June 9, 2010

By Electronic Delivery

National Telecommunications Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Washington, D.C. 20230

Re: Information Privacy and Innovation in the Internet Economy

Ladies and Gentlemen:

This comment letter is submitted on behalf of the Financial Services Forum (the "Forum") in response to the Department of Commerce ("Commerce") Internet Policy Task Force's Notice of Inquiry ("Notice") relating to privacy and the Internet economy, published in the Federal Register on May 10, 2010. The Forum is a non-partisan financial and economic policy organization comprising the CEOs of 19 of the largest and most diversified financial services institutions doing business in the United States. In this letter, the Forum has addressed those issues that are of particular importance to financial institutions. We appreciate the opportunity to comment on this important matter.

The U.S. Government Should be Sensitive to Overly Broad Regulation

As the U.S. government considers privacy and the Internet, it is critical that the government is sensitive to ensuring the delicate balance between innovation and regulation. An overly prescriptive regulatory regime would likely stifle innovation without truly protecting consumer privacy interests. Moreover, such a result could place U.S. companies at a competitive disadvantage with respect to their global competitors.

An example of this disadvantage can be seen in restrictions on cross-border data transfers of personal information that have provided little, if any, meaningful benefit to consumers, while imposing substantial costs on businesses and governments. As the world has grown more globally connected, restrictions on cross-border data transfers have become outmoded.

Complex, global data flows are necessary in order for businesses to provide the services that their customers expect, as well as to manage their operations in an efficient and cost effective manner, such as to obtain the benefits derived from centralized data servers or company-wide portals. In fact, global data flows are now a common and essential component of our daily lives. For example, when travelling abroad, information must flow across borders in order for individuals to use ATM cards, including to authorize transactions, and banks must maintain the necessary information technology to allow customers to do so. Similarly, when a fraudster located in another country tries to use a credit card for an unauthorized purchase, information must be able to flow across borders in order to prevent such fraud. The benefits of these data flows are passed on to consumers in many forms, including, for example, enhanced customer services (*e.g.*, 24-hour customer hotlines) and a greater choice of products and services at lower prices. Countries, in turn, benefit from increased global business investments and activity. All in all, consumers, businesses and governments receive enormous benefits from global flows. Countries that limit cross-border data flows or impose highly regimented privacy regimes impose significant costs on their economies, including the substantial costs associated with compliance for those businesses that continue to operate within those countries and the costs of business opportunities lost to other countries in the increasingly competitive global technology-driven information-based economy. Those costs disproportionately outweigh the limited benefits that the laws actually provide.

Businesses seek to offer consumers a wide array of goods and services at competitive prices and to promptly meet and respond to their customers' needs. To do so, businesses need to manage their global operations effectively. This may include, for example, centralizing certain functions for the organization (*e.g.*, a central database for processing the organization's human resources data). Also, today's technology allows businesses to allocate resources more effectively, including, for example, dividing work among employees and contractors located around the world so that work can be accomplished around the clock following the sun. In order to do so, a business must be able to transfer both non-personal information, such as analytical data, as well as personal information, such as customer and employee data, to their operations around the world.

While such transfers are necessary to manage the business in an efficient manner, they also permit the organization to offer services to its customers. For example, by relying on service representatives from different time zones throughout the world to "come online" at different times, a business can provide customer service to assist customers who may be located halfway around the world. To be effective and convenient for the customer, these service representatives must have access to the organization's databases containing customer information, such as a customer's credit, purchase or other transaction records. They also need access to the organization's employee data so they can, direct any required follow-up service to the correct office.

It is also important to note that large multi-national businesses rely on global data flows in order to comply with legal and regulatory obligations and for risk control and fraud prevention activities. For global financial institutions, in particular, moving and centralizing data around the world is critical in order to effectively identify, assess, monitor and manage credit, operational and other risks. Moreover, global data flows are essential for financial institutions to prevent fraud, money laundering and terrorist financing. Financial institutions must also frequently rely

on global data flows to share information as required or permitted by law (*e.g.*, in connection with litigation, for regulatory examination purposes, and to conduct internal investigations). In fact, existing U.S. privacy laws include exceptions to limitations on sharing that recognize the critical need to ensure these types of data flows. *See*, *e.g.*, 15 U.S.C. §§ 6802(e)(3), (4), (8) (GLBA); 15 U.S.C. §§ 1681b(a)(1), (4)-(6), 1681u, 1681v (FCRA).

Limitations on the free flow of information or rules that require over-notification and impose unnecessary burdens will have an adverse effect on innovation, will limit the choices provided to consumers, impede the ability to comply with law and control criminal activity and make it more difficult for U.S. companies to compete against their global counterparts.

A Sectoral Approach to Privacy is Appropriate

The U.S. model for regulating business practices is rooted in a recognition that overly broad regulation adversely impacts businesses and, in turn, the economy. This has led to a reluctance to regulate business practices absent a demonstrated need. As a result, Congress tends to adopt legislation to address specific instances of abuse, all while protecting important national interests, whether those be related to maintaining or bolstering a vibrant economy or maintaining accurate and meaningful information about consumers that is critical to commerce (*e.g.*, ensuring the availability of credit report information for legitimate and appropriate purposes, as discussed below).

As a result, the U.S. has concluded that an omnibus or "one-size-fits-all" legislative approach to privacy lacks the necessary precision to avoid interfering with the benefits that follow from the free flow of information, as well as the benefits to the national economy that are derived from entities that are regulated at the national level, such as financial institutions.

Instead, the U.S. approach to privacy (comprised in a number of statutes) focuses on particularly significant privacy interests. These privacy interests may relate to particularly sensitive types of information, such as information about children, or about inappropriate uses of information, such as abusive e-mailing. Thus, the landscape of U.S. privacy law is quite broad and varied. The following are examples of U.S. privacy laws that protect important consumer privacy interests:

- children's personal information (Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq.*);
- consumer telephone information (Telephone Consumer Protection Act, 47 U.S.C. § 227);
- consumer e-mail information (CAN-SPAM Act, 15 U.S.C. § 7701 *et seq.*);
- personal information collected by cable companies (Cable Communications Policy Act, 47 U.S.C. § 551);
- personal information collected by telephone companies (Customer Proprietary Network Information, 47 U.S.C. § 222);

- computer information (Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq*.);

- credit report information and information shared among affiliated companies (Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*.);

- information relating to customers of financial institutions (Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq*.);

- health information (Title II of the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191);

- driver's license information (Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq*.); and

- information about sex, race, color, religion and marital status (Equal Credit Opportunity Act, 15 U.S.C. § 1691 *et seq*., Equal Employment Opportunity Act, 42 U.S.C. § 2000e *et seq*. and Fair Housing Act, 42 U.S.C. §§ 3604-3605);

- student information (Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g);

- employee polygraph information (Employee Polygraph Protection Act, 29 U.S.C. § 2001 *et seq*.);

- employee retirement information (Employee Retirement Income Security Act, 29 U.S.C. § 1025);

- mail (39 U.S.C. § 3623);

- communications by debt collectors (Fair Debt Collection Practices Act, 15 U.S.C. § 1692 *et seq*.); and

- video rental information (Video Privacy Protection Act, 18 U.S.C. § 2710).

This sectoral approach appropriately focuses on limiting inappropriate use of information, while ensuring privacy and enhancing deeply rooted traditions, including both free information flows and avoiding overly broad regulation. For example, the U.S. should continue to rely on business's public declarations concerning their privacy practices (*e.g.*, privacy notices), reinforced by government enforcement to ensure that businesses actually implement and follow their privacy promises. Where the government must intervene, it should only do so where it determines that particularly sensitive privacy interests of individuals are not otherwise being sufficiently protected and then only in a way that is narrowly tailored to protect those interests (the approach used in the various federal privacy statutes listed above, as well as those discussed in greater detail below).

U.S. Law Provides Consumers with Substantial Protections for Financial Privacy Under a Sectoral Approach

One area of U.S. privacy law that has historically received substantial federal oversight is financial privacy. Of the various types of personal information relating to consumers, consumer financial information has generally been deemed particularly sensitive and, as a result, deserving of greater protection. Consistent with the approach to federal privacy legislation described above, Congress has enacted numerous measures that are narrowly tailored to protect specific privacy interests, but that also take into account the business realities of how financial institutions operate. Existing federal protections for consumer financial information are robust, including, for example, privacy protections in the Gramm-Leach-Bliley Act ("GLBA"), the Fair Credit Reporting Act ("FCRA"), the Electronic Funds Transfer Act, the Equal Credit Opportunity Act, and the Fair Credit Billing Act.

As a result, financial institutions are subject to a detailed array of privacy obligations and limitations with respect to consumer financial information. The laws that comprise the rigorous privacy regime to which financial institutions are subject are designed to complement each other and work together. For example, these laws recognize the unique holding company structure within which many, if not most, financial institutions operate.

It is important to note that these financial privacy laws have been the subject of congressional and regulatory debate and refinement over the past 40 years (dating back to the enactment of the FCRA in 1970). Over time, where Congress or federal regulators have identified new issues requiring financial privacy protection, they have stepped in and provided that protection. For example, in 2003, Congress amended the FCRA to address the use of certain types of information shared among affiliated entities for marketing purposes.

The various financial privacy laws are working as intended, balancing the legitimate and appropriate needs of financial institutions for free flow of information and the actual business realities of how financial institutions operate against consumer privacy interests. There is no need to abandon or replace this comprehensive scheme of financial privacy laws that has been tailored by Congress and financial regulators over decades to protect consumers' financial privacy.

The federal government should continue to support a sectoral model that is customized to specific industry sectors or specific types of information. In fact, the method of regulating financial institutions may be a model for, and could be extended to, other sectors. The focus of financial regulation is not on limiting the collection of personal information or on providing notice to consumers regarding each use of information made by the financial institutions. Rather, the focus is on ensuring that personal information is used only for appropriate purposes and that the use of personal information in areas of particular consumer sensitivity, such as sharing of personal information with non-affiliated third parties, are limited where appropriate or subject to consumer choice. The GLBA and FCRA are two examples of laws regulating the financial sector that have struck the delicate balance between regulation and innovation.

Gramm-Leach-Bliley Act

The GLBA is one of the cornerstones of U.S. law that protects consumer financial privacy. The GLBA includes detailed and comprehensive limitations on the ability of financial institutions to share their customer information with nonaffiliated third parties. For example, the GLBA prohibits a financial institution from sharing personal information relating to a customer with a nonaffiliated third party, unless the institution has provided the customer with a copy of its privacy notice and an opportunity to opt out of sharing.[1] 15 U.S.C. § 6802(a). This opt-out right allows consumers, for example, to prevent financial institutions from sharing their information with nonaffiliated third parties that would use the information to market to the consumers. Nonetheless, the statute includes sensible exceptions to this limitation that take into account appropriate and necessary sharing of information, including, for example, to process transactions requested by consumers, for third parties to perform services, to prevent fraud, for risk control, to comply with legal obligations, to comply with subpoenas and summonses, and to respond to judicial process. *See* 15 U.S.C. § 6802(e).

Moreover, the requirement that a financial institution provide its customers with a privacy notice is not a one-time disclosure. Instead, a financial institution must provide its customers with a copy of its privacy notice initially at the time of establishing the customer relationship and then not less than annually thereafter during the course of that relationship. 15 U.S.C. § 6802(a). In another example of Congress and regulators updating the financial privacy laws over time, the federal agencies responsible for enforcing the GLBA, recently issued a model privacy notice that financial institutions may use. *See* 74 Fed. Reg. 62,890 (Dec. 1, 2009). The model was developed over the course of five years, in which the agencies conducted extensive qualitative and quantitative testing with consumers. The agencies' goal was "to identify barriers to consumer understanding of current privacy notices and to develop an alternative . . . that consumers could more easily use and understand." *Id*. at 62,893. As a result, the financial regulators have gone to great lengths to develop a model privacy notice that they believe is understandable. In so doing, the financial regulators appear to have reaffirmed their belief that a properly tailored notice that is given at the inception of the relationship and annually thereafter is appropriate and strikes the right balance.

The GLBA is not limited to the privacy of financial information; it also addresses the security of such information. In this regard, the GLBA requires that each financial institution implement a comprehensive, written and risk-based information security program that is designed to safeguard customer information. Specifically, a financial institution must develop, implement, and maintain a written, comprehensive information security program that includes administrative, technical, and physical safeguards that are designed to protect the financial institution's customer information. *See*, *e.g.*, 12 C.F.R. pt. 30, App. A (OCC). These safeguards extend to all handling of customer information by a financial institution. Moreover, the federal banking agencies require that banks also implement programs to respond to security incidents involving customer information, including notifying customers where appropriate. *Id.*

[1] It is important to note that the scope of the information to which this privacy protection extends is not limited, but is in fact quite broad. Specifically, the GLBA applies with respect to personally identifiable information that a consumer provides to a financial institution, that results from a transaction with, or a service performed for, a consumer or that is otherwise obtained by a financial institution. 15 U.S.C. § 6809(4).

Fair Credit Reporting Act

The FCRA was enacted in 1970 to address a specific concern—dissemination of incorrect consumer credit reports. In this regard, the FCRA regulates, among other things, the disclosure of credit report information by the consumer reporting agencies that aggregate this information and the use of this information by businesses, including, for example, financial institutions (*e.g.*, banks, insurance companies, and broker-dealers), utilities, landlords, and employers. Nonetheless, the FCRA begins with the express premise that the availability of fair and accurate credit report information is critical to the U.S. economy; stating specifically that the "banking system is dependent upon fair and accurate credit reporting." *See* 15 U.S.C. § 1681. For this reason, the FCRA permits the use of credit report information without consumer consent, but imposes strict limitations on who may obtain credit report information and the purposes for which the information may be used (*i.e.*, a narrow and statutorily defined set of uses, including, for example, determining a consumer's eligibility for credit, insurance, or employment). *See* 15 U.S.C. § 1681b(a). Moreover, the FCRA includes robust mechanisms to ensure that this information is accurate. These mechanisms include requirements that consumers be provided with access to information that is maintained and disseminated about them and the right to respond to information they believe to be inaccurate. *See, e.g.*, 15 U.S.C. §§ 1681g, 1681i, 1681m, 1681s-2. Among other things, the FCRA provides that, if a consumer suffers an adverse action based on credit report information (*e.g.*, a denial of credit, insurance or employment based on a credit report), the entity taking the action is required to notify the consumer of the action, identify the consumer reporting agency that provided the information and provide the consumer with a right to a free copy of that information. *See* 15 U.S.C. § 1681m(a). Consistent with its purpose, the FCRA provides consumers with the ability to limit the sharing and use of credit report information. *See* 15 U.S.C. § 1681a(d)(2)(A)(iii).

It is important to note that, in crafting the financial privacy laws, Congress and the regulators have struck a balance. In their judgment, every law need not provide the same rights and obligations. In some laws, such as the FCRA, access and correction rights are provided to ensure that information is accurate. In certain instances, the regulators have determined that other means of providing transparency and the opportunity for correction are appropriate (*e.g.* the issuance of periodic statements). Just as there is not one right answer for notice across every sector and every medium, so too lawmakers and regulators must have flexibility in determining which rights and obligations are appropriate for different situations.

Federal Agencies Examine and Enforce Compliance with Financial Institutions' Privacy Obligations

As indicated above, the GLBA and the FCRA comprise only two of the important financial privacy laws with which financial institutions must comply. In this regard, it is important to highlight that financial institutions are subject to a robust and mature regulatory model that is designed to ensure that financial institutions comply with their privacy obligations and with their publicly stated policies and procedures, including, for example, their GLBA privacy notices. Financial institutions have an existing and long-standing legal and regulatory oversight structure relating to privacy. In this regard, financial institutions are subject to detailed and rigorous examination and supervision by their functional regulators with respect to the various privacy requirements and limitations to which they are subject.

The following example of the examination and enforcement structure for national banks gives a sense of this regulatory oversight. Pursuant to the National Bank Act ("NBA"), the Office of the Comptroller of the Currency ("OCC") charters, regulates and supervises all national banks. The NBA directs the OCC to "examine every national bank." 12 U.S.C. § 481. The NBA further provides the OCC with the power "to make a thorough examination *of all the affairs* of [a national] bank." *Id*. (emphasis added). As a result, when an OCC examiner examines a national bank for compliance with, for example, the privacy obligations of the GLBA and the FCRA, the examiner will review the bank procedures designed to comply with its obligations. Moreover, the examiner will review the institution's privacy notice, its information security program, its incident response program and its FCRA affiliate sharing and affiliate marketing notices and related documentation.

If a particular harm is perceived with respect to the use of information collected over the Internet, it would be appropriate to craft specific oversight, regulation or legislation designed to address that harm, rather than create omnibus legislation that would supplant the sectoral system that has worked well. Financial institutions are required by federal law, including, for example, the FCRA and GLBA, to have robust and well-documented policies and procedures relating to the privacy and protection of personal information. These laws have been the subject of congressional and regulatory debate and refinement over the past 40 years. Because these existing financial privacy laws are effective and strike the right balance between transparency and efficiency, they should not be abandoned or replaced. If the decades worth of refinement that has gone into crafting these privacy protections is abandoned or replaced in favor of a new model, the significant costs that would be imposed on financial institutions to revise their privacy practices and disclosures would likely far outweigh any limited benefit.

A Use-Based Approach Runs the Risk of Harmful Unintended Consequences

Commerce's Notice suggests that a use-based approach may be considered as an alternative to the notice and choice model. A use-based approach is particularly difficult to implement by decentralized organizations that interact with consumers and customers through multiple and diverse platforms, channels, and venues and, therefore, needs careful consideration.

It is not clear that the use-based system that Commerce references in its Notice is a true alternative to a notice and choice system. For example, the proposed use-based approach appears to simply "move" the trigger for notice and choice from the time of collection to the time of use. As posited by Business Forum for Consumer Privacy, the use-based approach continues to rely on notice and choice, but rather than provide the notice and choice at the time of collection, notice and choice are provided for nearly each new use.

Moreover, to the extent that a use-based model is considered, it should take into account consumer expectations. In this regard, many uses of personal information should not result in notice. For example, if a bank or its service provider uses its customer's personal information in order to prepare and mail the customer her monthly statement, notice should not be required. This notice would not be meaningful to the customer. Rather, when a consumer opens a checking account, she not only expects but wants her bank to use her information to provide her with important information regarding her account. Similarly, notice should not be required for

other necessary and important uses, such as to prevent fraud, for risk control and to comply with legal requirements.

Notifying the customer of such use will likely result in over-notification which would cause the customer to overlook the notices that really matter. If a bank were required to provide notice for nearly every use of information, not only would it be extremely difficult to implement, but its customers might well receive more than a hundred notices a year (from the bank alone) to take into account all the various legitimate and appropriate bank uses of information, *e.g.*, to verify customers' identities, underwrite applications, process transactions, prepare and provide monthly statements, ensure funds are available, route customer service calls, prevent fraud, and perform credit risk analysis. Needless to say, consumers over time begin to ignore similar and frequent notices that they receive. If a consumer receives nine notices of a business use of her information that are consistent with the service she has requested (*e.g.*, to process her transactions), she is not likely to focus on the tenth notice. Moreover, to the extent that consumers actually try to make sense of this plethora of notices, it is unlikely that they would make any meaningful privacy decisions based on those notices. Under the use-model, consumers would be literally inundated and overwhelmed with notices from hundreds of businesses nearly every time there is a new use of the information. As a result, Commerce should be cognizant of over-notification and the diminution to the value of notification that such over-notification causes.

The sectoral approach is appropriate because it focuses on limiting inappropriate uses of information and protecting particularly sensitive types of information. If there is an unaddressed issue, the government should determine if particularly sensitive privacy interests of individuals are not otherwise being sufficiently protected and then should intervene only in a way that is narrowly tailored to protect those interests. There are legitimate concerns that a use-based model cannot be narrowly tailored and crafted in a similar way.

Identifying and Fixing the Internet Problem

No matter what type of approach is ultimately adopted with respect to the Internet, one must begin by identifying the privacy interests that are not being sufficiently protected in the online world. After identifying the "problem," consistent with the U.S. approach to regulating privacy described above, a solution that is narrowly tailored to protect those interests should be identified; it is not necessary to adopt an omnibus, one-size-fits-all privacy "solution" that would stifle innovation and increase compliance costs for business. In considering these issues, it may be found that there are varied solutions. In the past when Congress perceived a specific type of information required protection (*e.g.*, information about children or genetic information) and when Congress viewed certain uses of information as inappropriate (*e.g.*, discrimination), Congress has a proven track record of enacting legislation to address the specific issue in a narrowly tailored fashion.

In the end, a one-size-fits-all approach that requires notice at the point of collection or for each use would likely prove counterproductive, because consumers would literally be overwhelmed with notices by hundreds of companies. Instead, as indicated above, the federal government should continue to support a sectoral model and should remain committed to ensuring personal privacy through a variety of means that also reflect its deeply rooted tradition of enhancing the

free flow of information and avoiding overly broad regulation and its unintended, but harmful, consequences.

Moreover, the government should be cognizant of the privacy laws that are currently in place, including the comprehensive protections that federal law provides for consumer financial information. The various financial privacy laws are working as intended, balancing consumer privacy interests with the legitimate and appropriate needs of financial institutions for access to information and the actual business realities of how financial institutions operate. There is no need to abandon or replace this comprehensive scheme of financial privacy laws that has been tailored by Congress and financial regulators over decades to protect consumers' financial privacy because of particular issues with respect to the Internet.

* * * *

We appreciate the opportunity to comment on this important matter. If you have any questions concerning these comments or if we can otherwise be of assistance in connection with this matter, please do not hesitate to contact me.

Sincerely,

Mark Schuermann
Senior Vice President for Government Relations
Financial Services Forum