

Web: [www.peterswire.net](http://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](http://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.<sup>1</sup> 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.<sup>2</sup>

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, securities, and other financial services industries. Since the 1930's, the Glass-Steagall Act had largely separated these industries. Gramm-

---

† 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.

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,<sup>3</sup> 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.

In short, this article shows the surprising merits of the GLB privacy

---

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](http://www.osu.edu/units/law/swire.htm).

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.<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup> 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.<sup>7</sup>

---

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](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 Information Infrastructure: Principles for Providing and Using Personal Information*

## A. NOTICE

The FTC calls notice “[t]he most fundamental principle . . . .”<sup>8</sup> Without notice, the consumer “cannot make an informed decision as to whether and to what extent to disclose personal information.”<sup>9</sup> 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”).<sup>10</sup> This personal information may not be disclosed to another corporation unless the consumer is provided a notice.<sup>11</sup> 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].”<sup>12</sup> 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.<sup>13</sup> 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.

## B. CHOICE/CONSENT.

The choice/consent principle has been a major source of contention,

---

(June 6, 1995), available at [http://itf.doc.gov/ipc/ipc/ipc-pubx/niiprivprin\\_final.html](http://itf.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 Doc. 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).

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.”<sup>14</sup> 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.<sup>15</sup>

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.<sup>16</sup>

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.<sup>17</sup> Industry has also supported the ability to share data with nonaffiliated third parties.<sup>18</sup> Privacy proponents have maintained that sharing with

---

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. Transportation Appropriations Act, Pub. L. 106-346, § 309. Stat. (2000) (amending 18 U.S.C. § 2721). 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).

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).

