



January 27, 2011

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: **Commercial Data Privacy and Innovation in the Internet Economy:
A Dynamic Policy Framework**

Dear Sir or Madam:

The Mortgage Bankers Association¹ (MBA) appreciates the opportunity to comment on the Department of Commerce Internet Policy Task Force's "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." MBA supports commercial data privacy protections that safeguard consumer information and the integrity of transactions performed in the digital economy. We agree that consumers and taxpayers need to be protected; the result, however, should not be merely more procedural hurdles, but clear guidance concerning privacy protection for consumers. MBA also supports privacy standards that will allow economic growth and enable businesses to continue to offer products and services of interest to consumers.

The comments included in this letter address the following issues:

- Bolstering Consumer Trust Online Through Privacy Standards
- Advancing Consumer Privacy Through a Focus on Transparency, Purpose Specification, Use Limitation, and Auditing
- Maintaining Dynamic Privacy Protections Through Voluntary, Enforceable, FTC-Approved Codes of Conduct
- National Requirements for Security Breach Notification
- Preemption of State Laws

¹ The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 280,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets; to expand homeownership and extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 2,100 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, Wall Street conduits, life insurance companies and others in the mortgage lending field. For additional information, visit MBA's Web site: www.mortgagebankers.org.

I. Bolstering Consumer Trust Online Through Privacy Standards

An underlying question presented in the Department of Commerce green paper is whether privacy standards should be established by statute or other means to address how privacy laws are enforced. MBA agrees standards could help ensure privacy for consumers and the further development of the Internet economy. Privacy principles need to be flexible because technologies and business models evolve quickly. Therefore, MBA questions whether the legislative process is sufficiently adroit to be compatible with the dynamic nature of privacy considerations. MBA recommends that regulators and industry representatives collaborate to develop voluntary and flexible guidance and principles.

Fair Information Practice Principles

The Department of Commerce green paper suggests enhancing consumer trust online through recognition of revitalized Fair Information Practice Principles (FIPPs) that “promote increased transparency through simple notices, clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes, and expanded use of robust audit systems to bolster accountability.”² MBA believes that FIPPs would provide a framework for the development of privacy guidelines. However, we caution that data collection restrictions and audit systems must be designed with care; we address these issues in later sections of this letter.

To be effective, the FIPPs developed would need to be a single set of standards to ensure they are consistent across the government. Consultation and cooperation between regulatory agencies are key to the development of a framework to guide commercial data privacy. While guidance on privacy is needed, a framework must ensure there are no unnecessary restrictions on product development and that any standards do not impede business innovation or interfere with necessary business operations.

Recently, the Department of Commerce and the Federal Trade Commission (FTC) both released privacy frameworks, and the green paper, produced by the Department of Commerce, recommends that “The FTC should remain the lead consumer privacy enforcement agency for the U.S. government.”³ We note, however, that the new Consumer Financial Protection Bureau (Bureau) has been granted broad powers and authorities with respect to consumer financial products and services to ensure “markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation.”⁴

Additionally, when prescribing rules to prevent unfair, deceptive or abusive acts or practices, the Bureau is directed to consult with the federal banking agencies, or other federal agencies, as appropriate, concerning the consistency of the proposed rule with prudential, market, or systematic objectives administered by such agencies. Considering the Bureau’s important role going forward, we believe involvement with the Bureau is necessary, as well.

² Department of Commerce, Internet Policy Task Force, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,” (2010), pg. 4.

³ *Id.*, pg. 51.

⁴ Dodd-Frank Act, Pub. L. No. 111-203, § 1021(b)(5), 124 Stat. 1376, 1980 (2010).

In the green paper, the Department of Commerce recommends the creation of a Privacy Policy Office⁵ (PPO) within the Department of Commerce with the authority to convene multi-stakeholder discussions about commercial data privacy and best practices. While MBA needs further information to understand the exact role the PPO would play, the PPO might provide an opportunity for information collected from stakeholders to be jointly shared between regulatory authorities. MBA believes that federal regulatory agencies should ensure there is adequate time for stakeholders to consider proposals and provide needed input. To this end, we urge the Department of Commerce to work in tandem with the FTC and the Bureau to avoid duplicative, overlapping or confusing guidance concerning privacy.

Furthermore, the Department of Commerce asks in the green paper if baseline commercial data privacy legislation should include a private right of action.⁶ MBA does not believe there is a need for a private right of action if the privacy standards are clear and subject to government review. Additionally, the permanent threat of action could hinder new product research and development, thus stifling further technological advances.

II. Advancing Consumer Privacy Through a Focus on Transparency, Purpose Specification, Use Limitation, and Auditing

Data Collection Practices and Data Restrictions

MBA acknowledges that the ultimate goal of a consumer privacy program is the safeguarding of sensitive nonpublic consumer information. MBA agrees that privacy standards should be important in the collection and use of information, both online or offline. Consent to collect information must be flexible so that requirements are not onerous to business operations or limit the use of information for legitimate business needs. Also, consumer choice and consent should not be necessary for commonly accepted data practices, including product and service fulfillment, internal operations such as improving services, fraud prevention, legal compliance and first-party marketing activities. When information is collected online, a privacy policy can be delivered in concert with the collection of information, along with consumer choice about collection practices. However, it may not be feasible to make the requisite level privacy policy disclosure in tandem with the collection of information in the offline environment. Privacy policies should be flexible to allow for adequate timing of a privacy notice and consumer choice regarding the collection of information once it is collected in an offline environment.

In addition, limits on data retention requirements or a required purge of information may disrupt business operations. For example, a forced purge of information may delete data about a borrower's successful payment history that would have allowed for a favorable adjustment of a consumer's rate or term of a loan. In addition, sometimes a consumer provides unsolicited information as part of a required document. For instance, a paycheck stub collected for proof of income may include unsolicited information, such as marital status or number of dependents. If a regulation prohibits the retention of this information, it would be problematic for an institution. Redacting the information would be burdensome and confusing. Also, it could compromise the integrity of the audit process; it may not be clear what information was redacted and whether it was material to a decision on the loan.

⁵ Department of Commerce, Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," (2010). pg. 45.

⁶ *Id.*, pg. 30.

Proper safeguards are essential, but we respectfully request that they are reasoned with requirements of business operations.

Privacy Impact Assessments

The green paper suggests that a means to manage privacy profiles and provide further transparency is through Privacy Impact Assessments⁷ (PIA). The paper further suggests that “if prepared in sufficient detail and made public, PIAs could create consumer awareness of privacy risks in a new technological context, where norms are not yet clear.”⁸ Further, it states that PIAs could guide organizations as to what activities or approaches would help prevent privacy risks. MBA believes that an internal audit of privacy profiles would be helpful in identifying risks and bolstering accountability to an institution and consumers. An internal process would show what steps an institution has taken to guard privacy of consumers. However, developing such assessments may entail skill sets or resources not common to every entity, which would then result in additional costs imposed by a third party. MBA cautions against developing a new audit procedure specific for PIAs and requiring an independent audit of these activities. If an independent audit is mandated, as recommended by the National Institute of Standards and Technology in its “Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid,”⁹ the cost may be prohibitive to the information technology infrastructures of smaller companies. Therefore, MBA recommends that validation of the compliance be performed internally or externally, and that the audit be performed at least annually. The green paper is not clear about how a compliance program would be structured and what auditing requirements would be required to demonstrate compliance.

MBA further recommends that a compliance program for PIAs should include clear and objective enforcement standards. MBA also recommends that auditing requirements reuse other assessment and auditing mechanisms where possible, reach out to industry standards organizations and be consistent across vertical industries. For example, the Payment Card Industry Data Security Standard (PCI DSS) is an internationally used compliance program to prevent credit card fraud through increased requirements for the access control and handling of cardholder information.

III. Maintaining Dynamic Privacy Protections Through Voluntary, Enforceable, FTC-Approved Codes of Conduct

Safe Harbor

MBA appreciates the Department of Commerce’s recognition that privacy legislation might be prohibitive and could cause “locking-in outdated rules that would fail to protect consumers and stifle innovation.”¹⁰ Clear guidance about managing privacy expectations is needed; MBA believes the possibilities suggested in the green paper should further be explored:

- “Baseline commercial data privacy policies that would fill any gaps in existing U.S. law;
- Support for development of voluntary, enforceable codes of conduct that enable continued flexibility in rules that can evolve with new technologies and business models;

⁷ Department of Commerce green paper, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,” (2010), pg. 34.

⁸ *Id.*, pg. 35.

⁹ *Id.*, pg. 35, FN 109.

¹⁰ *Id.*, pg. 29.

- Safe harbors against FTC enforcement for practices defined by baseline data privacy or voluntary, enforceable codes;
- Limited rulemaking authority over certain baseline FIPPs if it is established that market failures require prescriptive regulatory action; and
- A framework likely to lead to lower barriers to the global free flow of goods and services online.”¹¹

MBA believes that there should be a safe harbor for companies that comply with and follow a voluntary code of conduct for commercial data policy. As suggested in the green paper, a voluntary code of conduct would have to meet certain requirements and have approval by the FTC for sufficiency to be eligible for a safe harbor. We are in agreement with the Department of Commerce that “FTC approval of a voluntary enforceable code of conduct as sufficient would establish a presumption that an entity that demonstrates compliance with the code would not be subject to an enforcement action under FIPPs-based commercial data privacy legislation.”¹² We believe an approach that includes the FTC working in concert with a broad spectrum of relevant industry representatives to establish a voluntary code of conduct would be the best way to safeguard consumer data privacy. A voluntary code should not restrict innovation in business and should continue to allow companies to offer beneficial products and services to consumers.

Do Not Track

MBA appreciates that the Department of Commerce is encouraging discussion about technologies such as “Do Not Track” (DNT).¹³ However, MBA questions the need for a new DNT requirement in light of the many comparable options that currently exist in lieu of other potential solutions. There are technology solutions that could serve the same purpose without requiring the creation of a specific DNT standard. Two easily implementable components would serve the same purpose as a DNT standard while eliminating additional expense and operational requirements.

1. Many existing browsers permit users to change settings to prevent the download of or allow for deletion of cookies on their machines. This solution is easily accomplished by the consumer, on their own computer, without the need to visit websites to record such information.
2. To prevent companies from tracking usage, a new HyperText Transfer Protocol (HTTP) header could be created. The browser would permit the consumer to change the setting to permit or deny tracking. The HTTP header, containing the consumer’s tracking preference, would be transmitted with every web request from the consumer. This approach would require modification to browsers. However, many browsers already have add-ons that demonstrate how the additional HTTP header may be used for DNT. This additional header would be read by the receiving institution and would immediately communicate what a consumer’s preference is in regards to tracking. The HTTP header will require that the financial institution adhere to the consumer’s preference. However, there is the question of how this will be enforced. To this end, MBA recommends that a standard be developed so that the parties, types of data and retention periods are clearly delineated. Furthermore, MBA

¹¹ *Id.*, pg. 29.

¹² *Id.*, pg. 44.

¹³ *Id.*, pg. 51.

recommends that compliance to implementation of the HTTP header be fully defined and vetted in a cross-industry forum.

The technology solutions noted above would be fairly easy to implement and would provide the consumer with the same control as with the proposed DNT. In his testimony before the House Subcommittee on Commerce, Trade and Consumer Protection, Daniel Weitzner acknowledges that universal blocking can largely be accomplished with existing browser settings and tools already available. He suggests “greater consumer education about tools already available might be all that is needed.”¹⁴ MBA agrees that the necessary technology already exists to meet the goals of DNT and that consumer education regarding these tools is a more effective and efficient mechanism to meet the goals than a standardized, prescriptive program. Another available option to further educate consumers is for the Department of Commerce to include information about using browser settings on its Web site.

MBA foresees significant operational expense that would be required to interact with a prescribed DNT option. For example, this option would conceivably require an institution to direct all internet queries against the DNT to validate whether it could be tracked. This contrasts with the simple directive suggested that would accompany a query under the proposed new HTTP header.

IV. National Requirements for Security Breach Notification

In its green paper, the Department of Commerce recommends that “Consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Such a framework should track the effective protections that have emerged from State security breach notification laws and policies.”¹⁵

MBA understands that strong data security is crucial for the operation of our modern real estate finance system and for a digital economy. A national security framework should be consistent with the Gramm-Leach-Bliley Act¹⁶ (GLB) so that new legislation effectively builds on/or leverages GLB privacy stipulations. In addition, MBA firmly believes in a need for strong preemptive language, to avoid the regulatory burden of staying current with an ever-changing patchwork of state and local laws. State laws should be reviewed to help identify best practices, but broad preemptive language is needed. Penalties for security breach notification violations should be identified that are commensurate with the type and scope of a security breach. MBA supports the development of agreeable and concise security breach triggers that will not cause a lender to be unnecessarily overburdened with providing notifications, especially if there is not a perceivable threat of identity theft. We agree that all breaches need to be addressed in some manner; we suggest establishing a clear definition of an information breach that warrants full action and reporting.

¹⁴ “Do-Not-Track’ Legislation: Is Now the Right Time?” Hearing before the Subcommittee On Commerce, Trade and Consumer Protection, Energy and Commerce Comm., 111th Cong. (2010) (statement of Daniel J. Weitzner, Associate Admin. for Policy Analysis and Development, U.S. Dept. of Commerce) pg. 11.

¹⁵ Department of Commerce, Internet Policy Task Force, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,” (2010), pg. 57.

¹⁶ Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338 (1999).

V. Preemption of State Laws

The Department of Commerce recommends that “Any new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.”¹⁷

MBA believes that guidance ought to be provided to industry that is responsive to consumers’ privacy expectations, and balanced with business opportunities. However, on the question of federal preemption of state laws regarding privacy, if a national privacy statute was enacted, MBA believes that strong preemptive language should be included. MBA would advocate this language to provide consistency for mortgage lenders operating in more than one state. On the other hand, guidance could also be provided for federal and state governments to adopt that would be more flexible as new technologies are implemented. In addition, a policy statement may be amended more easily than a statute.

Conclusion

MBA supports the creation of a privacy policy framework. However, we caution the Department to carefully consider potential unintended consequences. If there is not a clear understanding of business operations that must coincide with the suggested guidelines before they are implemented, there will likely be unintended consequences to the mortgage industry.

We look forward to assisting the Department of Commerce to further develop the ideas presented in the green paper. For questions or further information, please contact Sandra Troutman, Director of Public Policy, stoutman@mortgagebankers.org or (202) 557-2858.

Sincerely,



John A. Courson
President and Chief Executive Officer
Mortgage Bankers Association

¹⁷ Department of Commerce, Internet Policy Task Force, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,” (2010), pg. 61.