institutions to protect privacy only if consumers had complete information about what the companies are doing with their private information. But consumers do not have this knowledge. They have no way of knowing - or learning - how their information is actually used. Moreover, even the financial institutions can only imagine how the information will be used in the future.

To illustrate: If my buying habits are profiled, my negotiating position becomes much weaker. If sellers know that I have bought the last 15 virtual reality simulators with an underwater theme, they may decide not to offer me a discount on the next one; if they practice perfect price discrimination, they may try to charge me extra. If I can maintain my anonymity, I may be in a better bargaining position. My prospects are not auspicious.<sup>3</sup>

---

<sup>2</sup> The proposed rules, which would amend chapter I of title 12 of the Code of Federal Regulations, can be found at [www.occ.ustreas.gov/ftp/regs/npr0203.pdf](http://www.occ.ustreas.gov/ftp/regs/npr0203.pdf).

<sup>3</sup> See A. Michael Froomkin, *Anonymity and its Enmities*, 1995 J. Online L. art 4, par. 43, [www.law.cornell.edu/jol/froomkin.htm](http://www.law.cornell.edu/jol/froomkin.htm) (visited 9/11/96).

Traditional methods of customer profiling lose none of their appeal under the Financial Services Modernization Act. The privacy policies that are published once a year can be completely obscured by a smokescreen of advertising, and customers can be turned away if they refuse to “consent” to subsequent disclosures.

This cripples the power of mere individuals to negotiate with companies that engage in financial activities. It’s no use to suggest that consumers will take their business elsewhere; privacy is but one of many issues to be considered. Motorists didn’t flock to cars with seatbelts, despite ample evidence that they saved lives. Sometimes legislation is necessary.

The five essential components of privacy protection are notice, choice, access, security and enforcement.<sup>4</sup> Gramm-Leach-Bliley falls short in every category. For disclosures among “affiliates” there will be no notice. Consumers will not have meaningful choices because they cannot know how their private information is being used. Consumers cannot get an accounting of disclosures about them, and they have only limited power to prohibit unrelated uses of information about them. The enforcement mechanisms available are self-regulation and government sanctions; individuals have no redress under the statute.

### **Privacy Loopholes In The Financial Services Modernization Act**

Financial institutions are free not only to share private information with their affiliates, they are also free to sell valuable private information to other companies, so long as they publish their privacy policies and give their customers a chance to opt-out. Here examples of loopholes in the law that permit maximum exploitation of private information:

---

<sup>4</sup> See “Elements of Effective Self-Regulation for Protection of Privacy (Discussion Draft)” available at [www.ntia.doc.gov/reports/privacydraft/198dftprin.htm](http://www.ntia.doc.gov/reports/privacydraft/198dftprin.htm).

1. “Public” information can be defined to include anything that can be found somewhere in the public domain. For example, if your name and address can be found in real estate records or security interest filings, your bank or insurance company can disclose them without notice. Questions remain as to whether information is “public” if it can be found in the phone book, on the Internet, in court documents, bankruptcy filings, or motor vehicle records. See proposed rule at §40.3(n).
2. “Nonpublic” information can be disclosed without affirmative consent. Consumers will have the burden to opt out if they don’t want their personal information disclosed. §40.4.
3. Health records are included among the records that can be disclosed. Financial conglomerates will have personal medical information on their customers, through their insurance subsidiaries. The statute contains no prohibitions on disclosure of health data. §40.3(j)(k).
4. Private information can be disclosed to an unrelated financial institution without notice, and with no chance to opt out, so long as the financial institutions enter into a “joint agreement” to market products or services. Thus, even if the unrelated financial institution has no business relationship with the consumer, it can still get information without that consumer’s consent. §40.9.
5. Financial institutions can decline to serve customers who withhold consent to further dissemination. For example, a mortgage lender can decline to serve customers unless they “consent” to receive calls from the affiliate selling homeowners insurance.
6. The statute creates no private right of action for consumers who believe their privacy rights have been violated.
7. Financial institutions are free to obfuscate in their annual privacy policies, using generic language to describe the kinds of personal information they exchange with their affiliates. For example, “application information” means assets and income; “identification information” means name and social security number; “transaction information” includes purchases and account activity; and “consumer reports” include credit histories. §40.6(a)(3).
8. Financial institutions are not required to make any kind of accounting of the disclosures they make about consumers.
9. Former customers get no notice and no chance to opt out before their information is shared with an affiliate. §40.6(a)(4).

10. Your mortgage lender may sell your account to a different financial institution without providing notice of the second bank's privacy policy.
11. It is not clear whether financial institutions would be required to honor letters from consumers asking to opt out. The proposed rules permit "partial opt out" provisions, suggesting that comprehensive opt out requests may not be honored. §40.8.
12. Financial institutions are not required to develop policies and procedures to ensure that third parties will comply with limits on redisclosure. If the third party makes a further disclosure to another under a separate "joint marketing agreement," the consumer may not get notice or a chance to opt out. §40.9.
13. It is not clear whether the statute applies to foreign financial institutions that solicit business in the United States but do not have offices in the United States.
14. It is not clear how the statute applies to joint accounts: What if one account holder opts out but the other doesn't? What if a trustee manages an account for multiple beneficiaries? §40.7(a)(1).
15. Providing notice and a chance to opt out will not address the fundamental principles of
  - (a) using data only for its intended purpose (purpose limitations)
  - (b) collecting only the necessary data (data minimization)
  - (c) limiting the amount of time the data can be used (duration of storage).

## **Market Failure**

Gramm-Leach-Bliley repealed the New Deal banking laws that were enacted on the theory that a separation between bankers and brokers would reduce potential conflicts of interest that were thought to have contributed to the speculative stock frenzy before the Great Depression. The Banking Act of 1933 broke up the powerful House of Morgan, divided Wall Street between investment banks and commercial banks, and restricted what banks could do in the insurance business. Granting that the world has changed dramatically since the New Deal, the fact remains that there is a place for government regulation when economic markets fail to serve most citizens.

There is no reason to believe that the current marketplace will protect individual privacy because it is valuable to consumers; to the contrary, the economics are all wrong

today for transparency in the private sector.<sup>5</sup> Corporations make big profits from the secret collection and sale of personal information, with little to no accountability. The risk of harm to corporate financial interests from the abuse of personal information has been extremely small, and the technology industry has only tentatively responded to privacy concerns, even in the face of heavy criticism when violations are uncovered.<sup>6</sup>

Abuses and public resentment have inspired some companies to drop the mantra that self-regulation is the best solution.<sup>7</sup> A few of the more scandalous failures in self-regulation include:

- According to a health care survey, 19 of the 21 top health web sites posted privacy policies but failed to live up to their promises that they would not share information with third parties. New York Times February 2, 2000.
- Chase Bank's settlement in January 2000, after accusations of violating its own privacy policy. The bank failed to meet its promise to its customers when it transferred to a marketing company the personal records of 18 million credit card and mortgage holders. The Attorney General claimed the bank's conduct amounted to deceptive business practices under state law. New York Times January 26, 2000.
- USBank settled in 1999 after it was sued for selling to a telemarketer its clients' social security numbers, credit card numbers, checking account information, details of credit card transactions, account balances.
- Intel admitted in 1999 that it incorporated an imbedded identifier in each of its Pentium III chips.

---

<sup>5</sup> See, e.g., "The High Cost of Net Privacy," an op-ed by Kevin O'Connor, CEO of DoubleClick, Wall Street Journal, March 7, 2000.

<sup>6</sup> See Joel Reidenberg, Restoring Americans' Privacy in Electronic Commerce, Berkeley Tech. L.J. 1999, [www.law.berkeley.edu/btlj/articles/14\\_2/Reidenberg/html/note.html](http://www.law.berkeley.edu/btlj/articles/14_2/Reidenberg/html/note.html) (visited April 5, 2000).

<sup>7</sup> See "E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise," Wall Street Journal, January 26, 2000, page A24.

Commercial efforts to self-regulate are vapor thin. The Better Business Bureau, for example, conceived BBBOnline as an enforcement mechanism for privacy disputes, but it has licensed only a trivial number of companies that operate websites in the United States. As of April 6, 2000, it has 4,500 participants, and has fielded only two dozen complaints. Half of these complaints have been deemed “ineligible.”<sup>8</sup> “Seal” programs like BBBOnline offer no damage remedy to individuals if companies fail to fulfill their privacy promises.

This self-regulatory pretense has been an embarrassment for the United States abroad. The European Union has rejected a purely market-based approach to individual privacy, adopting legislation that guarantees a broad set of privacy rights and “information self-determination.”<sup>9</sup> The discrepancy between the European approach and that of the United States is a major obstacle for international data exports. The United States cannot participate in meetings of data protection commissioners around the world, since it doesn’t have one, and the EU has so far rejected all the “safe harbor” proposals advanced by the Department of Commerce.<sup>10</sup>

The European experience shows that legislation guarantees neither consensus nor compliance, but it does give people a chance to develop an argument that their individual rights may occasionally trump business interests.<sup>11</sup> The answer must lie in a combination

---

<sup>8</sup> See [www.bbbonline.com](http://www.bbbonline.com) (visited April 6, 2000).

<sup>9</sup> Information and news on the European Data Directive can be found at [http://europa.eu.int/comm/internal\\_market/en/media/dataprot/index.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm).

<sup>10</sup> The International Trade Administration of the U.S. Department of Commerce released its most recent proposal on March 17, 2000. See [www.ita.doc.gov/td/ecom/menu1.html](http://www.ita.doc.gov/td/ecom/menu1.html).

<sup>11</sup> See Organization for Economic Co-Operation and Development, Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. C58 (final), reprinted in 20 I.L.M. 422 (1981), available at [www.oecd.org](http://www.oecd.org); Ronald Dworkin, Rights as Trumps, Theories of Rights (Jeremy Waldron, ed., New York: Oxford Univ. Press 1984).

of law, technical standards and activism. The United States government should not abdicate its responsibilities to individuals in a market that favors the promiscuous sale of personal information. Privacy is essential for participatory government; totalitarian governments prefer the panopticon.

The current patchwork of federal privacy protection statutes is uneven and incoherent. Substance abusers and children enjoy much greater protections than other adults, save for the confidentiality of video rentals.<sup>12</sup> The Children's Online Privacy Protection Act, 15 U.S.C. §6501 et seq., imposes the following requirements on operators of websites directed to children under 13 or who knowingly collect personal information from children under 13 on the Internet:

1. Post notices of how they collect and use personal information from children under age 13.;
2. Obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions);
3. Upon request, provide a parent with the ability to review the personal information collected from his or her child;
4. Provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child;
5. Limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and
6. Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

64 Fed. Reg. 22750 (4/27/99) (to be codified at 16 C.F.R. pt. 312). United States citizens lose most of their privacy rights when they reach 13 years of age.

---

<sup>12</sup> See, e.g., 42 U.S.C. §§290dd-1, dd-2, ee-3 (substance abuse); 18 U.S.C. §2710-2711 (video rentals).

COPPA shows that it is perfectly possible to enact statutes that are consistent with the notion of self-regulation. COPPA includes a safe harbor provision, under which industry groups and others may seek FTC approval for self-regulatory guidelines. Web site operators who participate in such approved programs may be subject to the review and disciplinary procedures provided in those guidelines in lieu of formal FTC investigation and law enforcement. The safe harbor is intended to serve as an incentive for industry self-regulation and as a means of ensuring that COPPA protections are implemented in a manner sensitive to industry-specific concerns and developments in technology. The COPPA rules go into effect April 21, 2000.

### **State Privacy Protections Are Not Preempted**

The Financial Services Modernization Act specifically provides that states may enact stronger privacy protections that will not be preempted by the federal statute. §§ 507, 524. New Jersey should enact legislation that would: (a) prohibit financial institutions from denying financial products or services to consumers who opt out; (b) give consumers the right to examine personal information that has been made available to third parties; (c) give consumers the opportunity to dispute the accuracy of nonpublic personal information; (d) give consumers the right to prohibit subsequent disclosures by third parties; and (e) create a private right of action for privacy violations.

Fortunately, New Jersey provides a statutory scheme for protecting the privacy of individual health records.<sup>13</sup> Generally, an insurance company may not disclose medical information about a person without that person's written authorization. N.J.S.A. 17:23A-13. However, there are numerous circumstances under which an insurance entity can disclose without authorization, and consumers' bargaining power with respect to giving consent is not particularly strong when they are applying for coverage. New Jersey does

---

<sup>13</sup> See [www.healthprivacy.org/resources/statereports/newjersey.htm](http://www.healthprivacy.org/resources/statereports/newjersey.htm).

create a private right of action, with a fee-shifting provision, for statutory violations.

N.J.S.A. 17:23-A-20.

### **Incentives for Privacy Protection**

There are good business reasons for protecting privacy. Health care researchers have found, for example, that privacy violations imperil their industry. One out of every six patients engages in some kind of privacy-protective behavior, to shield themselves from the misuse of their health information. These behaviors include lying to doctors, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out-of-pocket for care that is covered by insurance, and, in the worst cases, avoiding care altogether. This skews health data, distorting epidemiological and outcome studies, to everyone's detriment.<sup>14</sup> The current census uproar should similarly provide an incentive for protecting privacy.

It is not too lofty and ethereal to say that surveillance has a chilling effect on everyone. Without privacy for financial records, we may find ourselves shackled by a kind of "consumer orthodoxy." Innovation in the marketplace requires trial and error, unconventional views, and first attempts that miss the mark. If an early failure puts a black spot on someone's record, which then gets broadcast to a financial institution's affiliates and third parties, the repercussions may extend beyond the influence of that particular individual. Risk-takers will have fewer opportunities, and pressures to conform will hinder innovation.

The criminal penalties provided by the Financial Services Modernization Act, §§523-524, cannot substitute for the positive goal of supporting innovation, participation, autonomy and self determination.

---

<sup>14</sup> See "Confidentiality of Patient Records," testimony by Janlori Goldman, Director, Health Privacy Project, before the House of Representatives Subcommittee on Health of the Committee on Ways and Means, February 17, 2000, quoting a January 1999 survey by the California Health Care Foundation. Available at [www.healthprivacy.org/resources](http://www.healthprivacy.org/resources) (visited April 10, 2000).

## **Conclusion**

Financial institutions should not be permitted to create their own panopticon. The evils of excessive surveillance have emerged from century to century whenever excessive power is sought by the few at the expense of the many. Adamson v. California, 332 U.S. 46, 89 (Black, J. dissenting). Privacy rights should not be viewed as restrictions on commerce; to the contrary, they facilitate innovation. Government should use legislation and other incentives to stanch the erosion of individual privacy.

The final rules for implementing the Financial Services Modernization Act are due May 12, 2000, and will take effect November 12, 2000.