UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 4 | Issue 1 Article 9

2000

Tentative Steps toward Financial Privacy

David W. Roderer

TENTATIVE STEPS TOWARD FINANCIAL PRIVACY*

DAVID W. RODERER†

I. INTRODUCTION

Until last November, no federal law purported to ensure the privacy of personal financial information routinely entrusted by individuals to their bankers and other financial services providers. In most part, the concept of privacy pertaining to personal financial information has remained legally undeveloped, and seemingly beyond public consciousness or concern. In the waning hours at the last Congressional session, however, that changed. Spurred by the alleged misuse of account information by one lender, Congress enacted a hydra-headed regulatory scheme with a mandate to establish minimum federal safeguards for the capture, use, and sharing of financial information about customers by a wide range of businesses. Belatedly engrafted onto the provisions of the financial services modernization law, now formally known as the Gramm-Leach-Bliley Act[1], the new federal policy regime builds upon recent legal developments and bank regulatory pronouncements that sought to encourage certain financial services providers to voluntarily adopt and abide by announced privacy standards.

As recently described by New York Attorney General Eliot Spitzer, the idea of personal privacy is "a fundamental American notion" that the individual has "a right to be left alone."[2] In the new

---

† Of Counsel, Goodwin, Procter & Hoar, LLP, Washington, D.C.; B.A., University of Dayton; JD, George Washington University.

1. *See* Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 1999 U.S.C.C.A.N. (113 Stat).1338.

2. *New Privacy Protection Sought for Information Age: Spitzer Agenda Would Expand Individual's Control Over Personal Data*, Jan. 25, 2000 (visited Feb. 17, 2000) <http://www.oag.state.ny.us/press/2000/jan/jan25a_00.html> (press release of

information age, privacy proponents have only begun to organize in order to strengthen privacy protections and to reclaim that asserted right.

It would be wrong to assume that broad legal protections are in place to ensure the privacy of individuals in their most private matters, including their personal finances. Few statutory safeguards exist. Federal standards are often ambiguous, piecemeal, and reflect inconsistent policy perspectives and purposes. Some federal statutes explicitly protect individuals from narrowly defined categories of unwarranted intrusion; thus, the Right to Financial Privacy Act,[3] for example, inhibits unauthorized access to, and sharing of individuals' financial data by federal agencies. Moreover, the Fair Credit Reporting Act[4] has been interpreted to restrict access to individuals' credit information, as well as to provide some modicum of assurance to individuals as to the accuracy of such information. In contrast, several state courts have discovered more durable rights to privacy in their own state constitutions and laws. The common law also protects some aspects of privacy, such as the individual's right to determine how his or her likeness will be used for commercial purposes. Taken together, these statutes and judicial decisions do not, however, effect broad protections for the privacy of an individual's financial information. The newest federal law and anticipated federal regulations do little more than establish another cumbersome procedural device by which some aware customers may insulate themselves from the more intrusive scrutiny of unwelcome telemarketers and other vendors.

Even prior to the new federal enactment, state and federal regulators had stepped into the breach to promote and instigate various measures designed to expand their reach to perceived systemic abuses concerning individual privacy rights. Most prominently, the Attorney General of Minnesota sued U.S. Bancorp, extracting a consent decree over allegations that the bank improperly disclosed customer account numbers to telemarketers and debited customer accounts for transactions with third-party vendors with-

---

the office of New York State Attorney General).

3. 12 U.S.C. §§ 3401-3422 (1994).

4. 15 U.S.C. § 1681 (1994).

out customer knowledge, much less explicit authorization.[5] It was that quickly settled action, without any admission of wrongdoing by the bank, which provided the most immediate impetus for federal legislation. Other agency initiatives that also contributed to the discussion, such as the Federal Trade Commission's report released in June 1998, criticizing Internet website operators and, in particular, financial institutions.[6] Federal banking regulators also prepared the ground for sowing of financial privacy legislation by calling for the adoption of voluntary industry privacy standards.[7]

Those initiatives, and particularly, the U.S. Bancorp settlement, energized privacy advocates to seek federal statutory protections. Further stimulated by perceptions of a growing threat to personal privacy from the evermore pervasive technology used by increasingly larger financial institutions in the delivery of products and services, the proponents of federal privacy protections seized upon the financial modernization bill then pending in the House of Representatives to advance their agenda. Bipartisan support quickly coalesced around the push for minimum federal privacy standards. In late October, the essential compromises were made to clear the way for passage by the House of a broad financial package which, at the insistence of the White House, included minimum federal financial privacy standards.

II. MANDATORY FEDERAL SAFEGUARDS AND DISCLOSURES

The new federal law, embodied in Title V of the Gramm-Leach-Bliley Act,[8] is comprised of five elements:

---

5. *See* Hatch v. US Bank National Association ND, Civil Action No. 99-872 (D.Minn. Oct. 4, 1999).

6. *See Privacy Online: A Report To Congress* <http://www.ftc.gov/reports/privacy3/toc.htm> (visited Feb. 15, 2000).

7. *See Acting Comptroller Urges Banks to Act on Privacy Issues,* <http://www.occ.treas. gov/ftp/release/98%2D109.txt> (visited Feb 15, 2000); <http://www.ots.treas.gov/docs/25097.pdf> (visited Feb 15, 2000); <http://www.ots.treas.gov/docs/73078.pdf> (visited Feb 15, 2000).

8. *See* Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, §§ 501-510, 1999 U.S.C.C.A.N. (113 Stat.) 1338, 1436-1443.

- an "affirmative and continuing obligation" is purportedly established for each financial institution ''to respect the privacy of its customers and to protect the security and confidentiality" of customers' non-public personal information;

- a written privacy policy is mandated to be adopted and disclosed by each financial institution that transfers non-public personal information to unaffiliated entities, except as authorized by the new law;

- an "opt out" mechanism is required to be provided to individual customers concerning information transfers to unaffiliated parties, subject to various exceptions;

- the transfer of account numbers and access codes to telemarketers and other unaffiliated third parties is prohibited, except to credit bureaus; and

- a prohibition on pretext calling, or customer "identity theft," to obtain personal financial information through false or fraudulent means.

Viewed broadly, the new federal scheme proclaims— but does not secure— a range of individual rights to privacy in financial matters. It identifies four areas of substantive concern: (i) security and confidentiality of information; (ii) customer knowledge of each financial institution's information-sharing practices; (iii) customer control over the uses to which personal information may be put; and (iv) the security threat posed by ''pretext calling."

Significantly, the new federal law does not empower consumers to act to ensure their own interests in such matters. Rather, the law establishes a procedural device and overlapping regulatory supervisory enforcement mechanisms to identify and correct abusive policies and practices rather than to remedy or resolve individ-

ual rights affected by specific infractions. The structure is thus somewhat illusory, lacking in any recourse for an individual to remedy the infringement of his or her privacy. Moreover, absent a single federal enforcer, the new statutory scheme empowers each of the various so-called "functional regulators," that is, seven federal agencies and some fifty-plus state insurance regulators, to separately adopt rules to ensure the maintenance of systemic safeguards without explicitly authorizing them to pursue or remedy individual violations. In stark contrast to the largely toothless enforcement regime of the regulatory agencies as to first three above-listed safeguards, the new law, however, makes pretext calling a federal crime.[9] Definition and enforcement of individual privacy rights and remedies are left largely to the states.

III. THE EXCEPTIONS

The federal privacy safeguards are honeycombed with exceptions, leaving the new regime, despite its reassuring public appearance, to be significantly less than comprehensive. Most conspicuously, the privacy provisions of the new law do not apply to all consumer information, but only to so-called "non-public personal information." The term appears broadly inclusive: encompassing all personally identifiable financial information that is provided to a financial institution by a customer, or results from any transaction with the customer, or is otherwise obtained by the financial institution. However, the term does not include information covered by one of several statutory exemptions.

Seemingly most enormous is the exemption of all "public information," which at least one legal commentator has already speculated may exclude any information available over the Internet. Moreover, all information "derived from" public information is exempted as well. Those exclusions, in particular, blithely ignore the substantial threat to privacy posed, not by access to specific bits of information, but rather by the compilation and sharing through

9. *See generally* Kristen S. Provenza, Note, *Identity Theft: Prevention and Liability*, 3 N.C. BANKING INST. 319 (1999).

modern technologies of otherwise available data affecting individuals— the development of which is arguably the greater threat to privacy, and is yet unaffected by the new law.

Moreover, the full range of federal privacy safeguards does not apply to information sharing by financial institutions with either affiliates or third-party providers and servicers of the institution. A disclosure of an institution's privacy policies is mandated in order for an institution to share information with third parties, including aligned marketers, but prior notice is not required. In addition, so long as a financial institution discloses that it will share customer information with its third-party service providers, its customers are given no way under the new law to opt out of or prohibit such sharing. The statutory requirement that an institution enter into confidentiality agreements with service providers with whom it shares customer information is likely of little or no benefit to bank customers not party to such agreements.

A long list of exemptions riddles the protective coverage of the new federal privacy regime. Pursuant to these exemptions, a financial institution can share information with many other entities apparently without providing notice or a right to opt out, and presumably can do so without threat of legal retaliation by subject individuals under either common or contract law.

Specific categories of information-sharing permitted by the exemptions include:

- disclosure of information "necessary" in connection with transactions, products or services requested by the consumer; account maintenance or servicing (including in connection with private label credit card or other programs); proposed or actual securitizations and secondary market sales (including sales of servicing rights); or similar transactions;

- provision of information with the consent or at the direction of the consumer;

- provision of information in order to protect the confidentiality or security of the institution's records or to fight actual or potential fraud; for "required institutional risk control" purposes; or to resolve customer disputes or inquiries;

- disclosure of information to persons holding a legal or beneficial interest relating to the consumer, or acting as representatives or fiduciaries of the consumer;

- provision of information to insurance rate advisory organizations, guaranty funds or agencies, persons assessing compliance with industry standards, rating agencies and services, and the institution's attorneys, accountants or auditors;

- provision of information to or by a consumer reporting agency pursuant to the Fair Credit Reporting Act;

- provision of information in connection with the proposed or actual transfer as part of the sale of all or part of a business, if the information concerns solely consumers of such business; and

- disclosure of information in compliance with federal or state law, summons, subpoena, regulatory investigation, etc.

In the breadth and sheer number of specific exemptions taken together, an enormous range of statutorily permissible transfers of information can occur outside the notice and opt out requirements of the new federal scheme.

IV. THE NEXT STEPS: FEDERAL

The enactment of the new law was heralded by many as effecting sweeping protections for consumer privacy. In signing the new law, President Clinton cautioned, however, against assuming it to be the final word on the subject. The financial services industry and its very effective advocates are likely to be disappointed, however, in any hope that the federal law will establish enduring, uniform standards under which business can be conducted without further disruptive legal and regulatory encumbrances.

Federal regulations are mandated to be adopted in final form by each of the agencies within six months after enactment of the law, that is, by no later than May 12, 2000, to be effective six months thereafter. These regulations may narrow some of the more gaping exemptions and clarify others, but the regulators themselves are also empowered to open even more "as deemed consistent with the purposes" of the act. Significantly, the regulators are not explicitly permitted to create further exemptions from the requirements that financial institutions disclose their privacy policies to customers, however, they are broadly empowered to create new exemptions from the "opt out" rule. The enthusiasm of the regulators to clarify the scope and ambiguities of the new law, or to tighten uncertain standards will await agency rulemakings that are likely to draw far more than usual public attention to agency proceedings.

Federal lawmakers may not yet be done. Further pressure has already surfaced from the Congressional privacy proponents whose pursuit of a more aggressive privacy agenda was thwarted in the first round of federal legislation. Representative Markey (D-MA) and Senator Shelby (R-AL), on November 10, 1999, even before the President signed the new law, introduced essentially identical legislation, H.R. 3320 and S. 1903 respectively, to amend and expand the new federal law. The proposed amendments would, among other things, prohibit financial institutions from sharing customer information with either affiliates or non-affiliates absent explicit customer authorization-- that is, "opt in" to such sharing. Moreover, financial institutions would be required to provide an individual wide freedom to obtain access to information

pertaining to himself or herself, and to demand correction of errors in such information. Although no such federal legislative action is imminent, the likelihood is substantial that the privacy issue will catch fire in next year's politically charged campaign environment— at both the federal or state levels.

V. THE STATES NEED NOT WAIT

State lawmakers are also likely to feel mounting pressures to take and may initiate strong privacy stands. Most significantly, the law explicitly leaves open the authority of the states— and by extension the courts under state law— to further buttress and fill in the cracks of the federal privacy structure. More particularly, the privacy provisions explicitly provide that state statutes, regulations, orders and interpretations that afford "greater protection" than the federal law are not preempted. Some state legislators may well be tempted, therefore, to create additional protections to shield their citizens from the intrusion of commercial vendors into financial institutions' data banks.

More immediately, and without need to await the delayed effectiveness of the federal scheme, state officials, such as seen in Minnesota and New York,[10] may be similarly tempted to read broad privacy rights into their own state schemes, or to breathe new life into old privacy-related legal doctrines. The likely result is legal balkanization, with differing state privacy standards and legal regimes disrupting would-be nationwide financial institutions' cherished dreams of unencumbered national markets.

The US Bank was a harbinger of the restrictive legislative proposals then under consideration by the House of Representatives. In early October of last year, U.S. Bancorp and the Minnesota Attorney General Mike Hatch settled a lawsuit brought by the State of Minnesota against the bank holding company regarding telemarketing arrangements with third parties. The action by the Attorney

---

10. *New Privacy Protection Sought for Information Age: Spitzer Agenda Would Expand Individual's Control Over Personal Data*, Jan. 25, 2000 (visited Feb. 17, 2000) <http://www.oag.state.ny.us/press/2000/jan/jan25a_00.html> (discussing *In the Matter of Chase Manhattan Bank US* and *In the Matter of InfoBeat LLC*).

General alleged various violations of federal and state laws affecting the privacy rights of bank customers. Without admitting the allegations, the bank holding company essentially agreed, in light of recent voluntary revisions to its privacy policies, to various additional terms as part of the settlement, including:

- contribution of an additional amount of approximately $3 million equal to the total revenue the bank has ever received in the past from cooperative marketing programs as follows:
- $1.5 million to chapters of Habitat for Humanity in Minnesota;
- $500,000 to the State of Minnesota;
- $1,034,000 to charities or public bodies in other states in which the bank does business;
- to inform customers of the bank's privacy policies and to provide notice of customers' rights to "opt out" of the sharing of information with bank affiliates for the purposes of marketing financial products and services; and
- to make refunds to any Minnesota customers who purchased the services and are dissatisfied (and did not use the service).

Notably, the voluntary policies established by the bank would allow customers to "opt out" of information-sharing even with affiliates— thus, restricting information-sharing even more than provided by the later enacted federal statute.

VI. CONCLUSION: AND THE BEGINNING

The fashioning of a balanced legal scheme that properly weighs serious privacy concerns against legitimate business activities without creating an overburdensome regulatory regime remains yet to be done. Whether the privacy reform agenda recently put forward by the New York Attorney General or some other formulation by federal and state policymakers prevails will await to be seen— in time.

Meanwhile, financial institutions and many businesses alike must grope their own ways across the legally and politically pockmarked landscape. Each institution entrusted with the personal financial information of its customers must now— and before the delayed effectiveness of the new federal scheme— undertake to review and revise its policies and practices in the sensitive area of customer information usage and, particularly, transfers to others. A privacy policy can no longer be simply drafted and announced, as has been commonplace in the past, by the marketing department. Programmers and those who put together the business systems of financial institutions need be directly involved, to ensure the veracity and conformance of actual business practices to announced policies. The issue is no longer simply a public relations concern, but rather one of compliance and potential liability. The best and most wise course is to proceed cautiously and to participate in the public debate likely to fashion and reshape the laws and regulatory policies affecting this most fundamental American notion—privacy.