

March 31, 2000

Secretary  
Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue N.W.  
Washington, DC 20580

Re: Gramm-Leach-Bliley Act Privacy Rule, 16 CFR Part 313-Comment.

To whom it may concern:

Thank you for the opportunity to provide comments with respect to the proposed new privacy rules (16 CFR Part 313) applicable to all financial institutions. The following comments are in regard to the proposed new privacy rules as they appear in the March 1, 2000 Federal Register.

The authors of this letter are David Gonzalez, a third-year evening law student at the University of the Pacific McGeorge School of Law, and Professor J. Clark Kelso, who is the Director of the Institute for Legislative Practice at the University of the Pacific McGeorge School of law. As a matter of policy, the Institute for Legislative Practice does not support or oppose any legislation or administrative rules. Instead, these comments are intended simply to highlight for your consideration certain issues raised by the proposed rules.

Consistent with GLBA, the proposed provisions of the new privacy rules appear to focus primarily on providing customers with notice of their financial institution's policies regarding privacy and personal data. The "opt out" provision seems to be the only method available under the proposed new rules that grants the customer some direct control over the use of their personal data with respect to nonaffiliated institutions, and there is virtually no control over the use of personal data by affiliated institutions. Exercising this "opt out" right to secure private information may seriously limit a customer's ability to benefit from acceptable and often necessary disclosures of personal information between financial institutions and nonaffiliated third parties. As drafted, the "opt out" provision seems to embody an all-or-nothing approach when a more finely-tuned, flexible approach might better accommodate consumers' needs.

While § 313.7(c) provides that a financial institution *may* offer a customer a partial "opt out" of the disclosure of personal information, this provision is not mandatory. Therefore, a customer may be forced to either remain silent regarding the disclosure of their personal data, or "opt out" entirely from the beneficial and often necessary disclosures of personal information between financial institutions and nonaffiliated third parties. We wonder whether consumer's would be better served by mandating that financial institutions offer a partial "opt out," which would create more flexible privacy protections.

The proposed new privacy rules also do not appear to address many issues regarding potential abuses in the use of customers' personal data. Instead, as noted above, the primary mechanism for safeguarding privacy is the "opt out" provision.

The issue of safeguarding the privacy of personal data has gained worldwide attention. In 1980 the Organization for Economic Cooperation and Development (“OECD”) established eight basic principles regarding the protection of the privacy of personal data (which may be retrieved from <http://www.oecd.org/dsti/sti/it/secur/prod>). These eight basic principles have been accepted by all of the members of OECD, which includes the United States. We think it is useful to compare the recently enacted provisions of GLBA and your proposed new rules regarding privacy, which essentially duplicate GLBA’s privacy provisions, to these eight generally accepted principles proposed by the OECD. Our comparison of GLBA’s privacy protections with the eight OECD principles (see Appendix A) indicates a wide gap between GLBA and the proposed rules and privacy principles that have been widely adopted around the world.

Many states are now considering legislation that would fill the gaps between GLBA and the proposed rules, on the one hand, and OECD privacy principles, on the other hand. In the interest of national uniformity, you may wish to consider whether some additional privacy protections in your rules would reduce the perceived need for individual state privacy regulation.

Again, we thank you for the opportunity to provide these comments.

Respectfully,

David Gonzalez  
&  
J. Clark Kelso, Professor of Law and Director,  
Institute for Legislative Practice  
University of the Pacific McGeorge School of Law

**Appendix A**  
**Comparison of GLBA privacy provisions with eight OECD privacy principles**

**1. COLLECTION LIMITATION PRINCIPLE.**

*The GLB Act does;*

- A) Under 15 U.S.C. 6802 prohibit a financial institution from disclosing a customer's nonpublic personal information without providing them with notice of that institution's practices and policies regarding disclosure of nonpublic personal information to third parties.
- B) Under 15 U.S.C. 6802 prohibit a party that receives nonpublic personal information from a financial institution from disclosing that information to other parties.
- C) Under 15 U.S.C. 6821 contain prohibitions against the collection of customer information under false or fraudulent pretenses.

*The GLB Act does not;*

- A) Generally require that the collection of personal data be done with the knowledge or consent of the data subject.
- B) Apply the prohibitions of 15 U.S.C. 6821 to:
  - 1) law enforcement agencies,
  - 2) financial institutions in some cases like investigating allegations of misconduct,
  - 3) insurance institutions for investigations of insurance fraud,
  - 4) situations where a person is obtaining information that is otherwise available as a public record filed pursuant to the securities laws, and
  - 5) collections of child support judgements.

**2. DATA QUALITY PRINCIPLE.**

*The GLB Act does not;*

- A) Specifically require that personal data that has been collected be relevant to the purposes for which they are to be used. The focus of the GLB Act is on regulating the disclosure of personal data.
- B) Require personal data be kept accurate, complete and up-to-date.

**3. PURPOSES SPECIFICATION PRINCIPLE.**

*The GLB Act does not;*

- A) Require an entity to specify the purposes for which personal data are collected.
- B) Limit the subsequent use of personal data to the purposes originally specified by the data controller.

**4. USE LIMITATION PRINCIPLE.**

*The GLB Act does;*

- A) Under 15 U.S.C. 6802 prohibit a financial institution from disclosing a customer's nonpublic personal information without providing them with notice of that institution's practices and policies regarding disclosure of nonpublic personal information to third parties.
- B) Under 15 U.S.C. 6802 prohibit a party that receives nonpublic personal information from a financial institution from disclosing that information to other parties.

*The GLB Act does not;*

- A) Require a data controller to limit its use of personal data for only those purposes which the data controller specifies.

**5. SECURITY SAFEGUARDS PRINCIPLE.**

*The GLB Act does;*

- A) Under 15 U.S.C. 6801 state that it is the policy of Congress that each financial institution have an affirmative and continuing obligation to protect the security and confidentiality of its customer's nonpublic personal information.
- B) Under 15 U.S.C. 6801 state that certain agencies shall establish standards to insure the security and confidentiality of customer records and information.

**6. OPENNESS PRINCIPLE.**

*The GLB Act does;*

- A) Under 15 U.S.C. 6803 provide that at the time of establishing a customer relationship, and not less than annually, a financial institution shall provide clear and conspicuous information to a customer regarding that financial institution's policies and practices with respect to disclosing nonpublic personal information.

*The GLB Act does not;*

- A) Require that means be readily available for establishing the existence and nature of personal data, the main purposes of their use, and the identity and usual residence of the data controller.

## **7. INDIVIDUAL PARTICIPATION PRINCIPLE.**

*The GLB Act does not;*

- A) Give an individual the right to obtain from a data controller confirmation as to whether or not the data controller has data relating to them.
- B) Give an individual the right to challenge data relating to them.

## **8. ACCOUNTABILITY PRINCIPLE.**

*The GLB Act does;*

- A) Under 15 U.S.C. 6805 provide that the prohibitions regarding disclosure shall generally be enforced by the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission.
- B) Under 15 U.S.C. 6822 provide that the prohibitions regarding fraudulent access to information be enforced by the Federal Trade Commission.
- C) Under 15 U.S.C. 6823 provide criminal penalties for anyone who knowingly or intentionally violates the prohibitions regarding fraudulent access to information.