E-mail: peter@peterswire.net
Telephone: (240) 994-4142
Web: www.peterswire.net
March 29, 2004

Comment on Interagency Proposal to Consider Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act

To the Agencies:

Thank you for the opportunity to comment on how short notices might be incorporated into the overall privacy notice regime under the Gramm-Leach-Bliley Act. My comments here are in response to the Advance Notice of Proposed Rulemaking in the Federal Register of December 30, 2003. 68 Fed. Reg. 75164.

My comments focus on the following topics: keep the short notices short; have comparability and yes/no choices; focus attention on the key issues; give good linkage to the long notices; link to the opt-out as well; and provide safe harbor language where necessary.

Background of the author. I am now Professor of Law and a John Glenn Scholar in Public Policy Research at the Moritz College of Law of the Ohio State University. I offer these comments entirely in my personal and academic capacity, and have not been paid by any party to work on the short notices rulemaking. I have also met with other privacy experts in a process convened by the Center for Democracy and Technology, and believe that the principles filed by CDT today should be carefully considered by the agencies as they proceed with the rulemaking.

My comments here are based in part on my previous writings on the issues of privacy notices. Today I am submitting for the record two documents that are relevant to these issues. The first is a law review article entitled "The Surprising Virtues of the New Financial Privacy Law," 86 Minn. L. Rev. 1263 (2002). Part IV of that article discusses financial privacy notices. The second is a comment letter on short notices that I wrote in 2002 in connection with the HIPAA medical privacy rulemaking. Both of these documents, as well as my curriculum vita, are also available at my website at www.peterswire.net.

The comments here are also based on my experience from 1999 until early 2001 as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that position, I was part of the Administration team that worked with Congress during consideration of what became Title V of the Gramm-Leach-Bliley Act. Once the law was enacted, I participated in many of the inter-agency meetings during development of the rulemaking under Title V.

Substantive comments. At the request of the agencies, I met with an inter-agency group on short notices on February 5, 2004. The comments here summarize the main

points that I gave during that session. I have not changed my views since that session, and so hope that my comments at that time will be considered part of the record.

Here are my principle points to consider:

1. *Keep the short notices short.* As discussed in my law review article, there is a difficult trade-off between long notices, which are detailed and facilitate accountability, and short notices, which are more understandably by the consumer. I support a layered notice approach in which the long notice becomes the key document for accountability purposes. In that setting, the short notice truly should be short and expressed in plain language. As a rough guideline, a short notice should fit on one ordinary sheet of 8.5" x 11" piece of paper in ordinary 12-point font. That length can then serve as a budget for what should be included.

2. *Have comparability and yes/no choices.* A chief virtue of a short notice is to facilitate informed choice by consumers. As with nutrition labels, a standard format is enormously helpful to reduce the time and trouble it takes for a consumer to understand and act on the information. In order to foster comparability, it is very helpful to consumers to have yes/no choices or perhaps other clear ways to communicate information.

3. *Focus attention on the key issues.* For Gramm-Leach-Bliley purposes, the biggest issues by far are whether information is shared with third parties and whether it is shared with affiliates. Anyone who has lived through the legislative and regulatory debates knows that these issues have been top-of-mind for consumers, politicians, and industry actors. The short notices should thus have a clear format for announcing how the company handles sharing with third parties and affiliates.

4. *Give good linkage to the long notices.* For short notices to work, there must be very clear linkage to accessible long notices. Quite possibly, a condition for using short notices on a stand-alone basis should be a web address that immediately shows the customer the long notice. Quite possibly, there should be an 800 telephone number as well.

This approach would be consistent with the claimed virtues of short notices. The short notice would provide the key information to consumers. Providing only the short notice in certain settings could save costs for industry. In return, there must be continued ready access to the long notice.

5. *Link to opt-out as well.* For companies that share information in ways that are subject to opt-out, the short notice should provide a ready mechanism for that opt-out. One good practice is that any mechanism that is considered secure enough to permit financial transactions should also be considered secure enough to implement choice on opt-out. If a financial institution has a web site to conduct transactions, for instance, then that web site should also have a mechanism for exercising opt-out.

6. *Provide safe harbor language where necessary.* One risk for financial institutions is that short notices will be so short that some court or other decisionmaker will find the summary language to be misleading. For instance, the exceptions under Section 502(e) of Title V themselves take roughly a full page to print. How can financial institutions safely summarize these exceptions within a short notice?

I believe the agencies should consider language that can act as a safe harbor in such circumstances. For instance, the agencies might draft sample language that says: "Your personal information may also be shared in ways that comply with the law, such as to prevent fraud or where required by regulators."

In considering what topics deserve this safe harbor treatment, the agencies can examine existing Gramm-Leach-Bliley notices to see where there is small variation but a large amount of standard language. These areas of "boilerplate" are good candidates for standardized, short treatment in the short notices.

My thanks once again to the agencies for their consideration of these important issues.

Sincerely,

Peter P. Swire

The Surprising Virtues of the New Financial Privacy Law

Peter P. Swire†

The financial privacy law passed by Congress in 1999 has been the target of scathing criticism. On one side, banks and other financial institutions have complained about the high costs of the billions of notices sent to consumers, apparently to widespread consumer indifference.[1] On the other side, privacy advocates have condemned the law as woefully weak, and some have argued that its so-called privacy provisions actually resulted in weakening privacy protection.[2]

This paper disagrees with the criticisms. The new financial privacy law, known more formally as Title V of the Gramm-Leach-Bliley Act of 1999, works surprisingly well as privacy legislation. It does so in ways that address legitimate industry concerns about excessive cost and barriers to needed information. In addition, the ability of states to draft additional legislation in the area means that an effective mechanism exists to correct the key weaknesses of the law over time.

The financial privacy provisions were enacted in 1999 as part of sweeping legislation to update the structure of the banking, insurance, se-

† Professor of Law, the Moritz College of Law of the Ohio State University. From March, 1999 to January, 2001 I served as Chief Counselor for Privacy in the U.S. Office of Management and Budget. My thanks to helpful comments from participants in the Minnesota Law Review Symposium on Privacy. My thanks also for comments by Rick Fischer, Lauren Steinfeld, and Art Wilmarth, and to Larry Glasser for research assistance.

1. For instance, one estimate was that the financial privacy rules would require 2.5 billion consumer disclosure statements annually, with a compliance cost of compliance (which I believe is high) of $1.25 billion. Michele Heller, *Banks Want More Time on Reform's Privacy Rules*, AM. BANKER, Apr. 12, 2000, at 3.

2. Frank Torres, legislative counsel for Consumers Union and an active participant in the legislative debates, bluntly described the new privacy law: "The much ballyhooed privacy provision of the Gramm-Leach-Bliley Act does not protect consumers' privacy." Don Oldenberg, *To-Do Over Privacy Legislation*, WASH. POST, April 5, 2000, at C4. Torres also lamented: "[GLB] has a few meager privacy provisions, but it contains so many exceptions that it gives consumers no real privacy protection at all." Steven Brostoff, *Privacy Legislation Draws Industry Fire*, NAT'L UNDERWRITER LIFE & HEALTH-FIN. SERVICES EDITION, May 8, 2000, at 46.

curities, and other financial services industries. Since the 1930's, the Glass-Steagall Act had largely separated these industries. Gramm-Leach-Bliley, as signed by President Clinton in November, 1999, culminated many years of regulatory and legislative debate about how to modernize the financial services sector. From now on, a single financial holding company can own banks, investment banks, insurance companies, and a wide array of other institutions.

Part I of this article introduces the main provisions of Title V, showing the better match with basic privacy principles than many have realized. Part II explores the history of how the financial privacy provisions became law, placing the enactment into the context of a historical peak of privacy policy activity in the late 1990's. Perhaps this history will be of particular interest because of my unusual dual perspective, both as an academic who has written extensively about financial privacy,[3] and also as the Clinton Administration's Chief Counselor for Privacy during the period.

Part III looks at the most hotly-contested issue in the privacy debate, the rules for sharing personal information with affiliated entities and third parties. GLB establishes a basic rule that information can flow freely within a financial institution and to its affiliates. Customer choice—an opt-out ability to prevent sharing—applies for transfers to non-affiliated companies. This article argues that an exception to that principle of customer choice, the so-called "joint marketing exception," should be repealed. It then explores the knotty issue of how to handle data sharing in today's vast financial conglomerates, suggesting a number of possible modifications to GLB's Title V.

Part IV of the article looks at the much-maligned notices that financial institutions have sent out in compliance with GLB. The critics have accurately complained about the legalistic and detailed language in the current notices. The critics have largely overlooked, however, important benefits from these notices. Perhaps most significantly, publication of the notices and the new legal obligation to comply with them has forced financial institutions to engage in considerable self-scrutiny as to their data handling practices. The current notices, even in their imperfect form, have reduced the risk of egregious privacy practices. Improved notices, as described in this article, would enhance accountability while also communicating far more clearly with ordinary customers.

3. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 102-21 (1998); Peter Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461 (1999); Peter P. Swire*, The Uses and Limits of Financial Cryptography: A Law Professor's Perspective* (1997), *available at www.osu.edu/units/law/swire.htm.*

In short, this article shows the surprising merits of the GLB privacy provisions. Considerably more was accomplished in the Act than observers would have predicted in the spring of 1999 or than critics have recognized to date. Important flaws do exist, but specific and achievable changes in the statute and implementing regulations can go far toward reducing the magnitude of those flaws.

I. THE PRIVACY PROVISIONS IN GRAMM-LEACH-BLILEY

Perhaps the clearest way to understand what was and was not enacted in the Gramm-Leach-Bliley Act (GLB) on privacy is to compare the law as enacted with standard definitions of fair information practices. Codes of fair information practices are an organizing theme of privacy protection. They were first set forth in comprehensive form in a United States Department of Health, Education, and Welfare study in 1973.[4] The precise list of fair information practices has varied somewhat over time, but the use of such a list has been a standard feature of privacy regimes. For instance, they are incorporated into United States law in the Privacy Act of 1974, which applies to United States federal agencies.[5] They are listed as the "core principles" of the most important consensus document internationally, the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, issued in 1980. They are central to the European Union Directive on Data Protection, issued in final form in 1995 and binding on the fifteen member states of the European Union.[6] In the 1990s, as the rise of the Internet helped make privacy a more prominent public policy issue in the United States, the fair information practices were used as organizing principles for the debate. Likely the best known version was that of the Federal Trade Commission, which contained five principles: notice/awareness; choice/consent; access/participation; integrity/security; and enforcement/redress.[7]

4. U.S. DEPT. HEALTH, EDUC. & WELFARE, Records, Computers and the Rights of Citizens (1973).

5. Privacy Act of 1974, 5 U.S.C. § 552a (2000).

6. Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L 281) 31 (Oct. 24, 1995), available at http://europea.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html [hereinafter European Union Data Protection Directive]. *See generally* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

7. Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf [hereinafter 1998 FTC Report]. The list of the FTC, which is an independent agency, was generally consistent with formulations by the Clinton Administration. *See Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Infor-*

A. NOTICE

The FTC calls notice "[t]he most fundamental principle . . . ."[8] Without notice, the consumer "cannot make an informed decision as to whether and to what extent to disclose personal information."[9] The notice principle is addressed in detail in GLB, although debates continue about how best to provide notice.

The GLB notice requirements apply to "nonpublic personal information" (often described in this article as "personal information" or "personal data").[10] This personal information may not be disclosed to another corporation unless the consumer is provided a notice.[11] At the time of establishing a customer relationship, and at least annually after that, a financial institution "shall provide a clear and conspicuous disclosure of the institution's privacy policies [to the consumer]."[12] The privacy policy must give the policies for sharing data with both affiliates and nonaffiliated third parties, including the categories of information that may be disclosed.[13] The notice requirement of GLB is what led to the large number of individual privacy policies that customers of financial institutions now receive on an annual basis.

---

mation Infrastructure: Principles for Providing and Using Personal Information (June 6, 1995), *available at* http://iitf.doc.gov/ipc/ipc/ipc-pubx/niiprivprin_final.html; U.S. Department of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (Oct.1995), *available at* http://www.ntia.doc.gov/ntiahome/privwhitepaper .html.

8. 1998 FTC Report, *supra* note 7, at 7.

9. *Id*. The 1980 OECD Guidelines state, in the Collection Limitation Principle: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, OECD Dic, C(80) 58, *reprinted in* 20 I.L.M. 422, *available at* http://www1.oecd.org/dsti/sti/ it.secur/prod/PRIV-EN.HTM (latest update Jan. 5 1999) [hereinafter OECD Guidelines].

10. The term "nonpublic personal information" is defined in GLB Section 6809(4) to mean "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; (iii) or otherwise obtained by the financial institution." Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A) (2000) [hereinafter GLB]. The term "does not include publicly available information." *Id*. § 6809(4)(B). It does include "any list, description, or other grouping of consumers . . . that is derived using any nonpublic personal information other than publicly available information . . . ." *Id*. §6809(4)(C).

11. *Id*. § 6802(a).

12. *Id*. 6803(a).

13. *Id.* § 6803(a)(1).

B. CHOICE/CONSENT.

The choice/consent principle has been a major source of contention, both during passage of GLB and since. In the words of the FTC, "choice relates to secondary uses of information—*i.e.*, uses beyond those necessary to complete the contemplated transaction."[14] Privacy regimes generally limit data uses to those that fulfill the original purposes of the data collection, as well as others that are compatible with those purposes.[15]

In interpreting the choice/consent principle, there have been heated debates about what the default rule should be. Industry has generally favored a default rule of allowing sharing, with customers able to opt out if they choose to limit the data flow. Privacy advocates have generally favored a default rule prohibiting sharing, with data going for secondary uses only with an affirmative opt in by the individual. The default rule seems to matter a great deal in the privacy context, because experience seems to show that the bulk of customers generally stick with whichever default rule applies in a given context.[16]

The other heated debate has been about what sorts of sharing constitute secondary use. In the financial services area, industry has pushed especially hard for the ability to share data with affiliates, that is, with companies controlled by the same financial holding company.[17] Industry has also supported the ability to share data with nonaffiliated third par-

14. 1998 FTC Report, *supra* note 7, at 8. Similarly, under the 1980 OECD Guidelines,

> [t]he purposes for which personal data are collected should be specified not later than at the time of data collection and subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes. . . . Disclosure or use of data should then not be done except *a*) with the consent of the data subject; or *b*) by the authority of law."

OECD Guidelines, *supra* note 9.

15. *See supra* note 14.

16. This is my own view after experience with a wide range of privacy regimes. One example of the difference comes from the Drivers Privacy Protection Act of 1999. 18 U.S.C. § 2721 (2000). The Act restricts a state motor vehicles bureau from sharing individual drivers license information for marketing purposes except with choice or consent. It was enacted as an opt-out regime in 1994. *Id.* As such, opt out rates varied, based on my discussions with officials, from the low single digits to a high in some states of about 20 percent. In 1999, an appropriation rider switched the regime to opt in. Since that time, no state has even asked whether individuals wished to consent to sharing their drivers license information for marketing purposes.

17. "The term 'affiliate' means any company that controls, is controlled by, or is under common control with another company." GLB, *supra* note 10, § 6809(6).

ties.[18] Privacy proponents have maintained that sharing with either affiliates or nonaffiliated third parties constitutes secondary use, and should trigger a choice or consent requirement.

As enacted, GLB adopted the basic rule of requiring an opt-out choice before personal data could be shared with nonaffiliated third parties.[19] Financial institutions must give notice before they share data with affiliates, but customers are not entitled to an opt-out choice for affiliate sharing.[20] This basic rule is loosened in two ways. First, the "joint marketing exception" allows a financial institution to share information with nonaffiliated financial institutions in order to pursue joint marketing.[21] As discussed below, this exception has been controversial, and I believe it should be repealed. Second, the law sets forth a number of statutory exceptions where neither notice nor choice are required. These exceptions have been reasonably well accepted by many of the stakeholders in the privacy debates, and apply, for instance, to an institution's attorneys, accountants, and auditors, to consumer reporting agencies under the Fair Credit Reporting Act, to protect against or prevent fraud, and to comply with authorized law enforcement investigations.[22]

GLB is stricter than the basic rule in one respect. A financial institution cannot disclose, other than to a consumer reporting agency, a credit card or similar account number to any nonaffiliated third party for use in telemarketing, direct mail marketing, or e-mail marketing to a consumer.[23] The opt-out and account number restrictions are backed up by a limit on how third parties can redisclose the information.[24]

18. "The term 'nonaffiliated third party' means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution." GLB, *supra* note 10, § 6809(5).

19. *Id*. § 6802(b)(1).

20. *Id*. § 6802(a).

21. *Id*. § 6802(b)(2). The joint marketing exception is discussed in detail text accompanying notes ___ *infra*.

22. *Id*. § 6802(e). Other exceptions, described in more detail in the statute, include: an exception necessary to carry out a transaction; with the consent of the consumer; to protect the confidentiality or security of the institution's records; to provide information to persons assisting in compliance with industry standards; and in connection with a sale or merger of the business. *Id*.

23. *Id*. § 6802(d).

24. Essentially, a nonaffiliated third party that receives personal information shall not redisclose that information to any other person unless such disclosure would be lawful if made directly to such other person by the original financial institution. *Id*. § 6892(c).

C. ACCESS.

The third core principle is access. Access refers "to an individual's ability both to access data about him or herself—*i.e.*, to view the data in an entity's files—and to contest that data's accuracy and completeness."[25] Individuals in the United States have had a right to access their credit history—an accumulation of sensitive personal financial information—since passage of the Fair Credit Reporting Act in 1970.[26]

GLB itself does not implement any consumer access right. Proposed legislation, including that supported by President Clinton in 2000, would have provided access rights to financial information as a matter of law.[27] In practice, however, consumers often have an ability to access their personal financial information. For important accounts such as checking accounts, credit card records, securities brokerage accounts, and the like, individuals generally receive detailed records as a matter of course, and they can contest the accuracy and completeness of those records as problems arise.

D. SECURITY

As the FTC states: "Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data."[28] Privacy policies offer little protection

25. 1998 FTC Report, *supra* note 7, at 9. The OECD Individual Participation Principle states:

> An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

OECD Guidelines, *supra* note 9.

26. Fair Credit Reporting Act, 15 U.S.C. § 1681g (2000).

28. 1998 FTC Report, *supra* note 7, at 10. Similarly, the OECD Security Safeguards Principle states: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data." OECD Guidelines, *supra* note 9.

The FTC Report combines the security principle with the need to assure data integrity, where "collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to

unless security is in place. Otherwise, the best-intended policies can be quickly undermined by hackers or others who access and disclose the personal information.

GLB addresses security as part of the general obligation of financial institutions to protect privacy. The statute provides: "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[29] In furtherance of that policy, regulators are required to issue standards relating to administrative, technical, and physical safeguards to protect the security and confidentiality of customer records and information. The standards must protect against "anticipated threats or hazards to the security or integrity of such records," and protect as well against unauthorized access to records or information that "could result in substantial harm or inconvenience to any customer."[30]

E. ENFORCEMENT AND REMEDIES.

The FTC says: "It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them."[31] A phalanx of financial regulators have now issued regulations to implement the GLB privacy provisions for institutions in their jurisdiction.[32] In implementing these privacy regulations, the basic

data, and destroying untimely data or converting it to anonymous form." 1998 FTC Report, *supra* note 7, at 10. This definition of data integrity conforms to the principle, accepted in European countries, that "untimely data" should be destroyed or converted to anonymous form. The Data Protection Directive, for instance, states that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed." European Union Data Protection Directive, *supra* note 6, art. 6(e). Notwithstanding the FTC's support for "destroying untimely data," U.S. law has not usually included data destruction as a significant element of privacy principles.

29. GLB, *supra* note 10, § 6801(a).

30. *Id*. § 6801(b).

31. 1998 FTC Report, *supra* note 7, at 10. The OECD Accountability Principle states: "A data controller should be accountable for complying with measures which give effect to the principles stated above." OECD Guidelines, *supra* note 9.

32. The statute required seven agencies, working together with the Treasury Department, to prepare regulations. GLB, *supra* note 10, § 6804(a)(1). First, a set of standards—"The Interagency Guidelines Establishing Standards for Safeguarding Customer Information"—were developed by the GLB agencies and uniformly promulgated. *See, e.g.,* 12 C.F.R. § 30.2, app. B (Comptroller of the Currency); *Id*. § 208.3, app. D-2 (Federal Reserve); *Id*. § 364.101 app. B. (FDIC), *Id*. § 570.1, app. B (Office of Thrift Supervision), *Id*. § 748, app. A (NCUA). Second, the agencies each promulgated a rule that required financial institutions within their jurisdiction to comply with the Guidelines. *See, e.g., Id*. § 208.3 (Federal Reserve); 16 C.F.R. § 313.1 (Federal Trade Commission); 12 C.F.R. § 364.101 (FDIC); *Id*. § 568.5 (Office of Thrift Supervision).

GLB, *supra* note 10, § 509 (3)(B) specifically excluded the Commodity Futures Trading

rule under GLB is that financial regulators can deploy the full powers that they use in other enforcement actions.[33] Bank regulators can use the strict enforcement powers that they gained after the savings and loan abuses of the late 1980s.[34] State insurance authorities enforce for violations by state-regulated insurance companies.[35] The Securities and Exchange Commission, National Credit Union Administration, and Commodities Future Trading Commission can enforce against entities in their jurisdiction. The FTC can use its powers to enforce against unfair or deceptive trade practices against any other financial institution that is not subject to one of the above agencies.

F. SUMMARY ON GLB AND FAIR INFORMATION PRACTICES.

When matched against the standard list of fair information practices, GLB provides a better set of privacy protections than many have realized. GLB creates significant legal protections for the notice, security, and enforcement principles. For access, ordinary industry practice likely meets many consumer needs. The largest debate concerns the choice/consent principle. Privacy advocates are concerned that the opt-out choice is too weak and that too many data flows are permitted to affiliates and joint marketing partners without any choice at all. As discussed below, the Clinton Administration proposed legislation in 2000 to address these problems, and I personally would favor additional legal protections in the choice/consent area.

Other provisions in GLB show that it provides a better foundation for privacy protection than many have realized. First, the definition of "financial institutions," which are covered by the statute, is extremely broad. GLB allows a financial holding company to engage in any activity found by the Federal Reserve Board "to be financial in nature or incidental to such financial activity."[36] Going beyond that broad definition, the Board can authorize an activity that is "*complementary* to a financial ac-

Commission from the Act, but that was reversed by The Commodity Futures Modernization Act of 2000. 7 U.S.C. § 1 278f (2000). The CFTC issued proposed rules for GLB compliance in early 2001. 66 Fed. Reg. 15,550 (March 19, 2001).

33. GLB, *supra* note 10, § 6805.

34. *See* 12 U.S.C. 1818 (2000). The bank regulators with these powers to enforce the privacy rules are the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision.

35. Because of federalism limits against "commandeering" the states in a federal statutory scheme, *see* New York v. United States, 505 U.S. 144 (1992), the statute does not order state insurance authorities to adopt regulations to carry out the privacy protections. Instead, states that decline to adopt regulations will lose the power to override certain federal banking regulations. GLB, *supra* note 10, § 6805(c).

36. 12 U.S.C. 1843(k)(1)(A) (2000).

tivity and does not pose a substantial risk" to safety and soundness.[37] This broad definition is an advantage for banks and other institutions that are clearly financial in nature, because they are clearly covered by the privacy rules and can now combine with a wider range of entities. The broad definition, however, also has the effect of bringing more entities within the scope of GLB privacy protections than would be apparent from the term "financial institutions." Examples include many travel agencies, law firms that provide tax and financial planning advice, and retail stores with installment credit operations.[38] The reach of the privacy protections is thus greater than many initially realized.

State law may also operate in ways that make GLB more powerful for privacy than the statute would be standing alone. As enacted, GLB specifically provides that it acts as a floor, but states may provide stricter privacy protections if they so choose.[39] As discussed below, this possibility of additional state legislation serves as an important goad for financial institutions to reassure state legislators and the general public that they are treating sensitive data with the appropriate level of confidentiality. Stricter state law may turn out to be especially important in the enforcement area. GLB does not provide a private right of action. The statutory language on relation to state law, however, specifically permits an "order" or "interpretation" to be stricter at the state level.[40] This language may be important in the context of a state tort or contract claim that alleges that a financial institution failed to protect a customer's privacy. Even if GLB itself does not create the private right of action, the statute appears to allow the state claim to proceed to an eventual "order" by a judge who may "interpret" federal and state law. In a tort case, for instance, a bank's violation of the federal privacy regulation may assist a plaintiff in showing that the bank violated a standard of reasonable care. The level of privacy protection contemplated by GLB may turn out to highly relevant to what is held to be a breach of duty in state court.

II. THE HISTORY AND RATIONALE OF FINANCIAL PRIVACY LEGISLATION

The financial privacy provisions of GLB Title V were not inevitable. Indeed, financial reform came very close to passage in 1998 without having any noticeable privacy provisions.[41] In 1999, by contrast, privacy

37. 12 U.S.C. 1843(k)(1)(B) (2000) (emphasis added).

38. The definition of "financial institutions" clearly includes many travel agencies. 16 C.F.R. § 313.1 (2002). For an additional discussion of the breadth of the term "financial services," see 65 Fed. Reg. 33,647 (May 24, 2000).

39. GLB, *supra* note 10, § 6807(b).

40. *Id*.

41. *See* Financial Services Competitiveness Act of 1997, H.R. 10, 105th Cong.

became a leading political issue in the legislative debates. President Clinton put forward privacy proposals in May.[42] The House of Representatives almost unanimously passed a privacy amendment in July,[43] most of whose provisions were signed into law in November.[44] Upon signing the bill, furthermore, President Clinton called for additional privacy protections in future legislation,[45] and the Administration proposed such legislation in the spring of 2000.[46]

These financial privacy developments, furthermore, happened alongside heated debates on medical privacy, Internet privacy, and related topics. How can we capture the reasons why privacy and data protection issues climbed so swiftly up the policy agenda in the United States in the past few years? To answer this question requires us to recognize that we are currently in the second major wave of privacy law reform, and to understand what differs from the first major wave.

A. THE FIRST WAVE OF PRIVACY LEGISLATION

The first major wave of privacy activity took place in the early 1970's, largely in response to the rise of the mainframe computer. The chief worry in that period was the spectre of the enormous, centralized database. The chief areas of concern, as evidenced by the passage of legislation, were credit reporting agencies and the federal government.

For credit histories, the concern was that the fragmented legacy of local credit agencies was turning into a few nation-spanning databases. The newly national databases, according to contemporary studies, contained a disturbingly large amount of unverified and often incorrect information. Individuals were apparently being turned down for mortgages

(1998); *see also* Leslie Wayne, *Senate Panel Delays Vote on Overhaul of Banking Laws*, N.Y. TIMES, Sept. 4, 1998, at C4 (bill delayed even though "[m]omentum had been building in Congress for the Senate to take up the measure before adjourning in October").

42. Press Release, The White House, Press Background Briefing by Senior Administration Officials on Financial Privacy (Apr. 30, 2000), *available at* www.privacy2000.org/archives/POTUS_4-30-00_press_background_briefing_on_financial_privacy_htm.

43. The Oxley Amendment to H.R. 19 was agreed to by a vote of 427 to 1 on July 1, 1999. *See* H. Res. 235, 106th CONG. REC. 5304-16 (1999).

44. GLB, *supra* note 10, §§ 6801-09.

45. President William Clinton, Remarks by the President at Financial Modernization Bill Signing (Nov. 12, 1999), *available at* www.privacy2000.org/archives/POTUS_11-12-99_Remarks_by_president_at_financial_moderniztion_bill%20signing.htm.

46. Press Release, The White House, Office of the Press Secretary, Clinton-Gore Plan to Enhance Consumers' Financial Privacy: Protecting Core Values in the Information Age, (Apr. 30, 2000), available at www.privacy2000.org/archives. The Administration's bill was introduced in the Congress as H.R. 4380 and S. 2513. *See supra* note 27.

or jobs based on inaccurate information, some of which was provided by careless or malicious persons.[47] In the face of these concerns about the centralized databases, Congress passed the Fair Credit Reporting Act in 1970.[48] The Act establishes a number of fair information practices, including individuals' right to access their own records and to seek to correct mistakes in those records.[49]

A similar fear of centralized databases led to the Privacy Act of 1974, which governs the creation and use of federal government systems of records.[50] The fear of Big Brother—a unified and government-run database—was an important motivation for the Privacy Act. A crucial feature of the Act generally prohibits transfers from one federal agency to another except with the individual's consent.[51] Whatever the imperfections in the reach or application of the Privacy Act,[52] it has succeeded in preventing the creation of the omnivorous, unified federal database.

Since 1974, a number of significant privacy laws have been adopted in the United States, covering such areas as government access to financial records,[53] searches of materials related to publication and broadcast,[54] cable television records,[55] electronic wiretaps,[56] video records,[57] employee polygraph tests,[58] telemarketing calls,[59] motor vehicle records,[60] aspects of customer telephone records,[61] and children's records for on-line activities.[62] Not until recently, however, has there seemed a

47. *See generally* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS, (1971); L. RICHARD FISCHER, THE LAW OF FINANCIAL PRIVACY, ch. 1 (Warren, Gorham & Lamont Banking 1998).

48. 15 U.S.C. §§ 1681-1681U (2000).

49. *Id*. at § 1681g.

50. Privacy Act of 1974, 5 U.S.C. § 552a (2000).

51. *Id*. at § 552a(b). Transfers among agencies are also allowed in a number of other statutory exceptions, including for "routine uses" that are published in the Federal Register. *Id*.

52. Robert Gellman, "How to Amend the Privacy Act," Access Reports (1997).

53. Right to Financial Privacy Act of 1978, 12 U.S.C. §3402 (2000).

54. Privacy Protection Act of (1980), 42 U.S.C. § 2000aa (1994).

55. Cable Communications Policy Act of (1984), 47 U.S.C. § 551 (1996).

56. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-2519 (2000).

57. Video Privacy Protection Act of 1998, 18 U.S.C. § 2710 (2000).

58. Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2002 (1994).

59. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (1994).

60. Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721-2725 (1994).

61. Telecommunications Act of 1996, 47 U.S.C. § 222 (Supp. 111 1997).

collected in Marc Rotenberg, THE PRIVACY LAW SOURCEBOOK 2000 (Electronic Privacy Information Center). (Have source, locating)

real possibility of creating wide-ranging privacy rules that would reshape information practices in major economic sectors.

Shifts in the underlying technology spurred the wave of privacy reform in the 1990s.[63] First, the fear in the 1970's was prompted by the new mainframe technology. Today, everyone has a mainframe—a modern laptop or desktop computer outperforms the mainframes of the earlier era. The number of databases has thus grown exponentially. Second, in the 1970's, the Internet was only an experimental system available to some government agencies and scientific researchers. Today, transfers among computers are entirely different. For most practical purposes, transfers today are free, instantaneous, and global.

The new databases and new transfers among databases led to a major spike in public concern about privacy issues. The public expressed concern that sensitive personal data was becoming available in new ways to a new range of people. Perhaps the clearest message about the salience of privacy came from a Wall Street Journal poll in September, 1999, just as House and Senate negotiators were debating the privacy provisions in GLB. In the lead-up to the year 2000, the poll asked Americans what they feared most in the coming century.[64] Out of a dozen choices, including threats such as international terrorism, global warming, and nuclear holocaust, the leading answer was "erosion of personal privacy." The poll reported that 29 percent of respondents put privacy either first or second out of the dozen choices. No other issue received more than 23 percent.

B. THE SECOND WAVE: PRIVACY DEVELOPMENTS OUTSIDE OF FINANCIAL MODERNIZATION

A comprehensive history of the privacy politics in the 1990s has yet to be written. For the present purpose, to understand the origins of Title V of GLB, we can identify some of the major aspects of the wave of policy activity in the late 1990s.

Public attention focused most intensively on the growing issue of Internet privacy, especially information collected at web pages. The Clinton Administration early on gave some attention to the issue as part of the Information Superhighway project. The Federal Trade Commission became involved in Internet privacy by 1995. The FTC was increasingly viewed as the cop on the Internet beat due to its power to enforce against "unfair and deceptive" trade practices, such as violations of web

63. The shift from mainframes to distributed processing is discussed in more detail in SWIRE & LITAN, *supra* note 6, at ch. 3.

64. Christy Harvey, *American Opinion (A Special Report): Optimism Outduels Pessimism*, WALL ST. J., Sept. 16, 1999, at A10.

privacy policies. Within the Administration, e-commerce leader Ira Magaziner announced the basic policy of encouraging industry self-regulation in the summer of 1997. Secretary of Commerce William Daley personally became involved in encouraging industry to improve privacy practices as part of the development of e-commerce.

In May, 1998, Vice President Gore elevated the privacy issue to the White House level in a speech announcing an "Electronic Bill of Rights."[65] In this speech, and a follow-up event in July, 1998, the Vice President set forth a four-part policy structure that the Administration essentially followed until the end of its second term.[66] First, the Vice President called for privacy legislation to protect especially sensitive information. This category of "sensitive" information initially included medical records, children's activities on-line, and some financial records. Second, the Administration supported self-regulation for privacy in other areas, while continually pushing industry to take effective steps to improve privacy protection. The implicit understanding was that the Administration might switch to supporting Internet privacy legislation if industry did not act effectively. Third, the Federal government should act as a model for good privacy practices. Fourth, the Office of Management and Budget was given responsibility for coordination of privacy issues.[67] To assist in carrying out this task, I was named as Chief Counselor for Privacy, in OMB, in March, 1999.[68]

Meanwhile, a largely separate debate had been occurring for the area of medical privacy.[69] Medical privacy proposals were extensively

65. Vice President Gore announced the electronic bill of rights at a New York University Commencement speech. White House, Vice President Gore Announces New Comprehensive Privacy Action Plan for the 21st Century, (May 14, 1998), *available at* www.privacy2000.org/archives.

66. Office of the Vice President, "Vice President Gore Announces New Steps Toward an Electronic Bill of Rights," July 31, 1998, *available at* www.privacy2000.org/archives [hereinafter New Steps]

67. "OMB will be given responsibility for coordination of privacy issues, drawing on the expertise and resources of other government agencies. This will help improve the coordination of U.S. privacy policy, which cuts across the jurisdiction of many federal agencies." *Id*. OMB had long maintained responsibility of overseeing agency implementation of the Privacy Act. 5 U.S.C. 552a(v) (2000). The change was that OMB would now have responsibility to coordinate privacy issues generally, including financial and medical privacy issues, and not simply oversight for federal systems of records under the Privacy Act.

68. Robert O'Harrow, Jr., *Clinton Names Counselor on Privacy*, WASH. POST, Mar. 4, 1999, at E2.

69. The debate was "separate" in the sense of having different actors involved. The Department of Health and Human Services was the lead agency for medical privacy as opposed to the Department of Commerce and the independent agency FTC for Internet privacy. In the Senate, medical privacy was considered in the Health, Education, Labor,

considered leading up to passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[70] HIPAA mandated new rules so that providers and insurance companies would shift to electronic medical records. There was widespread agreement that privacy and security protections should be created as part of this shift to electronic records. In HIPAA, Congress set itself a deadline of August, 1999 to write medical privacy legislation. If it did not do so, then the Department of Health and Human Services (HHS) was required to promptly issue a medical privacy regulation.

The HIPAA deadline contributed to a new peak of privacy policy activity in the period before and during consideration of GLB in 1999. HHS Secretary Donna Shalala, drawing on a large inter-agency process, announced the Administration's recommendations for medical privacy legislation in the fall of 1997.[71] Vice President Gore announced medical privacy initiatives in the summer of 1998, and called for strong medical privacy legislation.[72] The Congressional committees responsible for health care worked on numerous legislative proposals, trying in vain to pass legislation before HHS

gained regulatory authority in August, 1999.[73] As it became increasingly clear that Congress was unlikely to act, the Administration prepared a detailed proposed medical privacy regulation. President Clinton announced the proposed rule in an Oval Office ceremony on October 31, 1999, less than two weeks before he signed GLB.

The Internet privacy and medical records debates helped create the affirmative arguments for why privacy protections would be appropriate as well for financial records. At the same time, the political context for GLB was being shaped by developments in the European Union, the U.S. debate on encryption policy, and the so-called "Know Your Customer" rules.

---

and Pensions Committee, while Internet privacy was in the Commerce, Science, and Transportation Committee. In the House, medical privacy was principally considered in the Ways and Means Committee and one subcommittee of the Commerce Committee, while Internet issues were handled in a different subcommittee of the Commerce Committee.

70. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191.

71. *See* Shalala Urges Congress to Protect Americans' Personal Medical Records, (Sept. 11, 1997), *available at* http://www.hhs.gov/news.press/ 1997pres/970911.html.

72. New Steps, *supra* note 66. For instance, the Vice President announced that the Administration would not develop standards for unique health identifiers as called for by HIPAA, until and unless strong privacy protections were in place. *Id*.

73. *Health Care Policy: Congressional Roundup*, 8 HEALTH L. REP. (BNA) No.42, at 1728 (Oct. 28 1999).

The European Union Data Protection Directive was ratified in 1995, with implementation scheduled for October, 1998.[74] The Directive requires harmonized and generally strict privacy protections within the fifteen member states of the European Union. Article 25 of the Directive said that personal information could be transferred to other countries only if they had "adequate" privacy protections.[75] Article 25 raised the possibility that trade with Europe could be significantly disrupted if the United States was found to lack "adequate" protections.[76]

Reasonable people can differ about the extent that the Directive pushed the United States toward passage of Title V or stricter privacy protections generally. In my view, the debates about the Directive at a minimum educated and sensitized a greater range of U.S. policy officials to privacy issues. Awareness of the detailed privacy regulations in Europe made it easier to imagine similar regulations in the United States and more difficult for industry to say that such regulations would be unworkable.[77] In the financial services area, the most publicized enforcement action in Europe was brought against Citibank, and policy discussions about the Directive foreshadowed the issues that arose in the GLB debates.[78]

The debate about encryption policy brought fervor to the privacy issue while involving many members of Congress.[79] The legal issue at the heart of the debate was setting the terms under which encryption software and hardware could be exported from the United States. Law enforcement and national security officials were concerned that criminals would deploy encryption domestically and that the United States would lose its ability to read messages that intelligence sources gathered from abroad. E-commerce companies supported strong encryption as a necessary tool for securely conducting business transactions over the Internet. Encryption enthusiasts and privacy supporters entered the debate with passionate

74. *See generally* SWIRE & LITAN, *supra* note 6.

75. Directive, Art. 25. Article 26 creates a number of exceptions that can permit transfers to countries that lack "adequate" protection.

76. Intensive discussions with the European Union, led on the United States side by David Aaron and Barbara Wellbery, eventually resulted in the spring of 2000 with a "safe harbor" agreement. Essentially, companies that agree to be bound by safe harbor privacy principles are allowed to share data freely between their European Union and U.S. operations. *See* safe harbor website, *available at* http://www.export.gov/safeharbor.

77. DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 259 (1995).

78. The Swire and Litan book about the Directive devoted a chapter specifically to financial services privacy issues, and also examined a number of the specific situations that became exceptions under GLB § 502(e). SWIRE & LITAN, *supra* note 6, at ch. 4.

79. For a detailed and readable history of the encryption debate, *see generally* PAUL LEVY, CRYPTO 1-2 (2000).

rhetoric about the importance of strong encryption to individual liberty on the Internet.[80]

The Clinton Administration initially sided with the law enforcement and national security position, supporting in 1993 the "Clipper chip" that would have facilitated government access to encrypted communications.[81] Encryption continued to be a hotly debated issue throughout 1998 and 1999.[82] In June, 1999—as the House was preparing to vote on the financial modernization bill—encryption privacy bills passed both the Senate and House Commerce Committees.[83] In September, 1999, as the financial modernization conference committee was deliberating, the White House announced a major shift on encryption in the direction of greater exports and privacy protection.[84] The encryption debate, stretching over several years, culminated in literally hundreds of members of Congress announcing their support for stronger encryption, and thus the greater privacy protections that would result.[85]

Meanwhile, the "know your customer" rule brought new attention to issues of financial privacy. The regulation was proposed by federal banking regulators in late 1998 as part of the ongoing efforts to crack down on money laundering.[86] The rule used language that provoked a privacy alarm:

> As proposed, the regulation would require each bank to develop a program de-

80. For a history of the policy debate from a civil liberties perspective, as well as current news and legislation, *see, e.g.*, http://www.cdt.org/crypto.

81. John Mintz, *U.S. Moves to Ensure Its Ability to Eavesdrop*, WASH. POST, Apr. 17, 1993, at A9 (discussing announcement of the Clipper Chip); *see also* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PENN. L. REV. 709, 717-718 (1995) (discussing legal issues implicated by Clipper Chip).

82. For a detailed chronology of the period, see http://www.cdt.org/ previousheads/encryption.shtml.

83. *Id*.

84. Press Release, The White House, Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire, (Sept. 16, 1999), *available at* http://www.privacy2000.org/archive. "I'm here to underscore that today's announcement reflects the Clinton Administration's full support for the use of encryption and other new technologies to provide privacy and security to law-abiding citizens in the digital age." Remarks of Peter Swire. *Id.*

85. *See, e.g.,* Joe Salkowski, *Encryption Campaign Ends With a Triumph for Common Sense*, CHI. TRIB., Sept. 27, 1999, § 4, at 6 (reporting that a majority of members of the House supported the House encryption privacy bill).

86. The discussion here draws on an analysis of money laundering laws and privacy, written in early 1999. Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 487-92 (1999). For an extremely detailed treatment of money laundering laws, see L. RICHARD FISCHER, THE LAW OF FINANCIAL PRIVACY ¶¶ 4.01-4.13 (3d ed. 1991).

> signed to determine the identity of its customers; determine its customers' sources of funds; determine the normal and expected transactions of its customers; monitor account activity for transactions that are inconsistent with those normal and expected transactions; and report any transactions of its customers that are determined to be suspicious, in accordance with the [agency's] existing suspicious activity reporting regulation.[87]

In immediate response to the proposal, press accounts appeared describing the rule as "an Orwellian intrusion into Americans' privacy."[88] Opposition arose from a combination of conservative, liberal, and libertarian groups, foreshadowing a coalition that emerged again in the GLB debates.[89] More than 200,000 comments rolled in, almost all of them negative.[90] Privacy had become a mobilizing issue politically. The rule was retracted in March, 1999.[91]

These five privacy debates—Internet privacy, medical records, the European Directive, encryption, and know your customer—were thus all in full swing in early 1999 as Congress prepared to debate the financial modernization bill. Many in the financial services industry thought that the 1999 modernization bill would closely resemble the 1998 bill that almost passed. These industry insiders had a difficult time understanding how privacy suddenly became so important in the 1999 financial debates. For those who had been engaged in the other privacy debates, however, the question seemed different—why shouldn't financial records, which most people consider very sensitive, be subject to privacy protections, too?

C. THE POLICY CONTEXT IN 1999 FOR FINANCIAL PRIVACY

In considering financial privacy legislation, one can start with some

87. Know Your Customer Requirements, 63 Fed. Reg. 67524 (Dec. 7 1998) (to be codified at 12 C.F.R. pt. 21).

88. Declan McCullagh, *Banking with Big Brother*, *available at* http://www.wired.com/news/print/0,1294,16749,00.html (last modified Dec. 10, 1998).

89. *Id*. Groups expressing opposition included the Free Congress Foundation, a conservative group, the Libertarian Party and American Civil Liberties Union, libertarian groups on the right and left, and the Electronic Privacy Information Center, a generally liberal group. In the GLB debates, generally conservative Republican Senator Richard Shelby and Representative Joe Barton teamed with generally liberal Democrats such as Senator Richard Bryan and Representative Edward Markey to support stricter financial privacy protections. *Digest*,WASH. POST, Nov. 11, 1999, at E1 (these four members of Congress introduce stricter financial privacy bill).

90. Robert O'Harrow, Jr., *Disputed Bank Plan Dropped; Regulators Bow to Privacy Fears*, WASH. POST, Mar. 24, 1999, at E1 (over 200,000 comments); Michael Kelly, *Banking With Big Brother*, WASH. POST, Feb. 3, 1999, at A17 (all but 12 comments to FDIC on the rule, out of 15,000, were negative).

91. O'Harrow, *supra* note 90.

basic goals. A first goal, in a democracy, is to have the laws match the desires of the public. In the legislative debates, one important consideration was the widely held view that financial records contain sensitive personal information. Repeated polls have shown that Americans place financial information in an especially sensitive category with medical records and certain other information, such as gathering data on children surfing on-line.[92] In a democracy, there is a straightforward logic to providing stricter protections for information that citizens consider especially important.

A second goal is to maximize the benefits of legislation. There is an efficiency argument for having stricter protections for sensitive data.[93] In the contract between an individual and a company, it is more efficient if the contract reflects what well-informed parties would agree to, if there were no costly hurdles to their reaching an agreement. Other things equal, individuals will bargain for greater protection for more sensitive data. Individuals may be indifferent if marketers know which flavor of toothpaste they use, but may care considerably more if their psychiatric history or the history of every purchase they had ever made became widely available. It is likely efficient to set stricter default rules for sensitive medical and financial data than for toothpaste sales.

A third goal is to minimize the costs of legislation. Some kinds of data sharing promote efficiency. One important example is the prevention of fraud. Lenders need accurate credit reports before they make loans, and credit card companies watch for out-of-pattern purchases that may indicate that a thief has stolen the credit card. A well-designed privacy regime would achieve the benefits of treating sensitive information carefully while permitting these desirable forms of information sharing.

Where the benefits of privacy protection appear to outweigh the costs, an additional question is how a legislative approach would compare with alternative institutional approaches.[94] In the privacy context,

92. A Gallup survey found that 84 % of respondents stated that the privacy of

93. For a more extended discussion of the efficiency argument, including discussion of typical market failures and government failures in privacy regulation, see Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* U.S. Dept. of Commerce, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 3, 5-8 (1997) [hereinafter, Swire, *Markets*].

94. On the importance of comparative institutional analysis, see generally NEAL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS,

one hope has been that technological measures could protect individuals' information without the need for legal protections. Perhaps encryption or other technical measures will mean that the only people who see the data are those that the individual chooses. I have argued elsewhere, however, that a purely technological approach will not work well for most personal financial data.[95] To give just one example, lenders will insist on seeing considerable financial data before trusting a borrower with a loan. We should thus expect that financial institutions will continue to gather considerable information about their customers, and the privacy challenge will be who will get to see that information, on what terms.

Another possible approach to consider is self-regulation, where industry creates the standards for privacy protection. How to choose between self-regulation and government rules is a complex question, with the answer varying with the circumstances.[96] For financial services, several factors tipped the balance toward a legislative approach. First, legislation is more generally appropriate for sensitive data where consumer concerns and potential harms from misuse are greater. Second, there was evidence that the banks were not performing well on self-regulation. A 1998 FTC report found that only sixteen percent of banks had any privacy notices or policies on their on-line web sites.[97] Third, the self-regulatory codes from bank industry groups were at a very high level of generality, and there was considerable uncertainty about the extent to which these codes were improving actual practice.[98] Finally, having financial regulatory agencies already in place made it easier institutionally to imagine an effective regulatory regime. For instance, bank examiners already had to check banks' internal systems, so they could fairly readily check as well to see whether privacy and security rules were being followed.

Given the weaknesses of technological or self-regulatory approaches, the case for a legislative approach became more compelling. That case was strengthened by two factors—industry convergence and

AND PUBLIC POLICY 1-50 (1994).

95. Peter P. Swire, *The Uses and Limits of Financial Cryptography: A Law Professor's Perspective*, *available at* http://acs.ohio-state.edu/units/law/swire.pscrypto.htm.

96. For my analysis of how to make this choice generally, *see* Swire, *Markets*, *supra* note 93.

97. The statistics from the 1998 FTC report were: only 16% of all financial web sites

Policy Notice." FTC, *Privacy Online: A Report to Congress*, at 27 (1998) *available at* http://www.ftc.gov/reports/privacy3/ index.htm.

98. *See generally* CONSUMER BANKERS ASSOCIATION, FINANCIAL PRIVACY IN AMERICA: A REVIEW OF CONSUMER FINANCIAL SERVICES ISSUES (1998) (constituting a collection of financial privacy statements from the period).

the newly increased level of detail in financial records.

Convergence was a principal industry goal for financial modernization legislation. The 1933 Glass-Steagall Act[99] and subsequent legislation created legal barriers to combining the major financial companies that serve consumers, such as commercial banks, insurance companies, securities brokers, and mutual funds. Over time, loopholes developed so that some alliances were permitted between commercial banks and other financial companies.[100] GLB swept away the remaining barriers to affiliation. As mentioned above, financial holding companies may now engage in any activity that regulators determine "to be financial in nature or incidental to such financial activity."[101] By bringing together previously separate institutions, proponents of modernization hoped to achieve substantial benefits, such as one-stop shopping for consumers, the ability to create new products and lines of business, and diversification of risk for previously specialized sellers.[102]

Those concerned about privacy, however, had a different perspective. They pointed out that privacy protections had been an essential component of medical system reform in HIPAA, as well as in the 1996 Telecommunications Act, which permitted convergence in the telecommunications industry.[103] There was both a political and policy logic to linking privacy with convergence. The political logic was that the best moment to create privacy protections, which industry opposed, was when industry badly wanted legislation to allow convergence, which industry favored.[104] It would be far more difficult to create legislative momentum for privacy except when industry also wanted a bill. The policy logic

99. Sections 20 and 32 of the Glass-Steagall Act, which were specifically repealed by the 1999 reform, were the key sections prohibiting combinations of commercial and investment banks. 12 U.S.C. §§ 78, 377 (*repealed by* Section 101(a)-(b) of the Gramm-Leach-Bliley Act).

100. For instance, "Section 20" affiliates allowed limited underwriting of securities through affiliates of commercial banks. Sec. Indus. Ass'n. v. Clarke, 885 F.2d 1034 (2nd Cir. 1989). *See generally* JONATHAN R. MACEY & GEOFFREY P. MILLER, BANKING LAW AND REGULATION (1992) (presenting abundant cases eroding Glass-Steagall barriers).

101. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102 §103(a), 113 Stat. 1338, 1342 (1999) (to be codified at 12 U.S.C. § 1843(k)(1)(A)).

102. *See generally* ROBERT E. LITAN, WHAT SHOULD BANKS DO? 60-143 (1987) (presenting an insightful analysis of the advantages and disadvantages of convergence); *but see* Arthur E. Wilmarth, Jr., *The Transformation of the U.S. Financial Services Industry, 1975-2000; Competition, Consolidation, and Increased Risks*, U. ILL. L. REV. (forthcoming, 2002) (expressing skepticism about the likelihood of these benefits being realized).

103. Telecommunications Act, P.L. 104-104, at Sec. 222, enacted in 1996.

104. I heard this rationale articulated most clearly by Rep. Edward Markey, who was unusual among members of Congress in having been active on HIPAA, the Telecommunications Act, and GLB.

was that convergence would result in larger enterprises as well as mergers of firms that previously were in separate lines of business. Larger enterprises would mean larger databases, with greater privacy risk. Mergers of separate industries would mean that consumers who gave information to a company in one sector would now have that data shared with different sectors—the sort of secondary use that fair information practices generally forbid unless there is customer consent.

The newly increased level of detail in financial databases provided another important argument in favor of privacy protection. The contrast with the 1970 Fair Credit Reporting Act had become stark. A credit report, for instance, might show that an individual had borrowed up to a $10,000 credit limit, and had once paid thirty days late. By 1999, by contrast, electronic financial databases operated at the level of each transaction rather than the summary level. As I have discussed elsewhere in detail,[105] there are strong trends toward having permanent, electronic, and searchable records of individual consumer transactions. Purchases are shifting from cash and checks, which do not usually go into searchable databases, to much greater reliance on credit and debit cards, which generally do. Consumers have incentives, such as frequent-flyer programs, to use credit and debit cards. Such cards have become the standard payment mechanism for the growing world of Internet purchases. And less affluent Americans are increasingly receiving government benefits through smart cards and other electronic-based systems.

These changes create a detailed, lifetime record of a large and growing fraction of individuals' purchases. Under Secretary of the Treasury Gary Gensler explained the problem in his testimony in the summer of 1999:

> A generation ago, financial privacy meant keeping private your salary, your bank balances, and your net worth. Today, financial privacy means keeping secret your entire way of life. . . . The credit card records of 1999 . . . can list each and every purchase ever made by that customer, sorted by date, location, and other details. Furthermore, if credit card companies work together with merchants, then the level of detail can become even more refined—each dish ordered at a restaurant or each book title bought at a store.[106]

This unprecedented level of detail, combined with the possibility of comprehensive matching with other merchant databases, is a distinctive feature of financial records. In response to this distinctive problem, there was a strong argument for a distinctive legal regime to address the prob-

105. Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, *in* BROOKINGS-WHARTON PAPERS ON FINANCIAL SERVICES 391-442 (Robert E. Litan et al. eds.) (1999).

106. *See* Testimony of Under Secretary of the Treasury Gary Gensler, *at* http://www.privacy2000.org/archives/Treasury_6-14-00Gensler_testimony%20_on_hr4585.htm (last visited Mar. 11, 2002).

lem.

D. THE 1999 LEGISLATIVE HISTORY

Early in 1999, the pressure to protect financial privacy was not easy to detect. Financial modernization had nearly passed at the end of 1998, only to get hung up when the Administration and Congressional Republicans could not agree on the Community Reinvestment Act and the role of the Treasury Department in financial regulation.[107] The House and Senate Banking Committees both passed financial modernization bills in March, with no significant privacy provisions.[108]

The situation changed shortly thereafter. On May 4, President Clinton gave what I believe was the first presidential address in history dedicated to privacy protection.[109] The President stated that financial data was sensitive information deserving of legal protection, and consumers should have an opt-out choice before data is shared with affiliates or third parties. Two days later, the Senate adopted some modest privacy provisions aimed at preventing "pretext calling," the fraudulent procurement of personal financial information.[110]

Attention to privacy climbed another notch on June 7, when lead bank regulator Jerry Hawke used unusually strong language in criticizing banks' privacy practices.[111] In a speech to industry, Hawke objected to practices "that are at least seamy, if not downright unfair and deceptive."[112] He particularly condemned the sale of customer financial information to telemarketing firms. Two days later, Minnesota Attorney General Mike Hatch announced a lawsuit against U.S. Bank for particularly egregious sales of such information. According to the complaint, U.S. Bank sold account numbers, Social Security numbers, and other detailed information to the marketing firm Member Works.[113] Member

107. Dean Anason, *Supporters of Reform Bill Rally for a Rematch*, AM. BANKER, Oct. 23, 1998, at 1.

108. Stephen Labaton, *Congress Acts to Alter Rules on Banking*, N.Y. TIMES, Mar. 5, 1999, at C4 (describing both bills without mentioning privacy).

109. Remarks Announcing the Financial Privacy and Consumer Protection Initiative, I PUB. PAPERS 682 (May 4, 1999) *available at* www.privacy2000.org/archives (last checked Mar. 17, 2002).

110. R. Christian Bruce, *Senate Clears Financial Modernization Bill, Defeating Operating Subsidiary Amendment*, BNA BANKING REP., May 10, 1999, at 825.

111. Remarks by John D. Hawke, Jr., Comptroller of the Currency, before a Conference Sponsored by the Consumer Bankers Association (June 7, 1999).

112. *Id*.

113. U.S. Bank provided the following information about its customers:

> name, address, telephone numbers . . ., gender, marital status, homeownership status, occupation, checking account number, credit card number, Social Security number, birth date, account open date, average account balance, account fre-

Works asked consumers on the phone if they were interested in saving money on dental or health plans. If the consumer said yes, then Member Works would send a postcard stating that the consumer had thirty days to opt out of the plan. If the consumer did not opt out, then Member Works would automatically withdraw money from the consumer's U.S. Bank account. The privacy policy of U.S. Bank, a major financial firm, said it would strive to maintain customer confidentiality.[114] It gave no indication that any data was supplied to telemarketers or other outside firms.

The next day, the House Commerce Committee reacted to this news.[115] The key action occurred during a discussion of an amendment offered by Rep. Edward Markey, a liberal Democrat who personally supported a strict opt-in before sharing with third parties or affiliates. Markey's amendment was similar to President Clinton's position, with opt-out before sharing with third parties or affiliates. The amendment also included language addressed to the U.S. Bank situation, barring release of bank account numbers to telemarketers. In a remarkable sequence, conservative Republican Joseph Barton expressed his anger at receiving a Victoria's Secret catalogue at his Washington apartment. He said that his address had been supplied by his credit card company, and stated his displeasure of what his wife back home in Texas would think of his perusing such a catalogue when he was in Washington. Democratic Representative Anna Eshoo said that someone had stolen her credit card number the previous year, and described how difficult it was to clear up this instance of identity theft. Ranking Democrat John Dingell suggested to his colleagues that their opponents in the next election would find it useful to leaf through the members' personal financial records. Suddenly, the Markey amendment was approved in a voice vote. Industry lobbyists were in shock. Privacy advocates were surprised and delighted.[116]

> quency information, credit limit, credit insurance status, year to date finance charges, automated transactions authorized, credit card type and brand, number of credit cards, cash advance amount, behavior score, bankruptcy score, date of last payment, amount of last payment, date of last statement, and statement balance.

Minnesota Attorney General Hatch Sues U.S. Bank for Disclosing Customers' Private Information to Telemarketer, PR NEWSWIRE, June 9, 1999.

114. *Id*.

115. The account here is based on my own recollection and corroboration from others who attended the House Commerce Committee markup.

116. The discussion here is primarily intended to describe the legislative history of GLB rather than to develop a theory of the legislative process. Nonetheless, the House Commerce Committee mark-up poses something of a puzzle for public choice theorists who expect a politically mobilized industry, such as the financial services industry, to succeed against those supporting the general public's diffuse interest in privacy protection.

The House Commerce Committee vote redefined the privacy debate for the year. The Administration, most Congressional Democrats, and a few Republicans tried to retain the privacy protections that the Commerce Committee had approved. Most Congressional Republicans worked with industry to draft more limited protections. At the next step, the Republican-controlled House Rules Committee eliminated the privacy protections approved by the Commerce Committee.[117] On the House floor, the privacy issue, which had been practically invisible a few months earlier, was the predominant topic of debate. On a procedural vote, the House rejected a Democratic proposal to reinstate the House Commerce version.[118] The House then, by a nearly unanimous vote, approved an amendment that required an opt-out for transfers to third parties.[119] Even those who had opposed the stricter privacy version spoke at length about the importance of keeping the bill's existing privacy protec-

117. *U.S. House Clears Way to Debate on Bank Overhaul Bill*, BLOMBERG NEWS, July 1, 1999.

118. For the final House vote, the Clinton Administration supported the privacy provisions ultimately included in the House bill while calling for the additional protections discussed in the President's speech in May:

> The President has stated the importance of adopting protections to ensure the privacy of consumers' financial records. Adoption of the amendment to be considered by the House would improve the bill by including new privacy protections, although it does not address all of the issues involved. The Administration will continue to pursue additional protections.

The White House, Statement of Administration Position, July 1, 1999, *available at* www.privacy2000.org/archives.

The White House objected to a provision that would have governed medical information in financial holding companies:

> The Administration also has serious concerns about the provisions on medical privacy in this financial services legislation. Unfortunately, the current approach would preempt important existing protections and does not reflect extensive legislative work that has already been done on this complex issue. The Administration thus supports striking the medical privacy provisions, and pursuing medical privacy in other fora.

Id. The medical privacy provision was eliminated in the GLB conference. President Clinton's 2000 legislative proposal would have addressed the issue of medical information that is held by financial holding companies but not covered by the HIPAA medical privacy protections. Consumer Financial Privacy Act, H.R. 4380, 106th Cong; Financial Information Privacy Protection Act of 2000, S. 2513, 106th Cong. The House Banking Committee approved such legislation in 2000, but the bill did not progress further. Medical Financial Privacy Protection Act, H.R. 4585, 102d Cong. § 2 (2000). The current legality of sharing medical data among affiliates, such as a life insurance company sending medical information to a lending affiliate, remains a possible impetus for additional privacy legislation that would affect financial institutions.

119. *House Passes Financial Services Bill by Large Margin after Procedural Skirmish*, BNA BANKING REPORT, July 5, 1999, at 5.

tions,[120] confirming the issue's importance as the House and Senate entered a conference to reconcile their bills.

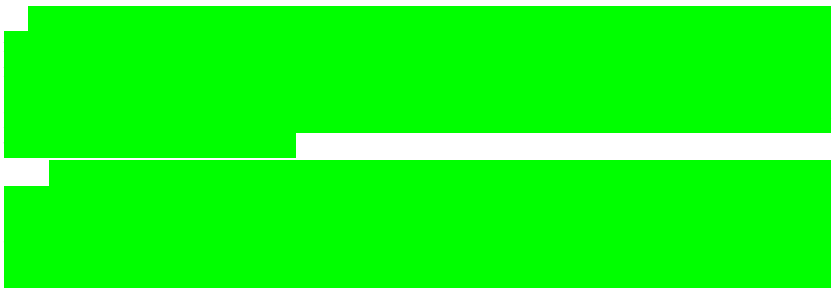
Negotiations in the conference committee lasted from early July to October. As the Republican committee chairmen neared a compromise proposal, the Administration for the first time included privacy as a basis for vetoing the bill if protections were not strict enough.[121] The committee chairmen then released their "chairmen's mark," which was weaker on privacy than the version passed in the House.[122] As negotiations on privacy and other issues continued, the conference committee made the chairmen's proposal stricter on privacy in three respects: the more protective House version mostly replaced the chairmen's mark; the bill required notice for transfers to affiliates, and not just to third parties; and the bill specifically provided that states can offer stricter privacy protections than the federal floor.[123] Stricter privacy amendments were rejected by the conference committee. After a few more days of grueling negotiations on other issues, the Administration and Congressional leaders reached agreement on October 22. President Clinton signed the Gramm-Leach-Bliley Act on November 12, praising the legislation in general but calling for stricter privacy legislation in the future.[124]

120. For instance, Republican Rep. Marge Roukema said about the amendment: "This gives us more privacy than under any law that we have ever had. This is a giant step in the right direction." *Id*.

121. Barbara A. Rehm, *Key Disputes Still Unresolved as Financial Reform Votes Near*, AM. BANKER, Oct. 11, 1999 at 1 (describing veto threat by White House Chief of Staff John Podesta). The Clinton Administration had repeatedly threatened to veto the bill on other grounds, but the inclusion of privacy in this veto letter was evidence of the increased importance of the issue in the course of the year. The letter's other bases for a possible veto concerned the allocation of regulatory authority between the Treasury Department and the Federal Reserve, the Community Reinvestment Act, and retaining restrictions on the ability of depository institutions to affiliate with nonfinancial firms.

122. Dean Anason, *GOP Reform Compromise Draws New Veto Threat*, AM. BANKER, Oct. 13, 1999, at 1.

123. For descriptions of the final negotiations, see Daniel J. Parks, *Financial Services Bill In the Final Stretch*, CQ WEEKLY, Oct. 23, 1999, at 2498; Kathleen Day, *Banking Accord Likely to Be Law*, WASH. POST, Oct. 23, 1999, at A1.



E. DEVELOPMENTS SINCE 1999

At the signing of GLB, President Clinton called on the Treasury Department, the National Economic Council, and the Office of Management and Budget to prepare new legislation to complete the financial privacy protections begun in GLB. President Clinton proposed the Consumer Financial Privacy Act (CFPA) in April.[125] With financial modernization now enacted, the CFPA gave the Administration an opportunity to present its views about how to protect financial privacy while gaining the benefits of technology, competition, and innovation in financial services.[126] Among other provisions, the CFPA called for an opt-out for affiliate sharing. It required an opt-in for sharing of medical information within a financial holding company. It also required an opt-in for transfer of the "personal spending habits" of individuals, essentially the list of every purchase made by an individual through a checking account, credit card, or similar instrument.

Proposal of the CFPA helped spur legislative activity in 2000 on financial privacy. The House Banking Committee passed a bill that included much of the President's proposed language, but limited to the sharing of medical information within a holding company.[127] In the Sen-

125. *See* Commencement Address at Eastern Michigan University, Ypsilanti, Michigan, I PUB. PAPERS 794, 796 (Apr. 30, 2000) (presenting CFPA), *available at* www.privacy2000.org/archives; *see also* The White House, Office of the Press Secretary, Clinton-Gore Plan to Enhance Consumers' Financial Privacy: Protecting Core Values in the Information Age, Apr. 30, 2000, *available at* www.privacy2000.org/archives; The White House, Office of the Press Secretary, Press Background Briefing by Senior Administration Officials on Financial Privacy, *available at* www.privacy2000.org/archives. The bill was introduced in the House as H.R. 4380 and in the Senate as S. 2513.

126. The Administration position was explained in Testimony of Treasury Under Secretary Gary Gensler before the House Committee on Banking and Financial Services, June 14, 2000, *available at* www.privacy2000.org/archives.

127. See *H.R. 4585 The Medical Financial Privacy Protection Act :Hearing Before*

ate Banking Committee, a coalition of Republican Senator Richard Shelby and committee Democrats created a situation where the committee could act on other matters only if financial privacy amendments were included.[128] Although no financial privacy legislation reached the House or Senate floor in 2000 or 2001, there has been a steady stream of proposed bills. For instance, the new Democratic Chairman of the Senate Banking Committee, Paul Sarbanes, re-introduced the Clinton Administration proposal in 2001 as his proposed basis for additional financial privacy protections.[129]

On the regulatory front, the group of seven regulatory agencies worked under the tight six-month deadline set in GLB to promulgate a proposed and final regulation.[130] The seven regulations were very similar to each other and in general closely tracked the statutory language in GLB. The most controversial aspect of the regulations was the handling of customer lists. After soliciting comments in the proposed rules, the agencies decided that a customer list—the name and address of a customer together with the fact that the individual was the customer of a specific financial institution—should indeed be covered by the opt-out and other provisions of GLB. This agency decision was upheld in court as a valid statutory interpretation.[131] Of perhaps greater long-term significance, the federal courts have upheld the interpretation against First Amendment challenge, holding that there was no impermissible limit on speech created by the statutory opt-out requirement.[132]

Perhaps the other most important developments for financial privacy have come at the state level. Vermont, Connecticut, and Alaska had opt-in laws before 1999,[133] and numerous similar bills were introduced in other states in 2000 and 2001.[134] Most prominently, a sweeping financial

128. Information on file with author.

Markey. Freedom from Behavioral Profiling Act of 2000, S. 536, 107th Cong. (2001); Consumer's Right to Financial Privacy Act, H.R. 2720, 107th Cong. (2001).

130. The seven agencies are the Federal Deposit Insurance Corporation, Federal Reserve Board, the Federal Trade Commission, the National Credit Union Agency, the Office of Comptroller of the Currency, and the Securities and Exchange Commission. State insurance regulators have been in the process of implementing the model rule issued by the National Association of Insurance Commissioners.

131. Indiv. Reference Serv. Group, Inc. v. FTC, 145 F.Supp.2d 6 (D.D.C. 2001).

132. *Id*.

133. Sarah MacDonald, *Vermont's Tough Opt-In Privacy Law Could Be Model for Other States*, AM. BANKER, July 6, 2000, at 1.

134. See the survey of proposed state laws in the annual survey by the Privacy & In-

privacy bill came close to passage in California.[135] Privacy advocates have praised these state initiatives as an important way to raise the privacy standards in the financial services sector. Industry has expressed concern about the need to defend against legislative initiatives in the fifty states, and has increasingly called for federal preemption of stricter state laws. The Clinton Administration position, for both financial and medical privacy, was that it may be appropriate to have federal preemption, but only if sufficiently strict standards were established at the federal level.

III. SHARING WITH THIRD PARTIES AND AFFILIATES

With the foregoing history in mind, we are prepared to look at the contentious issue of when consumers should have a choice before their financial data is shared with other organizations. Part III of this Article first looks at the "formal" and "functional" approaches a regulatory system can take toward this issue. It then examines the joint marketing exception under FLB, which too often allows sharing with outside entities without consumer choice. It concludes by suggesting options for how to create appropriate rules to govern sharing of data with affiliated companies.

A. FORMAL AND FUNCTIONAL APPROACHES FOR DEFINING SECONDARY USE

Under the fair information practices discussed in Part I, a key issue is how to create an administrable regulatory system that defines the permissible purposes for sharing of personal data. One approach is functional—define in the regulations which purposes are compatible. The other basic approach is formal—define some legal boundary within which use is permitted but beyond which choice is required. Title V of GLB largely adopted the latter approach, although the analysis here suggests that a more functional approach may instead be appropriate.

In implementing a formal approach, the GLB debates focused on three possibilities. The first possibility was to require choice for affiliate sharing. Privacy advocates and the Clinton Administration proposed that information could be used within one corporation, such as a bank, but choice would be requested upon transfer to a separate corporation, in-

formation Law Report.

135. *Financial Institutions: Strict Privacy Bill Fails in California; Predatory Lending Legislation Gains Approval*, BANKING DAILY (BNA), Sept. 21, 2001, *at* http://www.bna.com.

cluding affiliates of the bank.[136] The second possibility, partly implemented by GLB, was that information could be used within a financial holding company, but choice would be required upon transfer to a non-affiliated corporation (a "third party"). The third possibility, supported by those opposed to privacy regulation, was to allow transfers to third parties without any choice requirement.

The case for the formal approach is strongest if two conditions are met. The first condition is that the formal boundary is well defined, so that regulators and regulated companies can agree when compliance is required. A well-defined boundary will reduce regulatory costs and promote certainty. At least in many instances, the formal boundaries adopted for financial privacy satisfy this condition. It is generally straightforward to determine when data moves from one corporation to another. The regulatory system has reasons to define and police this boundary, such as where the Office of the Comptroller of the Currency's supervision of a national bank ends and the Federal Reserve's supervision of a state bank begins. It is similarly straightforward in most instances to determine whether a company is an affiliate of a financial institution or else an unaffiliated third party. The Federal Reserve has extensive experience in administering when a holding company "controls" a corporation so that the corporation is considered part of the holding company.[137]

A formal approach is also desirable to the extent that the formal boundary is a good proxy for the underlying purposes of the regulation. To illustrate, suppose that all transfers within a bank were considered a primary use, and all transfers to other corporations were considered secondary uses. If this were true, then the corporate boundary would be an ideal proxy for defining uses that are compatible with the original use. On the other hand, one might find that many uses within a bank were unrelated to the original purposes of processing, while many transfers to other companies were in fact compatible with the original purposes. If the true state of affairs resembles this latter scenario, then the corporate boundary would be a bad approximation of when the individual should have a choice about new uses of the data.

136. Privacy advocates generally supported having opt-in for transfers to affiliates and third parties, while the Clinton Administration supported an opt-out choice.

137. The statute, 12 U.S.C. § 1841(a), provides three conditions for testing control over a bank: (1) owning, controlling, or having the power to vote 25 percent of any class of voting securities; (2) controlling the election of a majority of the board of directors; and (3) exercising a direct or indirect controlling influence over the institutions management policies.

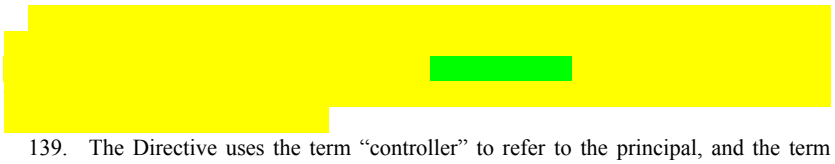
The benefits of formal boundaries—transfers to a separate corporation or an unaffiliated third party—will thus largely depend on whether the formal boundaries accurately distinguish between primary and secondary uses. To the extent that the boundaries do not supply an accurate distinction, then it becomes more important to explore the possibility of a functional approach, where the regulatory attention more explicitly addresses whether a particular use is compatible with the original use of the data or is otherwise desirable.

B. THE JOINT MARKETING EXCEPTION

GLB embodies the basic principle that transfers to unaffiliated third parties constitute secondary use. Choice should be required before such transfers are made. I believe that this principle makes sense and that transfers to third parties violate most consumers' expectations. Customers of a bank don't expect the details of their transactions to be made available to their employers, neighbors, or business competitors. They don't expect outside companies to get detailed information about their financial activities or purchasing habits. For data this detailed and sensitive, it makes sense to have legal guarantees that those outside of the bank's corporate family do not have access to the data unless the customer has at least had a chance to say no.

1. Defining the Scope of the Problem

Some transfers to unaffiliated third parties are sensible and are properly part of GLB. For instance, Section 502(b)(2) contains a provision that allows a financial institution to act as principal and have another company act as its agent "to perform services for or function[] on behalf of the financial institution, including marketing of the financial institution's own products or services."[138] Solid efficiency reasons support this rule. A principal should be able to choose whether to hire employees or an independent contractor to do a task, such as print checks for a bank. Otherwise, the privacy rules could distort economic decisions about how to structure the business. If a bank could not hire an independent contractor, for instance, it might have to create an inefficient in-house check printing capability. This sort of permission to hire independent contractors is a standard feature of data protection laws, including the European Union Data Protection Directive.[139] The accompanying safeguards, un-



139. The Directive uses the term "controller" to refer to the principal, and the term

der both GLB and the Directive, are that the agent should act on behalf of the principal and the agent should assure the confidentiality of data it receives.[140]

Another part of Section 502(b)(2), though, contains language that permits a large amount of secondary use. The "joint marketing exception" allows an unaffiliated third party to receive data from one or more financial institutions and use the data for its own marketing purposes.[141] The statute provides only limited safeguards. The third party must be a "financial institution," although the scope of activities that can qualify as "financial" is very broad under the new law.[142] There must be notice to customers that such transfers may occur, and the third party must contractually promise to maintain the confidentiality of such information.[143]

One objectionable aspect of the joint marketing exception is that it was passed as a "bait and switch"—sold as one thing but in fact another. Essentially, the exception was justified as a way to solve certain problems for small banks. In practice, the exception has become a much broader tool, used intensively by the largest financial institutions. Based on press reports and my own participation in the legislative process in 1999, the joint marketing exception was primarily discussed in a single context. A large bank, such as Citibank, might offer a wide array of products with the Citi label. The products are often supplied by affiliated companies—insurance from one affiliate, mutual funds from another, and other products from dozens or hundreds of other affiliates. Customers of Citibank might see the "Citi" label on this range of products and never even realize that the products were coming from separate, affiliated corporations.

"processor" to refer to the agent. Article 16 of the Directive states that the processor "must not process [personal data] except on instructions from the controller." Article 17 sets forth related requirements, such as that a processor have a written contract and that the processor "shall act only on instructions from the controller."

140. *Id.* For principal/agent relationships under section 502(b)(2), the services performed by the agent are "on behalf of" the principal, the financial institution "fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information."

141. The statute allows sharing of data for "financial products or services offered pursuant to joint agreements between two or more financial institutions . . . ." 15 U.S.C. § 6802(b)(2). The financial institution that receives the data must itself comply with the GLB privacy requirements. *Id.*

142. Under the new law, a financial holding company may engage in any activity that is determined to be "financial in nature or incidental to such financial activity." GLB, Pub. L. 106-102, § 103(a), 113 Stat. 1342-43 (as codified at 12 U.S.C. § 1843(k)(1)(A)). It may also engage in additional activities that are "complementary to a financial activity" where there is no substantial risk to safety and soundness. 12 U.S.C. § 1843(k)(1)(B).

143. 15 U.S.C. § 6802(b)(2).

The business practices of small financial institutions, however, are often different. The Smallville National Bank might also offer its customers a range of products with the "Smallville" label. The difference is that the insurance might be underwritten by a non-affiliated outside company, and the mutual funds might be sold and managed by a different outside company. Direct marketing might come directly from the insurance or mutual fund company, using the Smallville Bank's customer list. Sales might also be made in the bank branch, with the customer representative offering the outside companies' products with the Smallville label. When customers received the solicitation, they would be reassured by the Smallville Bank's name on the product, and the Smallville Bank would build goodwill with the customer. In the absence of such an arrangement, the Smallville Bank would face the risk of turning its customers over to large and potentially full-service competitors, and so might decide not to offer the products at all.

Looking to the legislative history, the joint marketing exception did not exist when the House of Representatives passed its bill in June 1999.[144] Opt-out was required for third parties, but no opt-out applied to affiliates. As one lobbyist explained at the time: "If you're a Citigroup, which has everything under one umbrella, you can share that information and market to your customer without giving an opt-out."[145] Under the House bill, though, "small banks and thrifts that want to achieve synergies with outside insurance or securities firms [would] have to notify their customers and let them block any information sharing."[146] The joint marketing provision was added in negotiations between the House and Senate. When the provision was approved, press reports underscored that it was intended to help small banks, allowing them to offer services on a par with large banks.[147]

Today, the joint marketing provision is used far beyond the small banks. Industry giants such as Chase include joint marketing notices in their privacy policies.[148] A study by the Center for Democracy and

144. See H.R. 10, 106th Cong. (1999).

145. Scott Barancik, *In the House, Banks Dodge Bullet on Privacy Limits*, AM. BANKER, June 28, 1999, at 1 (quoting unidentified lobbyist).

146. *Id*.

147. Dean Anason, *GOP Reform Compromise Draws New Veto Threat*, AM. BANKER, Oct. 13, 1999, at 1 ("Broadening exceptions to help small banks, financial institutions that have joint marketing agreements with nonbanks would not have to give customers an opt-out option."); *see also*

148. *See* CHASE, CHASE PRIVACY POLICY (2002), at http://www.chase.com (last visited Mar. 8, 2002)).

Technology in the summer of 2000 surveyed 100 top on-line financial institutions. Forty-four of the institutions said they did not share information with outside parties as defined by GLB, and thus did not offer any GLB opt-out. Yet two-third of these (30) gave notice that they reserved the right to share information with joint marketing partners.[149]

The credit card issued for the Target retail stores illustrates the deployment of the joint marketing provision by large companies as well as the large range of secondary uses permitted under that provision.[150] In the joint marketing part of the privacy policy, the bank that issues the credit card says "[w]e may partner with other [financial institutions] . . . to market products or services jointly. We may need to share the following information: Identification and contact information (for example, your name, address, and telephone number). Account transaction and experience information (for example, your balance, purchase, and payment history)."[151]

This privacy policy illustrates a two-way street for retailing and financial information. Under this policy, outside financial companies can apparently receive full details about what an individual has purchased at Target and its affiliated operations such as Marshall Fields, catalog operations, and web sites.[152] Similarly, outside financial institutions can provide detailed information to Target. For instance, an outside bank or credit card company could provide a list of every check or credit card purchase an individual had made in the past year, in order to assist Target in targeting that customer for retail sales. Under this policy, a retail use readily can become a use in a traditional financial setting such as a bank or insurance company. A financial use, such as operating a credit card or making a loan, can readily become a use in a retail setting on-line, through a catalogue or in a physical store. Secondary uses abound.[153]

The Target example suggests the weakness of the statutory safeguards built into the joint marketing exception. First, the requirement that

149. CENTER FOR DEMOCRACY & TECHNOLOGY, ONLINE BANKING PRIVACY: A SLOW, CONFUSING START TO GIVING CUSTOMERS CONTROL OVER THEIR INFORMATION 2 (2000), *available at* http://www.cdt.org (Aug. 29, 2001).

150. *See* RETAILERS NATIONAL BANK, RETALIERS NATIONAL BANK PRIVACY POLICY (2002), *at* http://www.target.com/common/financialservices/retailers_national_bank_privacy_policy.jhtr (last visited Mar. 8, 2002).

151. *Id*.

152. The policy of the Retailers National Bank, which issues the credit card, lists retail companies such as Target, Marshall Field's, and Mervyn's. It lists web sites including target.direct and associated sites. It lists catalogs such as Signals, Wireless, and Seasons, and associated web sites. *Id*.

153. For a detailed examination of how GLB governs co-branding and similar arrangements

the sharing be with a "financial institution" does not keep the data within a tight orbit of activities that an ordinary person would think of as "financial" in nature. GLB's broad definition of financial institution means that even activities that are "incidental" or "complementary" to a financial activity can be carried out by a financial institution.[154] Second, the notice requirement is vague and gives customers little information about the scope or type of the data sharing. Joint marketing disclosures typically do not list the quantity or names of the marketing partners. They often include comforting language that states that data will only be shared with carefully selected partners, but this language likely creates few or no legal limits on where the data can go.[155] Third, the quality of the required confidentiality contracts is suspect. The chief problem is that the marketing partner, who receives the data for joint marketing purposes, can then re-use the same data for any other purpose. The joint marketing partner is not limited to acting as an agent, on behalf of the principal that discloses the data.[156] The problem of having the recipient act as a principal is compounded by GLB Section 502(c), which is entitled "Limits on re-use of information." As actually written, Section 502(c) governs only subsequent *disclosures* to additional companies, and does not place any limits on subsequent uses of the data by a company that has already received the data.[157]

2. Responses to the joint marketing issue

In light of the weak existing safeguards under the joint marketing exception, new legislation should eliminate the exception or reduce its

154. 12 U.S.C. 1843(k) (2000). Most of these non-traditional "financial institutions" are regulated by the Federal Trade Commission. For regulations defining the scope of that term, *see supra* note 32.

155. For instance, the Target policy says: "We carefully select [our financial institution partners] to be sure they have procedures in place to protect your privacy." RETAILERS NATIONAL BANK, *supra* note 150 . This language would apparently support selection of a large number of partners, and proving a violation of this "careful selection" language would be highly difficult.

156. As discussed, *supra*, text accompanying note 140, an agent can receive data and act "on behalf of" a principal. GLB 502(b)(2), 113 Stat. at 1338, 1437. The "on behalf of" requirement does not apply to joint marketing partners, who can use the data they receive on their own behalf. *Id*.

157. Section 502(c) provides:

> Except as otherwise provided in this subtitle, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.

GLB § 502(c), 113 Stat. at 1437.

scope considerably. I will discuss eliminating the exception and then discuss an alternative that allows joint marketing to continue only for small financial institutions.

The Consumer Financial Privacy Act of 2000 proposed eliminating the exception entirely.[158] The CFPA retained the ability to use third parties as agents who act on behalf of a principal, and it retained the other GLB exceptions that allow transfers of data that are necessary to complete a transaction and for other priority uses.[159] I believe there is a strong case for adopting this position and eliminating the exception. Customers of one financial institution do not and should not expect that their personal data will be transferred to any other financial institution in the economy, with no choice in the matter. The ability of the recipient institution to re-use the data for any purpose means that current law permits too wide a range of secondary uses. The problem of secondary uses is made worse by the sensitive nature of much of the data held by financial institutions and shared under the joint marketing exception.

In assessing the effects of eliminating the exception, it is important to note that marketing might still be conducted on behalf of the marketing partner. Unless there were some additional legal provision that prohibited it, the original financial institution could send out marketing materials on behalf of the outside marketing partner. For instance, a bank could send out marketing materials on behalf of an outside firm, but the outside firm would not receive any personal information from the bank.[160] The outside firm would not receive any personal data except after a choice by the customer. The choice would be either a GLB opt-out for transfers to third parties, or after the customer has decided to initiate a transaction with the marketing partner.

This approach allows marketing *for* a third party but not *by* a third party. It has the significant privacy advantage of preventing the data from flowing to a third party, with all of the attendant regulatory challenges of tracing how the data is used or disclosed once it has left the original financial institution. It has the privacy disadvantage of permitting customers to be solicited by their own financial institutions on behalf of any outside party. To the extent one is concerned about this disadvan-

158. *See* Office of the Press Secretary, White House, Clinton-Gore Plan to Enhance Consumers' Financial Privacy: Protecting Core Values in the Information Age, (Apr. 30, 2000), *available at* www.privacy2000.org/archives (last visited Mar. 8, 2002) ("The plan also closes an unnecessary exception for 'joint marketing' from last year's bill.").

159. *See* H.R. 4380, 106th Cong (2000).

160. The data may be transferred to companies, such as companies specializing in direct mailing, who actually send out the materials. These companies, however, would be agents of the original financial institution. They would be permitted to use the data only "on behalf of" the institution, and not for their own purposes.

tage, one can define the circumstances in which marketing for the third party is allowed. These sorts of definitions exist, for instance, in the medical privacy rule that the Department of Health and Human Services issued in final form in 2000. Under that rule, for instance, a marketing communication must identify a hospital or other covered entity as the party making the communication, prominently disclose if the covered entity has received remuneration for making the communication, and offer an opt-out for future communications.[161] Although some privacy advocates have criticized these marketing provisions,[162] my own view is that this approach is sensible. An organization can contact its own customers, but if it conducts marketing on behalf of an outside firm, then the organization has to identify itself and take responsibility for any ill-will generated by the unsolicited marketing effort. Offers that are genuinely in the interest of the customer will proceed, while offers seen by many customers as annoyances will trace back to the financial institution that conducts the marketing.

Based on my work in the financial privacy area, including extensive discussions with stakeholders including industry and privacy groups, I would support eliminating the joint marketing exception. I would also seriously explore drafting a marketing provision analogous to that existing for medical privacy, so that marketing conducted for a third party could proceed only where the original financial institution clearly identified itself and took responsibility for making the marketing offer.

As an alternative, Congress could retain the joint marketing provision but strictly limit its use to its original justification. As discussed above, the provision was justified during the 1999 legislative debates as a mechanism for giving small financial institutions parity with large institutions. The logical legislative response to this concern would be to design the joint marketing provision to apply specifically to small financial institutions. For banks and other traditional financial institutions, there are numerous precedents for varying the regulatory regime depending on the size of the institution, such as the amount of assets held by a bank.[163]

161. "Marketing" is defined at Section 164.501 of the medical privacy rule. Section 164.514(e) sets forth these and other requirements that accompany marketing. For instance, if the covered entity targets a communication based on health status or condition, the communication must explain why the individual has been targeted and how the product or service relates to the health of the individual. Section 164.514(e)(3)(ii).

162. *See, e.g.*, Robert O'Harrow, Jr., *Patient Files Opened to Marketers, Fundraisers; Critics Decry Exemptions Won Through Lobbying*, WASH. POST, Jan. 16, 2001, at E1 (quoting Robert Gellman and others criticizing the medical privacy marketing provisions).

163. See, e.g., 12 C.F.R. Ch. III, Part 363.1 (2001) (annual independent audits and

Congress might set size limits itself, or delegate the task to the relevant regulatory agencies.

As a public policy matter, I am agnostic about the extent to which a small-institution exception is appropriate.[164] Small institutions may indeed rely more heavily on joint marketing arrangements than large institutions which have affiliates, although I am not aware of any empirical support for this claim. In general, small databases likely pose fewer privacy risks than very large databases, so the privacy harm from a small-institution exception may be modest.[165] Whatever the need for a small-institution provision, concern about small institutions needing parity is simply no argument for the current wide-open exception used by the largest financial institutions.

C. AFFILIATE SHARING

A major disagreement in passage of GLB in 1999 and consideration of financial privacy legislation in 2000 was whether there should be an opt-out before data goes to affiliated institutions.

1. Defining the Scope of the Problem

The number of affiliates in financial services is very high. Decades of regulation meant that there were multiple and compelling reasons for holding companies to create numerous subsidiaries. Geographic restrictions meant that banks typically could not branch across state lines, and sometimes not even across county lines.[166] A holding company would

For a critique of many previous attempts to provide exemptions based on the small size of a business, see Richard J. Pierce, Jr., *Small is Not Beautiful: The Case Against Special Regulatory Treatment of Small Firms*, 50 ADMIN. L. REV. 537 (1998). A joint marketing exception that applied only to small financial institutions might be more justifiable than the small-business exceptions criticized by Professor Pierce because the rationale for the exception is based precisely on the different way that small institutions conduct their business, rather than on alleged greater regulatory burdens suffered by small institutions.

164. As a political matter, it is far easier for legislators to support a provision that helps small banks compete effectively rather than a provision that is known to allow the largest conglomerates to share sensitive data freely.

165. For small databases, for instance, it is less likely to be cost effective to buy expensive data mining software for the smaller number of records. Those seeking information are also more likely to turn first to large databases that offer the possibility of comprehensive, one-stop information.

166. For an analysis of the law that historically applied to geographic expansion of banking, see LISSA L. BROOME & JERRY W. MARKHAM, REGULATION OF BANK FINANCIAL SERVICE ACTIVITIES 591-625 (2001).

own separate banks for separate geographic areas. Related lines of business, such as specialized lending subsidiaries, would be created in additional corporations when geographic limits did not apply to that line of business.[167] Service corporations, such as those providing specialized computer services, would support many different affiliates. Special statutes meant that banking, insurance, and securities usually could not be done in the same corporation, even when pieces of the same holding company could offer the services.[168] Other regulatory and tax provisions gave additional reasons to house different activities in separate, affiliated corporations.[169]

Many of the geographic and line-of-business restrictions eroded over time. Banks gained the full power to branch nationwide in 1994.[170] Securities activities were increasingly allowed in a bank holding company after regulatory changes in the late 1980s.[171] By the 1990s banks increasingly gained the power to offer insurance or insurance-like products, such as annuities.[172] By the time GLB was debated in 1999, it was roughly accurate to say that banking organizations could engage in all financial activities, but they had to undertake complex regulatory machinations to do so. For supporters of financial modernization, this complexity raised the cost of entering new businesses, and meant that transactions were too often driven by regulatory peculiarities rather than the economic efficiency.[173]

For supporters of financial modernization, a great advantage of GLB

167. See the discussion of the development of interstate banking in JONATHAN R. MACEY, GEOFFREY P. MILLER & RICHARD S. CARNELL, BANKING LAW AND REGULATION 32-33 (3d ed. 2001).

168. For instance, bank holding companies were required to form affiliates outside of the bank when they gained new powers to underwrite securities. Sec. Indus. Ass'n. v. Bd. of Governors of the Fed. Reserve Sys., 807 F.2d 1052 (D.C. Cir. 1986), *cert. denied,* 483 U.S. 1005 (1987).

169. For instance, national banks were allowed to charge higher interest rates, notwithstanding the usury laws of a customer's state, when loans were made from outside of that state. Marquette Nat'l Bank of Minneapolis v. First of Omaha Serv. Corp., 439 U.S. 299 (1978).

170. The prohibition on inter-state banking was repealed in the Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994, Pub. L. No. 103-328, 108 Stat. 2338 (1994).

171. *See Sec. Indus. Ass'n*, 807 F.2d at 1058-59.

172. *See* Nationsbank of N. C., N.A. v. Variable Annuity Life Ins. Co., 513 U.S. 251, 257-58 (1995) (upholding national bank authority to offer annuities).

173. *See generally* Arthur E. Wilmarth Jr., *The Transformation of the U.S. Financial*

GLB on safety and soundness, with special attention to the risks created by combination of previously-separate lines of financial activity).

was that it would spur a rationalization of the crazy-quilt structure of affiliates. The legacy of costly corporate separation would evolve into corporate structures that were based on market decisions about when to have separate affiliates. This rationalization would proceed gradually. In the early stages, new affiliates would start to coordinate their activities more closely. Over time, where the economic logic was strong, affiliates would merge together. Consumers, recognizing this trend, would expect information sharing among affiliates.[174]

Given this history, one can construct a plausible case for at least a good deal of sharing of personal information among affiliates. For affiliates that are on the road to a merger, sharing of data is a logical step toward eventual combined operations. More broadly, GLB offers the opportunity for banking, insurance, and securities activities to be marketed in a unified manner even where no merger is ultimately planned. For customers who want "one-stop shopping" for their financial services, the post-GLB holding company can offer a comprehensive package. The seller can suggest just the product that the customer may need to construct a personal financial plan. Indeed, some industry leaders went so far as to say that the principal point of GLB was to facilitate this sort of cross-marketing.[175]

---

174. Representative Oxley, a proponent of affiliate sharing, said that, "the integrated products and services today's consumer expects from his or her financial institutions require information sharing, especially among affiliates. After all, in the eyes of the consumer, what are affiliates other than different departments of the same company that they are dealing with." 145 CONG REC. H5310 (daily ed. July 1, 1999) (statement of Rep. Oxley).

175. For instance, Marcia Sullivan, a leading industry spokesperson on privacy issues, was reported as saying that "[o]verly strict privacy rules could even undermine the fundamental purpose of financial reform, which is to promote joint ventures, cross-marketing, and economic efficiencies." Scott Barancik, *House Privacy Hearing to Pit Banks Against White House*, AM. BANKER, July 20, 1999, at 2.

Jonathan Macey suggests a basis for affiliate sharing based on public choice theory rather than public policy:

> A more plausible explanation for the way that privacy issues are treated in the statute is that banks, insurance companies, and securities firms doing business (or anticipating doing business) in financial services holding companies are far more politically powerful than the finance companies, regional financial intermediaries, and others expected to remain independent after the statute was passed.

Jonathan R. Macey, *The Business of Banking: Before and After Gramm-Leach-Bliley*, J. CORP. LAW, 691, 714 (2000). The interest groups that Professor Macey mentions certainly played an enormous role in shaping GLB. At the same time, a public choice approach would not have been very helpful in predicting the precise outcome of privacy rules, which shifted repeatedly as the bill progressed through Congress, and with the Clinton Administration and privacy advocates as significant participants that Professor Macey does not mention. A public choice analysis, for instance, would find it difficult or impossible to account for the sudden swing in the House Commerce Committee to far greater

This regulatory history helps one better appreciate the fervor of the debate in GLB over affiliate sharing of personal information. From the industry side, a great deal of affiliate sharing was essential in order to rationalize operations and marketing in financial services. From the side of the privacy advocates, there were intense concerns about the agglomeration of previously separate databases from the banking, insurance, securities, and other industries. Ralph Nader, for instance, said: "The privacy protections that emerged in the banking reform legislation are a joke that will simply delude the public into believing privacy provisions exist where there are none."[176] He focused his concern on sharing across databases: "[T]he affiliates of the conglomerates and their telemarketers will be free to share many intimate details of an individual's buying habits, investing patterns, health records, entertainment choices, employment data and other aspects of one's existence."[177]

The Clinton Administration also expressed serious concerns about allowing unfettered sharing of personal data with affiliates. In contrast to the privacy advocates, the Clinton Administration supported the general project of allowing banking, securities, and the other lines of business to exist within a single holding company.[178] Together with the privacy advocates, however, the Administration believed that unfettered sharing of information with affiliates constituted a secondary use. During both the 1999 GLB debates and in its 2000 legislative proposal, the Administration supported having an opt-out choice for sharing with affiliates.[179]

The case for having an opt-out choice is strongest where the secondary use is very different from the primary use. In proposing stricter legislation in 2000, President Clinton gave examples:

---

privacy restrictions, including on affiliates, than favored by the industry groups that Professor Macey correctly describes as powerful. The approach taken in this article, rather than seeking to predict future developments as a matter of public choice theory, is to assess what privacy rules would be desirable.

175. Ralph Nader, *Banking Jackpot*, WASH. POST, Nov. 5, 1999, at A33.

176. *Id.*

178. For instance, the White House press statement accompanying the signing of GLB began by saying: "President Clinton today will sign historic legislation to modernize our banking and finance laws. For the first time, financial firms will be able to offer a full range of banking, securities, and insurance products, stimulating greater innovation and competition." Press Release, Office of the Press Secretary, The White House Financial Services Modernization for the 21st Century: Lowering Consumer Costs, Building Communities, and Boosting Competitiveness (Nov. 12, 1999), *available at* http://www.privacy2000.org/archives (last visited Mar. 8, 2002).

179. In signing GLB, President Clinton said: "Without restraining the economic potential of new business arrangements, I want to make sure every family has meaningful choices about how their personal information will be shared within corporate conglomerates. We can't allow new opportunities to erode old and fundamental rights." President Bill Clinton, Remarks by the President at Financial Modernization Bill Signing, (Nov. 12, 1999), *available at* http://www.privacy2000.org/archives (last visited Mar. 8, 2002).

> [T]he life insurance company could share information about your medical history with the bank without giving you any choice in the matter. The bank could share information from your student loans and your credit cards with its telemarketer, or its broker, again, without giving you any choice. I believe that is wrong.[180]

As another example, consider whether a travel agency should be able to look through all the checks you wrote in the past year in order to assess what sort of vacations you might like. With the passage of GLB, these insurance companies, banks, telemarketers, brokers, travel agents, and others could easily be within the same financial holding company, under the broad terms of what is "incidental" or "complementary" to financial activities.[181]

2. Responses to Affiliate Sharing

The affiliate sharing issue is difficult because the arguments on both sides are so compelling. From the privacy side, the examples show the remarkable range of secondary uses permitted under GLB. The Clinton Administration believed that these secondary uses violated consumers' reasonable expectations, and consumer choice was therefore appropriate before the information went to the different affiliate. From the industry side, a major achievement of GLB was to allow integrated operations for all types of financial services. Creating barriers to information sharing could severely undermine that achievement.

As a discussed above, there are two basic ways that one could limit affiliate sharing. The formal approach would focus on corporate separateness, with use within a corporation permitted, but transfers to different corporations including affiliates only done with consumer choice. This corporate separateness approach exists in GLB today, where transfers to unaffiliated corporations require an opt-out but transfers within a holding company do not. Second, one the functional approach would permit data flows for some functions but require consumer choice for others. The functional approach also plays a role in GLB today, with the 502(e) exceptions permitting transfers to outside parties for purposes such as law enforcement, fraud prevention, and so forth. Transfers are also permitted, without consent, to those acting as agents for the financial institution. As shown by GLB today, the formal and functional approaches can be used together, with transfers across corporate boundaries usually requiring consumer choice but with designated exceptions where

180. President Bill Clinton, Remarks by the President at Eastern Michigan University Commencement, (Apr. 30, 2000), *available at* http:// www.privacy2000.org/archives (last visited Mar. 8, 2002).

181. 12 U.S.C. 1843(k) (2000).

choice is not required.

The Consumer Financial Privacy Act, proposed by the Clinton Administration in 2000, proposed what I believe is an attractive blend of the two approaches. Its basic rule is formal—sharing of data with affiliates requires a customer opt-out choice. This rule is supplemented with the existing functional exceptions to GLB, such as law enforcement, fraud prevention, and sharing with agents subject to a confidentiality contract. The rule is also supplemented by a new proposed provision for sharing with affiliates. This provision would allow sharing in order to facilitate customer service, such as maintenance and operation of consolidated customer call centers or the use of consolidated customer account statements.[182] The provision was developed after consultation with industry and consumer groups, and was based on a belief that consumers would generally prefer a call center or other customer service operation to be able to provide information and carry out transactions for all of the customers' transactions with the holding company. Otherwise, a customer with a checking account, mutual fund, and investment account might feel coerced to consent to unlimited information sharing within the holding company simply in order to gain the ability to have a single customer service representative who could see all three accounts.

The CFPA also recognizes that stricter rules on information sharing are appropriate for especially sensitive categories of information. The bill proposes opt-in consent and other protections against the inappropriate sharing of medical data within a holding company.[183] The bill also restricts the transfer of information about personal spending habits. For checking, credit card, and similar instruments, a financial institution would not be able to transfer to another company "an individualized list of that consumer's transactions or an individualized description of that consumer's interests, preferences, or other characteristics."[184] To the extent that financial holding companies contain personal information with varying levels of sensitivity, distinct rules can thus govern what data is shared with affiliates and outside companies.

---

181. H.R. 4380, *supra* note ___, at § 10.

nation of all applicants, but banks would be unlikely to risk the wrath of customers before asking for the medical data of mortgage applicants.

183. *Id*. at § 3.

Instead of relying so much on formal corporate separateness, one can also imagine a more thoroughly functional approach to governing sharing of data with affiliates. Even the strictest data privacy regimes recognize that data can be used for the purposes for which it was collected. When it comes to a checking account, for instance, a bank will use personal data in a variety of ways when completing transactions, auditing its own books, and sending customer statements. The tricky issue is how far to construe these primary purposes. In American practice, I suggest, consumers would generally expect that the data would be used in the same "line of business." The monthly statement for a checking account, for instance, might include a solicitation for other banking products such as credit cards or certificate of deposit.

If there is agreement that data can be shared within the same "line of business," the next question is whether there are sensible extensions of that idea that correspond to consumer expectations and industry structure. For instance, my impression is that many Americans would not be surprised or unduly disturbed if the fact that they were a customer of a bank was made available to the affiliated insurance, mutual fund, securities broker, or other companies that might be called "core financial services." Concerns about sharing financial information with these core financial services affiliates are relatively low. ustomers may prefer to receive a consolidated statement for banking, mutual fund, securities, and insurance accounts. By contrast, concerns are greater when the sharing is done with affiliates that are not providing what I am calling "core financial services." If Target, Marshall Fields, a travel agency, or other seemingly non-financial enterprises receive the data, customers may understandably expect to have a choice before there is disclosure and secondary use.

I believe there is a reasonably strong case to be made for considering this "core financial services" approach. The advantage is that opt-in or opt-out would not be required when sharing occurs among the core financial services. The integration of consumer banking, insurance, and securities products can continue without the need to get a new opt-out for each transfer across corporate boundaries. As a correlate, an opt-out would be appropriate for transfers to affiliates that are not core financial services. Transfer to the travel agency or retail store should be considered secondary use, subject to consumer choice.

In suggesting this approach, I would like to address two potential objections. First is the question of administrability. How easy will it be to draw the line between core and peripheral financial services? For the industry, the answer may be that it would be easier to draw such a line than to have to re-separate the banking, insurance, and securities activities. For regulators, there would indeed be a line-drawing challenge over

time, although a large portion of actual consumer activities likely falls pretty clearly on one side of the line or the other.[185] Mutual funds are "core." Travel agencies are not.

The second, related objection is that the entire effort to pass Gramm-Leach-Bliley was precisely to get away from regulatory line drawing among different types of financial institutions. Untold effort was spent, for instance, deciding whether a bank's activities were impermissible "securities" or "insurance" activities. For weary veterans of these debates, it may seem bizarre to start a new regulatory effort based on distinguishing "core" from "peripheral" activities, with free information sharing only among the former.

In response, I submit that the core/peripheral distinction avoids a key flaw of the pre-GLB regime. Under the old Glass-Steagall approach, the regulatory categories meant the difference between being able to enter a line of business or not. Companies were simply prohibited from doing certain activities if the wrong label—"securities" or "banking"—was applied. Investment in different sectors was distorted by these yes/no decisions on where activities could take place. By contrast, the core/periphery distinction would not determine whether a company could engage in a particular activity. The distinction would have the lesser effect of merely requiring consumer choice before core financial information were shared for peripheral purposes. Where companies believed it was worth entering a line of business subject to this requirement, they could freely do so consistent with the free-investment philosophy of GLB.[186]

To sum up on affiliate sharing, I believe that most consumers find unrestricted sharing among all affiliates to go considerably beyond their reasonable expectations. One way to address the issue is to follow the Consumer Financial Privacy Act, requiring choice before sharing with affiliates, creating appropriate exceptions for customer service and other desirable flows, and providing stronger safeguards for the most sensitive information such as medical records and personal spending habits. Another way to address the issue is to explore a more functional approach, where sharing is allowed within each "line of business" and where greater choice is required when core financial services seek to share in-

186. A related justification for this approach is that it creates less of an incentive to put a wide range of activities into the financial holding company. If the privacy regime favors affiliate sharing over sharing with third parties, then holding companies will have reason to expand the permissible scope of what can be brought within the holding company. On the other hand, if peripheral financial activities are treated the same as third-party activities, this incentive will no longer exist.

formation with peripheral financial services. As financial institutions expand in scope, and the lines blur between financial activities and other activities in the economy, I believe it is not appropriate to assume that every item in a checking account or every balance in a mutual fund should be spread across the innumerable activities that a modern financial holding company is likely to operate. Looking ahead, I believe greater attention should be paid to identifying which data flows are most deserving of regulatory attention, which functional exceptions should be assured, along the lines for instance of the proposed customer service exception, and how to do all of this in a cost-effective way.[187]

IV. NOTICES

The notices to consumers required by GLB have been the target of vigorous attack from both industry and privacy advocates. Industry has complained that the notices impose a high cost for a low benefit. Estimates of the number of notices mailed out in 2001 range from one billion to 2.5 billion.[188] If each notice costs a first-class postage of 33 cents, as some in industry have (perhaps erroneously) assumed,[189] then the annual costs could range from $300 million to over $800 million.[190] What is

187. Concerning cost-effectiveness, my judgment is that a greater time should be allowed for implementation once legislation is enacted. The most effective and least expensive way to change data handling practices is when a system is updated. Instead of the six months given for implementation with the GLB rule, I would favor something on the order of a two year implementation schedule. In this way, industry could comply more cost-effectively, and otherwise-justified complaints about an unrealistic time schedule would have considerably less force in the political process.

188. W.A. Lee, *Opt-Out Notices Give No One a Thrill*, AM. BANKER, July 10, 2001, at 1 (more than a billion notices).

189. Many banks included the privacy notice in customer statements or other mailings, reducing printing and postage costs.

190. Ted Cornwell, *Privacy Regulations Require System Upgrades*, MORTGAGE SERVICING NEWS, Oct. 2000, at 1. Citing an attorney who represents banking industry clients, the article states that the financial services industry will send at least 2.5 billion pieces of mail, with postage of 33 cents each, for a total cost of $825 million.

Another potential cost would be due to the change in the information systems of financial institutions, which now will have to be able to keep track of consumer opt-outs in order to share personal information only where permitted. It is an interesting question how much to count these system changes as a cost of the regulation. If one assumes, as a baseline, that all personal information can be freely shared with all outside parties, then it is a cost of the regulation to place any limits on information sharing. If one assumes, by contrast, that personal information should be sent to outside parties only with the choice of the individual, then the system costs are part of the normal cost of doing business rather than a new cost of the regulation. This question of how to define the baseline is extensively discussed in the cost/benefit analysis for the HIPAA medical privacy regulation. 65 Fed. Reg. 82762 (2000).

gained from all of this paper? The actual number of opt-outs appears to be low, with five percent the most widely used figure but with some estimates of under one percent.[191] From an industry perspective, therefore, the notices can seem like an expensive exercise on an issue that consumers indicate they care little about.

Consumer groups, privacy advocates, and Members of Congress have also harshly criticized the GLB notices. In the summer of 2001, a coalition of groups petitioned the regulators to issue new notice rules, alleging that "most financial institutions have employed dense, misleading statements and confusing, cumbersome procedures to prevent consumers from opting out."[192] Representative John LaFalce, the ranking Democrat on the House Banking Committee, wrote a detailed letter to regulators stating that many of the notices fail to meet the "clear and conspicuous" notice requirement of the statute: "While a number of financial institutions have worked constructively to create effective privacy notices and opt out vehicles, too many others appear to have used the privacy notices to confuse their privacy obligations and engage in inappropriate marketing."[193] Representative LaFalce said the notices "are not readily noticeable among the marketing and promotional materials that consumers frequently ignore in monthly statements."[194] Notices are too long, the language is too complex, and the tone "minimizes the importance of the consumer's opt-out right."[195]

---

191. Marie Harf, *Nader Slams GLB Privacy Compliance*, AM. BANKER, June 22, 2001, at 1 (consumer advocate Ralph Nader discusses five percent reply rate); Lee, *supra* note 188 (five percent "has been circulating as the unofficial industry figure").

A survey by an industry group, America's Community Bankers, reported that about half the thrifts with over $ 1 billion in assets offered the opt-out. (Institutions that do not transfer customer information to non-affiliated third parties do not need to offer the opt-out.) Of these thrifts, 60 percent said that less than one percent of their customers elected to opt out. Rob Blackwell, *Privacy Costs Hitting Small Players Harder*, AM. BANKER, Nov. 21, 2001, at 1. The representativeness of this survey is subject to doubt, however. The response rate to the survey was low, the sample size for the less than one percent finding was small, and it is unknown how clear the notices were or how easy it was for consumers to opt out.

192. Petition for Rulemaking, July 26, 2001, at 2, *available at* http://epic.org/privacy/consumer/glbpetition.pdf (last visited Mar. 13, 2002).

193. Letter from Representative John J. LaFalce et al. to Alan Greenspan, Chairman, Board of Governors of the Federal Reserve System, et al., (June 22, 2001), *available at* http://www.house.gov/banking-democrats/pr_0106letter .htm (last visited Mar. 13, 2002).

194. *Id*.

195. *Id*. Rep. LaFalce discussed a study by the Privacy Rights Clearinghouse that found that the average privacy notice "was written at a third or fourth year college level, well above the junior high school reading level typically considered 'widely understandable' for purposes of government notices and business marketing." *Id*.

A. THE CASE FOR THE CURRENT, FLAWED NOTICES

To a certain extent, the industry and advocate comments about the notices show a predictable taking of positions rather than commentary on actual flaws of the current approach. For instance, industry would likely try to have it both ways when it becomes to discussing the implications of the opt-out rate. With the low current opt-out rate, industry argues that consumers are showing they don't care much about privacy, so there should be minimal privacy regulation. If the opt-out rate had been high, however, then industry would have argued that privacy protections interfered too much with their ability to carry out their business, so that again there should be minimal privacy regulation. This position-taking can occur as well from the privacy advocate side. With the low current opt-out rate, the point is that the notices are badly flawed, so stricter privacy protections are needed. If the opt-out rate had been high, this would have been evidence of how much consumers care about privacy, supporting stricter privacy protections. In short, the evidence on rate of opt out does not do much to sway the views of either side of the debate.

Recognizing the criticisms to date, and the limits of the available evidence, I would like to make the case for a decidedly more optimistic view of the effect of the GLB notices. Even in their current flawed form and even if not a single consumer exercised the opt-out right, I contend that a principal effect of the notices has been to require financial institutions to inspect their own practices. In this respect, the detail and complexity of the GLB notices is actually a virtue. In order to draft the notice, many financial institutions undertook an extensive process, often for the first time, to learn just how data is and is not shared between different parts of the organization and with third parties. Based on my extensive discussions with people in the industry, I believe that many institutions discovered practices that they decided, upon deliberation, to change. One public example of this was the decision of Bank of America no longer to share its customers' data with third parties, even subject to opt-out.[196] The detailed and complex notice, in short, created a more detailed roadmap for privacy compliance.

Related to this process of self-examination, many financial companies put in place new institutional structures for managing privacy and security. The most visible symptom of these changes has been the spread of the "Chief Privacy Officer." The number of CPOs rose rapidly in the immediate aftermath of GLB.[197] Based on my own experience as essen-

196. Michelle Heller, *Cost of Compliance Could Deter Data-Sharing*, AM. BANKER, June 26, 2000, at 1.

197. The Privacy Officers Association was started in early 2000. Mark Taylor, *Privacy Issues are Focus of New Group*, MODERN HEALTHCARE, April 10, 2000, at 42. For general reports of the rise of CPOs, see Michelle Kessler, *Position of 'Privacy Officer'*

tially the CPO for the Federal government,[198] I believe having a person visibly responsible for privacy is a helpful way to ensure that privacy issues are considered in the organization's actions. Privacy concerns may or may not win out in the eventual decisions, but having a person expert in privacy in the process means that the other participants at least have to articulate why the proposed actions are consistent with the organization's announced privacy policies. Even for those financial institutions that chose not to name a CPO, there were often people in the general counsel's office or elsewhere in the organization who gained new responsibilities for creating and implementing privacy policies. The institutionalization of privacy, in short, is perhaps the single most important and least appreciated effect of GLB. The privacy notice to all consumers, coupled with liability for violation of the notice, prompted a larger compliance effort than most observers have realized.

One important and related benefit, I believe, is that GLB substantially reduces the risk of egregious privacy practices by financial institutions. A comparison to environmental regulation illustrates the point. Suppose a new legal regime greatly reduced the likelihood of large toxic waste spills, measured in pounds or tons, but left in place the likelihood of low-level releases, measured in fractions of a pound. Critics of the law might justifiably complain that low-level releases continued. Supporters of the law, however, could say with some confidence that the level of pollution would decline considerably, with a consequent gain for the public health.[199] Supporters would also say that institutional learning

Coming into Public Eye, U.S.A. TODAY, Nov. 30, 2000, at 1B (noting that in the past 2 years the number of companies with CPOs rose from zero to seventy-five), Mary Mosquera, , *IT Companies Go Public About Privacy*, TECHWEB, Dec. 19, 2000, *at* http://content.techweb.com/ wire/story/TWB20001219S0016 (last visited Mar. 16, 2002) (noting companies such as Microsoft, IBM, and AT&T had all recently created the CPO position).

198. My title was "Chief Counselor for Privacy" in the U.S. Office of Management and Budget. At the time we named the new position in early 1999, I had never heard of the term "Chief Privacy Officer," and we did not use that title.

Ray Everett-Church began using the "Chief Privacy Officer" title in Sept.

199. Indeed, there is a considerable literature in the environmental area that suggests that the ratio of benefits to costs is greatest for the first generation of regulation. Mandatory rules often are most justified for behavior that clearly should be prohibited. The likelihood of net benefits declines as prohibitions apply to behavior that is not per se objectionable.

from the first round of legislation might teach valuable lessons for cost-effective efforts in the future to restrict the low-level releases.

I suggest that the environmental analogy is apt. The U.S. Bank case was the equivalent of a large spill, with the detailed records of hundreds of thousands of customers going to a telemarketing company that engaged in apparently deceptive practices, all without any notice to customers. In the wake of GLB, with privacy practices enforceable by law and the new CPO on the scene, is this sort of large spill nearly as likely to occur? The notice alerts employees and customers alike that privacy is part of the responsibility of the financial institution. Disgruntled employees, emboldened perhaps in the post-Enron period, will be able to cause considerable problems if they blow the whistle on unlawful or inappropriate privacy practices. The institution's managers will be educated to avoid the risks of practices that, in the words of Comptroller Jerry Hawke, will appear "seamy" to the regulators, the press, and the public. Bank supervisors will examine for compliance with privacy and security policies. As discussed above in connection with the joint marketing exception and affiliate sharing, I believe GLB allows too many spills of data without customer choice. Nonetheless, these spills occur within a framework that makes large, unregulated transfers to third parties much less likely. Egregious practices become risky for the company, even though less egregious practices continue in violation of what fair information practices would generally contemplate.

B. CREATING BETTER NOTICES

The analysis here suggests a dilemma in drafting GLB privacy policies. Neither a long nor a short notice seems acceptable. The virtues of long and detailed notices are that they have pushed companies to inventory and document their privacy practices, create institutional compliance structures, and avoid egregious practices. The vices of such notices are that ordinary consumers don't understand them—the right to opt out is swathed in folds of obscuring verbiage. On the other hand, a short and plain English notice would have the virtue of communicating more clearly to most consumers. This summary document, however, would be far less effective at prompting self-scrutiny of company practices and would be in such general terms that holding violators accountable would be essentially impossible.

The sensible way out of this dilemma is to have both a short and a long notice, with each used in appropriate circumstances.[200] For com-

tion).

200. As this article was being written, the federal regulators held a workshop in December, 2001 to study GLB notices. Interagency Public Workshop, *Get Noticed: Effective*

munications with consumers, the general approach would be to provide a short, plain English notice. The policy goal here should be to design notices that communicate effectively about privacy choices. Focus groups and other consumer survey techniques can aid in this task. To facilitate comparison shopping, it quite possibly makes sense to have a standardized format, as with nutrition labels.[201]

Institutions should also continue to have a more detailed notice, which sets forth the longer list of facts that are material to understanding and implementing a company's actual privacy policies. The short notice would tell how to access the detailed notice, presumably including a web link , and perhaps with the notice included in Securites and Exchange Commission documents.[202] The detailed notice might roughly correspond to the length of the current notice, although policymakers and financial institutions may wish to add or subtract detail over time. The policy goal here is to have a privacy policy that is detailed enough to ensure self-scrutiny, provide a mechanism for institutions to continue with internal compliance functions, and allow enforcement in the presumably rare cases where an institution is violating its stated policies.

Financial Privacy Notices, (Dec. 4, 2001), *available at*

Several of the participants at the workshop discussed the possibility of a two-tiered notice along the general lines proposed here.

201. I do not have a firm view on the extent to which the format should be standardized by regulation. One can construct plausible arguments for having one standard form, or a group of standard forms for major industries, or a safe harbor for companies that use a standard form with the option for companies to design variations. However much standardization occurs by legal action, the goals would be to communicate clearly, signal the choices that consumers have, and facilitate comparison shopping.

202. Having a link to a web page has important advantages including : (1) updates of the policy can be done on a single web page, at considerably lower cost than printing policies; (2) consumers can review the detailed policy before they begin doing business with an institution; and (3) compliance is easier, both for employees and those on the outside, when there is an authoritative place to go to read the current policy.

IDFN Taking this approach a step further, regulators should consider having a registry for the privacy policies of the financial institutions they regulate. All banks regulated by the Comptroller of the Currency, for instance, might be expected to place their current policies on the Comptroller's web site, searchable by bank name. Consumers could then comparison shop, journalists and watchdog groups could easily review privacy policies, and a dated log could exist of what an institution's policy was at any given time. The burden on industry would be the minimal cost of posting an already-drafted privacy policy to the Comptroller's page. A registry with some of these features exists currently for companies that have signed up with the U.S. Department of Commerce's "Safe Harbor" program for transfers of personal data from the European Union to the United

http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/ safe+harbor+list (listing entities participating in the safe harbor).

This two-tier approach adds considerable flexibility to the notice regime. There can be cost savings for institutions where it makes sense to provide only the shorter notice. For instance, a bank branch could have an easy-to-read flier in its lobby rather than providing six or eight pages of dense typeface.[203] It may be appropriate to save costs and include only the short notice in the annual mailing to customers, with a prominent link to the detailed notice. Updating of the detailed notice can also be done at lower cost, without the need to print and distribute notices to all customers for minor changes.

The two-tier approach also builds on the experience of other regulatory systems. Under the Privacy Act, for instance, federal agencies give a short notice on forms that collect personal information from the public. The details of how information is shared, including the so-called "routine uses," are then published in the Federal Register.[204] As with the proposed two-tier notices for GLB, agencies are held accountable to the detailed statements in the routine uses, with the short forms primarily designed to communicate clearly with the public.

Another useful comparison is to the securities disclosure laws established in the 1930s. The securities regime emerged to correct for the perceived lack of accurate disclosure in the stock market during the 1920s. Similarly, the privacy regime can be seen as a way to correct for the lack of accurate disclosure by U.S. Bank and, by implication, other financial organizations. In looking at securities disclosures, few observers believe that the prospectuses released by public companies are in plain English or are designed primarily in order to communicate effectively with the ordinary investor.[205] The detailed notices, however, require disclosure of all material facts and have resulted in an extensive internal process in most companies to determine the material facts and decide what to disclose. The detailed notices also facilitate enforcement if a company fails to disclose or is misleading in its disclosure.

Another advantage of the two-tier approach is how it resolves frustrations in the current debate. Currently, any request for more detail in the notice is greeted with the observation that the disclosures are already too long and confusing for most consumers. Any request for plain Eng-

203. The notice in the lobby might clearly note that a more detailed notice is available upon request.

204. 5 U.S.C. 552a(e)(4) (2000).

205. Regulators periodically try to make the disclosures more reader friendly, with limited success. *See* 17 C.F.R. § 228-30, 239, 274 (1998), SEC Plain English Disclosures, *available at* http://www.sec.gov/rules/final/33-7497.txt. The analysis here suggests that achieving readability for security prospectuses is not the over-arching goal. Another goal, more important in many respects, is to create a document that provides detailed disclosures against which the company can be held accountable.

lish is greeted with the companies' concern that broad promises will lead to violations and enforcement actions. Simple and short statements also concern privacy advocates who fear that companies will be afraid to make broad privacy promises and so will reserve the right to do whatever they wish with personal information. The two-tier approach, by contrast, allows plainer English in the short form and greater detail in the long form, while quite possibly reducing overall costs due to reduced printing costs where the short form is appropriate.

CONCLUSION

This article has examined the surprising merits of the new financial privacy law. From the privacy side, Title V of the Gramm-Leach-Bliley Act has moved financial institutions a long step toward implementation of the fair information practices of notice, choice, access, security, and enforcement. Due to the broad definition of "financial institution," the law brings these basic privacy principles to a wide range of organizations. Due to the ability of the states to enact stricter privacy protections, there is a credible threat of new financial privacy legislation, and financial institutions thus have an ongoing incentive to convince legislators and the public that they are acting responsibly with individuals' data.

This credible threat of further privacy legislation creates the possibility of re-examining the most important weakness in the current GLB law, which is the limited nature of choice before individuals' data is shared with other institutions. For the issue of choice, this article has advocated the elimination of the "joint marketing exception," which was justified in Congress as a way to help small banks but has been used instead as a major loophole for large financial institutions. This article has also advocated exploring any of several approaches to the issue of sharing with affiliates in the sprawling financial holding companies that GLB creates. One approach is that included in the Clinton Administration's proposed Consumer Financial Privacy Act, which would have required an opt-out choice for affiliate sharing. Another approach would adopt a general "line of business" rule, with sharing freely permitted within the same line of business but choice required before data is sent to different lines of business. This approach is essentially what applies under current European data protection rules. A related approach would define a set of "core" consumer financial services, with sharing permitted within this core but choice required before data is sent to "peripheral" financial institutions such as travel agencies or affiliated retailers. Within any of these approaches, it would be important to allow sharing for pro-consumer purposes such as fraud reduction and customer service, while seeking ways to prevent sharing in violation of reasonable consumer expectations.

From the business side, the experience to date with GLB indicates that protection of consumer privacy is consistent with financial modernization. GLB has allowed the merger or joint operation of consumer financial services companies that the old regulatory regime had kept separate. It makes sense to continue the trend toward having market forces rather than regulators determine which financial services should be offered jointly to consumers. At the same time, the case for merging financial services with non-financial businesses is far less clear. Keeping sensitive financial data within financial firms, while limiting its release to non-financial firms, is largely consistent both with good business practice and good privacy practice.

This article has also explained the surprising virtues of the GLB notice requirements. I agree with the critics that many of the current notices are very detailed and practically unreadable. This level of detail, however, brings with it important advantages. Notably, financial institutions have had to engage in considerable self-scrutiny of their data handling practices. This scrutiny has resulted in many institutions discovering practices that they decided to change. Many companies have also institutionalized privacy protection for the first time, by naming chief privacy officers or in other ways. By requiring financial institutions to make privacy promises, and making those promises enforceable for the first time, GLB has been an important step toward eliminating the most egregious practices and creating a structure for continued improvement over time.

The path to better notices, moreover, is quite clear. Detailed notices should be retained because they create the possibility of detailed accountability. At the same time, much shorter and more readable notices are appropriate in many instances. These short-form notices can resemble nutrition labels in highlighting the most important privacy information. They should be designed with attention to how to communicate effectively with consumers, while providing a ready link to the longer notices for those who want the details. With this two-tier approach, the notices can promote both accountability and clear communication, and likely save costs to the industry by permitting shorter, less-expensive notices to be distributed in many settings.

This article's focus on choice and notice is not intended to ignore other important debates and issues in the financial privacy area. Current law has a loophole that would allow medical information to be shared too freely within a financial holding company. Much more can be said about how to choose between an opt-in and opt-out choice. Stronger protections are likely appropriate for the personal spending habits revealed by

consumers' checking or credit card accounts. These and other issues were included in the Clinton Administration's Consumer Privacy Protection Act, which I continue to support. It would be surprising indeed if a sprawling law such as Gramm-Leach-Bliley got everything right. Perhaps more surprisingly, however, the law provides a better basis for good privacy and good business practice than one would suspect.

MORRISON & FOERSTER LLP

SAN FRANCISCO
LOS ANGELES
DENVER
PALO ALTO
WALNUT CREEK
SACRAMENTO
CENTURY CITY
ORANGE COUNTY
SAN DIEGO

ATTORNEYS AT LAW

2000 PENNSYLVANIA AVENUE, NW
WASHINGTON, D.C. 20006-1888
TELEPHONE (202) 887-1500
TELEFACSIMILE (202) 887-0763

NEW YORK
WASHINGTON, D.C.
NORTHERN VIRGINIA
LONDON
BRUSSELS
BEIJING
HONG KONG
SINGAPORE
TOKYO

April 26, 2002

Writer's Direct Contact
(301) 213-9587
pswire@law.gwu.edu

By Hand Delivery

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: Privacy 2
Hubert H. Humphrey Building
Room 425 A
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Madam or Sir:

This comment letter is submitted on behalf of Privacy Council in response to the request for comment published by the Department of Health and Human Services ("DHHS") in the Federal Register on March 27, 2002 concerning proposed changes to the medical privacy rule issued pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

This comment letter refers to the proposed modifications to Section 164.506, concerning consent, and Section 164.520, concerning notice of privacy practices. The focus of this comment letter is that DHHS, as it considers changes to these Sections, should continue to support plain language in notices to patients. It should continue to ensure that covered entities have the flexibility, when issuing notices to patients, to communicate in the clearest possible way.

This comment letter does not take a position on whether a consent should be required, as provided in the December 28, 2000 regulation (the "Final Rule"), or whether instead there should be acknowledgement of receipt of notice by the patient, as provided in the March 27, 2002 proposed changes (the "Proposed Rule"). The purpose of this comment letter, instead, is to confirm the understanding that plain language notices, with an opening section that highlights key aspects of the notice, are consistent with both the Final Rule and the Proposed Rule.

Attached to this comment letter is a draft law review article that I have written explaining how experience with the Gramm-Leach-Bliley Act strongly supports the use of relatively brief, plain-language notices to communicating effectively with consumers. The knowledge gained in the financial privacy area is important to assuring a successful implementation of notices in the medical privacy area as well.

Background

Privacy Council is a company that provides privacy and security solutions to business. Privacy Council has asked me to draft these comments on its behalf. I have done so through a consulting relationship with the law firm of Morrison & Foerster LLP, with whom I have been working to assist clients with implementation of the medical privacy rule. This comment letter supplements the comment on layered notices submitted on April 19, 2002 by Privacy Council and the Center for Information Policy Leadership of the law firm of Hunton & Williams.

I am Professor of Law at the Moritz College of Law of the Ohio State University, and director of its new program in Washington, D.C. From March, 1999 until January, 2001 I served in the U.S. Office of Management and Budget, as the Chief Counselor for Privacy. In that position I participated extensively in the drafting of the medical privacy rule, coordinating its development for the Executive Office of the President.

This comment letter fully reflects my own personal opinions, as shown by the attached draft article that will be published shortly in the Minnesota Law Review, entitled "The Surprising Virtues of the New Financial Privacy Laws." (The views expressed in the article are entirely my own, and do not reflect the views of Privacy Council.) A central recommendation of that article is that regulators should find ways to assure that individuals receive relatively brief and plain language notices so that the individuals can most effectively learn about an institution's privacy practices. At the same time, it is important and useful for institutions to also draft longer and more detailed notices of their privacy practices. These more detailed notices serve two crucial roles -- providing a way for interested individuals to get more detail about privacy practices, and creating a more detailed blueprint against which the institution's actual practices can be measured.

The Advantages of "Layered Notices"

The Final Rule requires that covered entities that use or disclose protected health information ("PHI") give individuals notice of the possible uses and disclosures of the PHI, and of the individuals' rights and the organization's legal duties with respect to the

information. The Final Rule specifies a substantial number of items, at least nineteen by some counts, that should be included in the patient notices. Research shows, however, that individuals have difficulty processing notices containing so many elements. Accordingly, individuals can get frustrated when confronted with notices that are more detailed than the reader can readily grasp. Individuals may believe that notices are intentionally complex, leaving them with the sense that the organization providing the notice has something to hide.

One solution to this dilemma is "layered" notices. A layered notice would contain: (i) a short notice that helps individuals understand the principal uses of information and the key choices they face with respect to that information; and (ii) a longer notice, layered beneath the short notice, that contains all the elements required by law. The short notice likely uses a simple vocabulary, and it may be formatted in a common template that can be easily compared from one organization to the next. This type of repetitive format, familiar from food labels in the grocery store, can ease the individual's understanding of the notice and bolster trust in the organization.

The use of layered notices is strongly indicated by the experience we have had in implementing the financial privacy provisions of the Gramm-Leach-Bliley Act. As discussed in the attached law review article, consumer groups, Congress, and regulators have been disappointed that the notices used in 2001 were dauntingly long, confusingly written, and ultimately frustrating to many individuals who received them. Financial services providers, in turn, have explained the densely written notices as a necessary response to the detailed requirements in the privacy regulations. A hearing by financial privacy regulators in December, 2001 showed widespread interest in finding ways to implement layered notices -- short and clear notices for customers to read, accompanied by longer and more detailed notices available where appropriate.

My considered opinion is that it is important for DHHS to indicate that use of layered notices is an appropriate part of implementing the HIPAA privacy rule.

I. The Legality of Layered Notices

This part of the comment letter discusses DHHS regulatory writings to date to show how a layered notice approach is consistent with the Final Rule, the Proposed Rule, and the overall goals of the HIPAA privacy process.

Plain language.

The Final Rule begins its discussion of required elements of notice by saying: "The covered entity must provide a notice that is written in plain language and that

contains the elements required by this paragraph." Section 164.520(b)(1). This overall policy of plain language applies to all of the subsequent discussion of required elements of notice. In considering the legality of layered notices, the plain language requirement in the regulatory text gives very strong support for an approach, such as layered notices, that uses clear and concise words to communicate with patients.

In the preamble to the Final Rule, DHHS stated that "we require the notice to be written in plain language. A covered entity can satisfy the plain language requirement if it makes a reasonable effort to: organize material to serve the needs of the reader; write short sentences in the active voice; using 'you' and other pronouns; use common, everyday words in sentences; and divide material into short sections." 65 Fed. Reg. 82548.

The preamble to the Proposed Rule restates the importance of plain language: "In addition, nothing in the proposed requirements described above would relieve any covered entity from its duty to *provide the notice in plain language so that the average reader can understand the notice*. As stated in the preamble to the Privacy Rule, the Department encourages covered entities to consider alternative means of communicating with certain populations, such as with individuals who cannot read or who have limited English proficiency." (emphasis added). By focusing on what the "average reader" can understand, and by considering alternative means of communication, this statement indicates that the intent of the privacy rule is effective communication in plain language, not ritualistic listing of numerous elements in a list.

Clarity.

The Final Rule requires a description of uses and disclosures for purposes of treatment, payment, and health care operations, as well as the other purposes for which disclosures are made. Section 164.520(b)(1)(ii)(A) & (B). For each of these purposes, "the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law." Section 164.520(b)(1)(ii)(C). The text here shows that the regulation intends "to place the individual on notice" of important information. In order to achieve the purpose of this regulatory provision, it is important to know what sort of notice *actually* puts "the individual on notice." For instance, an exhaustive notice written at the graduate-school level would provide more words for the patient to read, but quite likely would put the individual less on notice than a shorter, clearer statement. The goal, as already reflected in the Final Rule, is to have clear and effective notice to individuals, not impenetrable text that lists every way a hospital, for instance, uses medical data.

Similarly, the preamble to the Final Rule states: "We do not require particular formatting specifications, such as easy-to-read design features (e.g., lists, tables, graphics, contrasting colors, and white space), type face, and font size. However, the purpose of the notice is to inform the recipients about their rights and how protected health information collected about them may be used or disclosed. Recipients who cannot understand the covered entity's notice will miss important information about their rights under this rule and about how the covered entity is protecting health information about them. One of the goals of this rule is to create an environment of open communication and transparency with respect to the use and disclosure of protected health information. *A lack of clarity in the notice could undermine this goal and create misunderstandings.* Covered entities have an incentive to make their notice statements clear and concise. We believe that the more understandable the notice is, the more confidence the public will have in the covered entity's commitment to protecting the privacy of health information." 65 Fed. Reg. 82549 (emphasis added).

Flexibility.

The Final Rule clearly contemplates flexibility in how covered entities provide the notice. For instance, the response to comments stated: "On the whole, we found commenters' arguments for *flexibility* in the regulation more persuasive than those arguing for more standardization…. We also do not require particular formatting. We do, however, require the notice to be written in plain language. We also agree with commenters that the notice should contain a standard header to draw the individual's attention to the notice and facilitate the individual's ability to recognize the notice across covered entities." 65 Fed. Reg. 82721 (emphasis added).

This commitment to flexibility makes clear that a short, clear notice might appropriately be used as the top layer of notice, supplemented by the longer and more detailed notice that puts the most interested individuals on notice of the details of the covered entity's policy.

Short notices appropriate.

The Preamble to the Final Rule supports the view that short, easy-to-read notices are appropriate in at least some circumstances. For instance, the Preamble states "Covered providers that maintain a physical service delivery site must prominently post the notice where it is reasonable to expect individuals seeking service from the provider to be able to read the notice." 65 Fed. Reg. 82551. If the regulation were interpreted to mean that the only permissible notices were very lengthy, then it is difficult to imagine how such a notice would appropriately be posted on a wall where patients would be able to readily read the notice.

Recommended Action

In the Proposed Rule, DHHS proposed modifications to Section 164.506, concerning consent, and Section 164.520, concerning notice of privacy practices. As the Department responds to the present round of public comments, and continues to build on the administrative record developed in earlier rounds of public comments, the Department can and should clearly indicate that it is appropriate to draft notices in ways that most effectively communicate with the patients. As policymakers, consumer groups, and covered entities learn more about what notices work best, HIPAA should allow state of the art notices to be used without creating inadvertent regulatory obstacles to such use.

At a minimum, DHHS should indicate that there is enough flexibility in the regulation to permit a short, plain-language notice as the top layer for a more detailed notice. Many patients will prefer to read the short notice on top, while those who wish more detail can look at the detailed bottom layer as well. I have not been able to think of any legal or policy argument against the permissibility of this two-layer approach. If DHHS agrees with the permissibility and advisability of this approach, it might actually encourage such an approach as part of the overall effort to supply the most effective notice to patients.

I believe, in addition, that there is or should be room within the Final Rule and Proposed Rule for providing only the short, plain-language notice in certain instances. Consistent with the regulation's overall approach favoring reasonableness and flexibility, providing only the short notice seems appropriate where it is reasonably certain that it is easy for a patient who wishes to see the more detailed notice to do so. For instance, the short notice might reasonably be provided to a patient in a treatment room, so long as there is a prominent instruction that a more detailed notice is available at the front desk.

Going further, a short notice might be provided in circumstances where it is reasonably certain that the individual has ready access to the Internet, with a URL (web address) that gives the detailed notice. This approach might be appropriate, for example, in situations where patients are using the Internet as part of their interaction with the covered entity. In such circumstances, the detailed notice would be only a click away and the short notice should so indicate. The Final Rule provides that "covered entities that maintain a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site." Section 164.520(c)(3). The response to comments for the Final Rule also states that covered entities "may elect to distribute their notice

electronically (via email) provided the individual agrees to receiving the notice electronically and has not withdrawn such agreement." 65 Fed. Reg. 82724. In such instances, a short notice distributed by email, accompanied by an easy link to the detailed notice, would make it reasonably certain that the individual receiving the email could readily review the detailed notice as well.

As DHHS considers the proposed changes to the Consent and Notice sections of the regulation, its view about this important topic might be appropriate in the preamble, the response to comments, in Guidance that may be forthcoming, or by institutionalizing this understanding more formally in the regulation.

For more information on these comments, feel free to contact Toby Milgrom Levin of the Privacy Council at (202) 772-3106, toby.levin@privacycouncil.com, or myself at (301) 213-9587, swire.1@osu.edu.

Thank you for the opportunity to comment on the Proposed Rule, and my best wishes for its successful implementation.

Sincerely,

Peter P. Swire
Professor of Law
Moritz College of Law at the
Ohio State University

Enclosure
Draft version of "The Surprising Virtues of the New Financial Privacy Law", forthcoming in final form in the Minnesota Law Review.