



January 28, 2011

By Electronic Delivery

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

Re: “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.”

Ladies and Gentlemen:

This comment letter is submitted by the Financial Services Forum (the “Forum”) in response to the Department of Commerce (“Commerce”) Internet Policy Task Force’s report “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,” issued on December 16, 2010. The Forum appreciates the opportunity to comment on the issues and preliminary recommendations of this important report.

The Forum is a non-partisan financial and economic policy organization comprising the chief executives of 20 of the largest and most diversified financial institutions with business operations in the United States. In this letter, the Forum addresses those issues that are of particular importance to financial institutions.

The Proposed Framework includes policy recommendations with respect to privacy law and policy. Our comments on the Proposed Framework reflect our unique experience with the United State’s sophisticated financial privacy regime.

At the outset, we note that Commerce should not propose a shift of this country’s privacy regime toward an EU approach. Such a shift would be harmful to American business and American consumers. The U.S. and EU privacy regimes are based on fundamentally different cultural premises. Because of its experiences during World War II, the EU model begins with the premise that a wide array of information *cannot* be collected, used and transferred (except under limited circumstances). Conversely, the U.S. model, grounded in the First Amendment and the fundamental value of free speech,, begins with the premise that most information *can* be collected, used and transferred (except under limited circumstances).

The federal government should continue to support the U.S. approach to privacy, and to the extent that the current privacy dialogue is driven by a concern for a perceived particular harm, we believe that the most appropriate approach would be to craft specific requirements to address that harm. To instead engraft the EU approach on the U.S economy would be a

paradigm shift that is inconsistent with U.S. values, is unworkable, and would hinder U.S. economic growth, rather than promote it. If the federal government nevertheless seeks to adopt new broad-based requirements for the rest of the economy, we believe that the government should look to and ultimately follow the financial privacy framework particularly GLBA. This approach is established in the U.S., where there is experience with how it works.

In any event, with respect to financial institutions, we agree that there is no need to abandon, replace or add an additional layer of substantial regulation to the comprehensive scheme of privacy laws that has been tailored by Congress and regulators over decades to protect consumers' privacy.

The innovative and dynamic information economy that has developed in the U.S. is in part due to the information policies and practices that are in place in the U.S. that allow for the free collection and flow of information. Moving the entire U.S., or any part of our economy, to a more restrictive information collection/use regime would stifle many companies and thwart innovation.

EXECUTIVE SUMMARY

I. Commerce Should Maintain the U.S. Approach to Privacy Rather than Moving Closer to An EU Approach

We believe that the federal government should continue to support the U.S. approach to privacy, which is customized to address specific types of harm, rather than adopting an omnibus approach and moving closer to the EU. If, however, the federal government ultimately chooses to adopt new broad-based requirements, the government should use the same approach already in place for financial institutions under the financial privacy framework, particularly GLBA. 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 for appropriate purposes and that the use of personal information in areas of particular consumer sensitivity are limited where appropriate. The GLBA also strikes the delicate balance between regulation and innovation subject to sensible exceptions that take into account appropriate and necessary sharing of information.

The current privacy dialogue is driven by a concern with a perceived particular harm. The most appropriate approach, however, would be to craft specific privacy requirements designed to address that harm. It would be ill advised to create omnibus requirements or legislation. We believe that there would be severe unintended consequences if Fair Information Practice Principles ("FIPPs") similar to the EU are established across the U.S. economy, across all industry sectors or relating to all type of personal data. Where the government believes that it 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.

In any event, with respect to financial institutions, there is no need to add an additional layer of substantial regulation to a comprehensive set of financial privacy laws that has worked well in this country for nearly half a century.

II. Commerce Should Limit the Scope of Its Proposed Framework

As Commerce proceeds, we urge it to carefully consider the scope of all aspects of its proposal, even the seemingly mundane. We believe that the Proposed Framework is too broad and would have unintended consequences that would be far reaching. Specifically, while there would likely be other additional unintended consequences, we highlight just some areas and we believe that any framework ultimately proposed by Commerce should: (1) apply only to consumer-purpose data; (2) apply only to online data; (3) not apply to publicly available data; and (4) exempt service providers from direct applicability.

III. The FIPPs Would Impose Significant Burden Without Attendant Consumer Benefit

An omnibus approach encompassing a set of FIPPs would place a real and significant burden on all companies that process personal data, online or off, without addressing real harm or providing significant corresponding benefit to consumers. For example, purpose and use limitations are inconsistent with the U.S. approach, notice should be narrowly tailored and choice should be limited to where it matters. In addition, costs associated with broad access and correction are significant.

IV. Commerce Should Discourage Restrictions on the Movement of Data Globally

Many of the laws that restrict cross border data transfers are ill suited for today's globally interconnected world in which data flows in multiple directions simultaneously and national borders become meaningless. In contrast, we believe that an appropriate accountability model has the potential to offer uniform and consistent protections without regard to the jurisdictions to which the data may travel. In this regard, accountability is not a monolithic concept, but rather accountability can be established through multiple paths including with a sectoral privacy regime, such as that to which U.S. financial institutions are currently subject.

V. Commerce Should Support A National Standard Security Breach Notification Law

We support a federal data breach notification law that preempts state laws. Disparate state laws that impose myriad actual or potentially conflicting notification requirements that result in high costs, inordinately complex compliance obligations and do not serve the public interest. A common national standard with an appropriately tailored, risk based notice trigger, would avoid creating confusing and conflicting obligations and promote the public interest.

DETAILED ANALYSIS

I. Commerce Should Maintain the U.S. Approach to Privacy Rather than Moving Closer to An EU Approach

We believe that the federal government should continue to support the U.S. approach to privacy, which is targeted to address specific types of information that warrant protection from specific harms related to the use of consumer information. If the federal government nevertheless ultimately chooses to adopt new broad-based requirements, we believe that the

government should use the same approach already in place for financial institutions under the financial privacy framework, particularly the Gramm-Leach-Bliley Act (“GLBA”). If the federal government adopts new privacy requirements or legislation, we believe that financial institutions should not be subject to an additional layer of regulation, but should continue to be subject to the GLBA and other existing privacy requirements already imposed under federal law. 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 for appropriate purposes and that the use of personal information in areas of particular sensitivity, such as sharing of personal information with non-affiliated third parties for marketing purposes, are limited where appropriate. The GLBA also strikes the delicate balance between regulation and innovation subject to sensible exceptions that take into account appropriate and necessary sharing of information. Congress has adopted a well thought out approach with respect to the privacy of consumer financial information. As a result, Congress has enacted a number of statutes that are narrowly tailored to protect specific consumer privacy interests, but that also take into account both the legitimate need of financial institutions for free flow of information and the business realities of how such institutions operate. Existing federal protections for consumer financial information are robust and include, for example, privacy protections in the GLBA, the Fair Credit Reporting Act (“FCRA”), the Electronic Funds Transfer Act, the Equal Credit Opportunity Act, and the Fair Credit Billing Act.

Financial institutions are already subject to a detailed array of privacy obligations and limitations with respect to consumer financial information. Moreover, 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 involving affiliated entities within which many, if not most, financial institutions operate.

A. Overview of Financial Privacy Framework

The financial privacy laws have been the subject of rigorous Congressional and regulatory debate and refinement over the past 40 year, dating back to the enactment of the FCRA in 1970. Over time, where Congress and federal regulators have identified new issues requiring additional or different privacy protection, they have stepped in and provided that protection. We believe that 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. As a result, there is no need to abandon, replace or add an additional layer of substantive regulation on top of this comprehensive scheme of financial privacy laws that has been tailored by Congress and financial regulators over decades to protect consumers’ financial privacy. Instead, Commerce should use this approach as a model.

i. The Gramm-Leach-Bliley Act

The GLBA is the cornerstone 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, while permitting some

sharing with affiliated entities common in financial services companies. 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 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 the third-party sharing limitation that, as previously stated, 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.²

The GLBA is not limited to the privacy of financial information. The statute also addresses the security of such information. In this regard, the GLBA and accompanying regulations 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.³ These safeguards extend to all handling of consumer 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.⁴

ii. The Fair Credit Reporting Act

The FCRA is another significant U.S. financial privacy law. The FCRA was enacted in 1970 to address a specific concern; namely, the dissemination of consumer credit reports that included incorrect information. 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, among others, financial institutions (*e.g.*, banks, insurance companies, and broker-dealers). 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.”⁵ For this reason, the FCRA permits the use of credit report

¹ 15 U.S.C. § 6802(a). 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). This includes, for example, the varied types of information provided by consumers on applications, information obtained by financial institutions from third parties, such as consumer reporting agencies, and information generated by financial institutions regarding accounts and transactions.

² *See* 15 U.S.C. § 6802(e).

³ *See, e.g.*, 12 C.F.R. pt. 30, App. A (OCC).

⁴ *Id.*

⁵ *See* 15 U.S.C. § 1681.

information without consumer choice, but imposes limitations on who may obtain credit report information and the purposes for which the information may be used.⁶

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.⁷ In addition, the FCRA provides consumers with the ability to limit the sharing and use of credit report information where there is potential for consumer harm.⁸

iii. The Dodd-Frank Act

More recently, Congress has broadened the financial privacy requirements in connection with recent financial reform legislation. Specifically, the Dodd-Frank Act directs the new Consumer Financial Protection Bureau (“CFPB”) to prescribe rules that require a financial institution to make available to a consumer, upon request, information in the institution’s control or possession concerning the consumer financial product or service that the consumer obtained from the institution.⁹ This would include information relating to transactions and the account, including costs, charges and usage data. The Act, however, does include some relevant exceptions to this “access” requirement, including for any information collected by a financial institution for the purpose of preventing fraud or money laundering and any information that a financial institution cannot retrieve in the ordinary course of business.

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 credit report 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).

B. The U.S. Approach to Privacy is More Appropriate than an Omnibus Approach

To the extent that the current privacy dialogue is driven by a concern with a perceived particular harm, we believe that the most appropriate approach would be to craft specific privacy requirements designed to address that harm, rather than create omnibus requirements or legislation that would supplant a sectoral system that has worked well in this country for nearly a half century. Specifically, if the federal government seeks to adopt new broad-based requirements, then as previously stated and further described below, we believe that the government should follow the financial privacy framework.

In many respects, the Framework proposed by Commerce is grounded in establishing FIPPs across the U.S. economy and applying them in a fashion similar to that of the EU. We believe that there would be severe unintended consequences of requiring FIPPs compliance in such a fashion for all companies, across all industry sectors, relating to all types of personal data. As

⁶ See 15 U.S.C. § 1681b(a).

⁷ See, *e.g.*, 15 U.S.C. §§ 1681g, 1681i, 1681m, 1681s-2.

⁸ See 15 U.S.C. § 1681a(d)(2)(A)(iii) and 15 U.S.C. §1681s-3.

⁹ 12 U.S.C. § 5533.

a result, we believe that Commerce should not promote making FIPPs mandatory. To impose such requirements, even as currently contemplated by Commerce, would result in high ongoing compliance costs on virtually all companies that process personal information (and that actually set out to comply), without, in many cases, providing any real benefit to consumers. In addition, generally applicable rules that impose unnecessary burdens, such as over-notification, will adversely affect innovation, limit the choices provided to consumers, and make it more difficult for U.S. companies to compete against their global counterparts.

The U.S. model for regulating business practices is deeply rooted in a recognition that overly broad regulation adversely affects companies and, in turn, consumers and the economy. This has led to a valid reluctance to regulate business practices absent a demonstrated need. As a result, Congress tends to adopt legislation to address specific issues, all while protecting important national interests, whether those be related to addressing risk, fraud, protecting our nations' infrastructure or otherwise 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).

This approach has historically and notably been followed with respect to consumer privacy. Specifically, the U.S. has concluded that an omnibus or "one-size-fits-all" legislative approach lacks the precision needed to avoid interfering with the benefits provided by 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. has focused on significant privacy interests, relating to particularly sensitive types of information (such as financial information and information about children) or on inappropriate information uses (such as abusive e-mailing). Accordingly, the landscape of U.S. privacy law is broad and varied,¹⁰ focused on protecting sensitive information and limiting inappropriate uses of information, while ensuring privacy and enhancing deeply rooted traditions, such as free information flows. While there may be additional areas where regulation may be appropriate, Commerce should not assume that omnibus privacy regulation

¹⁰ The following are examples of U.S. privacy laws that protect important consumer privacy interests: Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq.* (personal information collected from children online); Telephone Consumer Protection Act, 47 U.S.C. § 227 (privacy from certain telephone calls); CAN-SPAM Act, 15 U.S.C. § 7701 *et seq.* (privacy with respect to commercial e-mail); Cable Communications Policy Act, 47 U.S.C. § 551 (personal information collected by cable companies); Customer Proprietary Network Information, 47 U.S.C. § 222 (personal information collected by telephone companies); Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.* (computer information and the content and other information relating to individuals' communications); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (credit report information and information shared among affiliated companies); Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* (information relating to customers of financial institutions); Title II of the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191 (health information); Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq.* (driver's license information); 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 (information about sex, race, color, religion and marital status); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (student information); Employee Polygraph Protection Act, 29 U.S.C. § 2001 *et seq.* (employee polygraph information); Employee Retirement Income Security Act, 29 U.S.C. § 1025 (employee retirement information); 39 U.S.C. § 3623 (mail); Fair Debt Collection Practices Act, 15 U.S.C. § 1692 *et seq.* (communications by debt collectors); and, Video Privacy Protection Act, 18 U.S.C. § 2710 (video rental information).

or legislation that treats all data for all purposes in precisely the same or even a similar manner is a panacea.

Where the government believes that it 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 (*e.g.*, the approach used in the various existing federal privacy statutes). In fact, we do not believe that any significant consumer privacy harm has been identified that would necessitate omnibus privacy requirements, as opposed to narrowly tailored privacy requirements to address certain identified harms. As discussed in greater detail below, we believe that Commerce should reconsider its approach and follow the U.S. financial privacy framework, which captures the intent of the FIPPs, but in an appropriately tailored manner.

II Commerce Should Limit the Scope of Its Proposed Framework

As Commerce proceeds, we urge it to carefully consider the scope of all aspects of its proposal, even the seemingly mundane. As described below, we believe that the Proposed Framework is too broad and would have unintended consequences that would be far reaching and harmful.

A. The Proposed Framework Should Apply only to Consumer-Purpose Data

As noted above, the Framework covers “commercial data privacy.” In many places throughout the Framework and the accompanying report, there are references to “consumers,” which implies that Commerce intends for the Framework to apply to information obtained from an individual in connection with personal, family, or household purposes (*i.e.*, a consumer-oriented interaction, as opposed to a business transaction). There are also references, however, to “individual” privacy, which could be read to cover personal data beyond that collected from a consumer. We believe that Commerce should define “commercial data privacy” to explicitly exclude information collected from or about an individual for purposes other than personal, family, or household purposes. For example, we believe that information about an individual in her capacity as a representative of an entity and used in the context of a business-to-business relationship should not be covered.

The use of business information for business purposes does not adversely affect individuals’ privacy rights. Individuals acting in their professional capacity, and their employers, expect and want their information (including the contact information found on business cards and company websites) to be shared easily with others. Indeed, individuals usually disclose such contact information for the purpose of making such information available to be freely used. Imposing privacy obligations with respect to this data would restrict the sharing of information that permits organizations to maintain their everyday operations and would consequently significantly hamper the flow of business operations and business-to-business communications, and impede economic activity, with little or no corresponding privacy benefits.

These and other FIPPs-imposed requirements would be extremely time-consuming, expensive, and burdensome with respect to such data. Restricting its use would impede economic activity without providing any corresponding meaningful privacy protection to individuals if

such information does not pertain to their personal, home or family lives. For these reasons, extending the Proposed Framework's protections to such information is unnecessary, would be wasteful and unduly interfere with everyday commerce.

There is federal precedent for taking such a view, including, significantly, the GLBA. As discussed herein, the GLBA extends privacy protections to the consumer customers of financial institutions. In this regard, the statute specifically defines a "consumer" as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes"¹¹ Similarly, the OCC and the other regulators implementing the GLBA privacy provisions expressly provided that the GLBA privacy regulations apply "only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes from the [covered] institutions."¹² Moreover, the OCC's rule states that it "does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes."¹³ Similarly, we believe that application of all the FIPPs to business information imposes significant burdens for little or no benefit and should not be required.

B. The Proposed Framework Should Not Apply to Offline Data

As drafted, it is not entirely clear whether Commerce intends for the Proposed Framework to apply only to personal information collected online or also to apply to information collected offline. While the very title of the Proposed Framework (*i.e.*, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework") and many references within it indicate that it is aimed solely at online data, other references, including those generally to "commercial data" could be read to suggest that the intended scope may be broader. We believe that Commerce should limit its scope to online personal information. Any other alternative would dramatically expand the scope of the Proposed Framework. At this stage, a more limited and circumspect approach is appropriate in light of potential unintended consequences, including a very heavy burden of implementation and compliance, especially to smaller businesses, and the apparent absence of meaningful benefit to consumers in many respects.

C. The Proposed Framework Should Not Apply to Publicly Available Information

The Proposed Framework covers "commercial data privacy." There is no indication as to whether this definition extends to publicly available information. It should not. Because such information is already in the public realm, it makes no sense to require businesses to incur the costs of adopting privacy protections for information that is lawfully and freely made available to the general public. The GLBA, for example, has adopted this approach. Specifically, the GLBA excludes information that is "publicly available."¹⁴ When information is already in the public realm, the information is by definition not private.

¹¹ 15 U.S.C. § 6809(9).

¹² *See, e.g.*, 12 C.F.R. § 40.1(b).

¹³ *Id.*

¹⁴ 15 U.S.C. § 6809(4).

D. The Proposed Framework Should Exempt Service Providers From Its Coverage

The Proposed Framework does not address service providers (*i.e.*, entities that process consumer data on behalf of others with no right to use the data for their own purposes). We believe that Commerce should provide that its Proposed Framework does not apply to service providers (whether third parties or affiliates) because the FIPPs almost uniformly are not relevant to the service provider relationship.

Application of FIPPs to affiliates and service providers would cause serious practical difficulties and inefficiencies. For example, because service providers do not have their own relationships with consumers, it would be very difficult for them to provide notice and choice. Any such notice and choice would, moreover, not only duplicate the notice and choice already provided by the company with the relationship to the consumer (that is, the company that has hired the service provider), but it would confuse and surprise the consumer (assuming that it was not completely disregarded) as they have no relationship with the service provider. The company with the relationship to the consumer is in the best position to comply with applicable privacy requirements and would be accountable for compliance by its service providers. Moreover, we believe that this is consistent with consumer expectations.

This approach (*i.e.*, not directly extending FIPPs-like requirements to service providers) is the approach adopted by the GLBA. The GLBA specifically permits a financial institution to disclose customer information to its service providers. Instead of imposing privacy obligations directly on service providers, the GLBA directs financial institutions to prohibit their service providers by contract from disclosing or using customer information other than for the reasons which the financial institutions disclosed the information.¹⁵ Similarly, financial institutions must require their service providers by contract to implement appropriate security measures to protect customer information.¹⁶ These privacy protections apply to the financial institutions, not directly to their service providers.

III.. The FIPPs Would Impose Significant Burden Without Attendant Consumer Benefit

The financial services industry is already subject to robust privacy principles that have been tailored to address information use, safeguarding and disclosure within the financial services context. These principles capture the intent of the FIPPs in a workable and successful manner without hampering innovation or the free flow of products and services, which are beneficial to U.S. consumers. For example, under existing laws, financial institutions maintain administrative, technical, and physical safeguards to prevent against risks of unauthorized access, use, modification, or destruction. In addition, an omnibus approach applicable to the whole economy encompassing a set of FIPPs would place a real and significant burden on all companies that process personal data, online or off, without addressing a real harm or providing significant corresponding benefit to consumers. Unlike the EU, we believe that not

¹⁵ 12 C.F.R. § 40.13(a).

¹⁶ 12 C.F.R. pt. 30, App. B.

all types of data need protection, and not all types of data processing call for regulation. We also believe that the substantial costs – in terms of dollars, manpower and diverted resources – associated with an omnibus framework are not justified, particularly during a time when the economy is recovering from financial instability not seen since the Great Depression and the President’s call for reduced regulatory burdens for businesses. As a result, we believe that Commerce should reconsider application of the FIPPs, as discussed below.

A. Purpose and Use Limitations are Inconsistent with the U.S. Approach

The approach taken by Commerce is more similar to that of the EU, where data cannot be collected, used or disclosed unless there is a legal basis. According to Commerce, use of data should be limited to an identified, relevant purpose. Such an approach is fundamentally inconsistent with the manner in which the U.S. has previously and currently operates, even with respect to its most sensitive data. In the U.S. (as well as most APEC economies), there is a presumption that data can be collected, used and disclosed unless there is a specific prohibition. If there are specific uses that are viewed as harmful (*e.g.*, spam), that can be dealt with based on the harms-based approach rather than limiting all uses to those specifically identified in a notice. Experience with the EU has shown that such a significant change in direction by the U.S. in this area would be wholly impractical and would likely have a significant adverse effect on the day-to-day operations of businesses.

Commerce recommends that companies abide by the FIPPs’ “purpose specification” and “use limitation” principles, which, together, require a company to state the specific reasons for collecting personal information and then permit the company to use the information only as specified. It gives the example of an ISP that wants to collect customer usage records to prepare bills, detect fraud, and settle billing disputes. According to the purpose specification principle, the ISP would state those three purposes in its privacy notice. “The use limitation principle would then enforce the ISP’s commitment to use the personal information it collects *only* to fulfill these three purposes.”¹⁷ Commerce adds to this example by supposing that “company executives have grown concerned with security threats against their network equipment and customers’ computers. The CEO approves a proposal to provide the [personal information] to in-house researchers, so that they can analyze network traffic and develop security countermeasures.”¹⁸ Even more importantly, in Commerce’s view, because the CEO’s proposed use would be contrary to the ISP’s specified purposes and may therefore come at the expense of customers’ privacy, it should not be permitted, even though the use “has the clear potential to bring privacy and security benefits to the ISP and its customers.”¹⁹

The purpose specification and use limitations are similar to those that have been adopted by the EU and would pose a legitimate threat to the interests of consumers and to the day-to-day operations of many companies and could make the effective operation of a business impossible. Companies make many legitimate uses of customer information, as well as many uses that are unlikely to be material to consumers’ decisions to transact with them. Nonetheless, it may be quite difficult to identify, before providing notice, all such legitimate uses of information. However, if a company is unable to do so and therefore fails to provide

¹⁷ Green Paper, p. 38 (emphasis added).

¹⁸ *Id.* at 39.

¹⁹ *Id.*

notice disclosing every such use, according to Commerce's proposal, it would be prohibited from later using the information for a non-disclosed use (absent re-notification and consent), even if such use is legitimate, reasonable, appropriate or even critical to the company's continued operation or in furtherance with national policy goals (e.g., the security of our economic infrastructure). This should not be an appropriate goal of any U.S. privacy regime and would severely impede innovation, which Commerce clearly seeks to avoid.

The application of the purpose specification and use limitation principles as suggested by Commerce also has the practical potential to directly undermine Commerce's concurrent recommendation that privacy policies be simple and clear.²⁰ In the ISP example above, if a company remembered in its initial privacy notice to include a statement that information would be used to protect the company's infrastructure or to prevent fraud, then no new notice or consent would need to be obtained. If the company failed (in the interest of making the notice clear and concise and not unduly long, *i.e.*, actually meaningful to consumers) not to include that obvious legitimate purpose, it would be required to provide a new notice and obtain consent for this "new" use. In order to avoid this potential "re-notification" issue, many companies would appropriately attempt to list every potential hypothetical use (no matter how unlikely or unforeseen). Such a notice would be long and unwieldy and ultimately counter-productive. In fact, the sheer volume of information disclosed and the likely irrelevance of a majority of this information to most consumers likely would cause many to simply ignore and disregard the notice. For those consumers who did try and wade through such a detailed notice, there is a distinct possibility that they would become lost in its content, missing the information that they are likely interested in. This level of detail is exactly what the financial services regulators avoided when they crafted their model privacy form.

B. Notice Should be Narrowly Tailored

We agree with Commerce that consumers are better served by privacy policies that are clear and concise, and we believe that a reasonable approach would be to permit companies the flexibility to describe their data uses via something other than a granular list. In fact, we think that the most effective privacy policy would be one that did not even list the obvious or expected categories of information use. There are many categories of uses and disclosures that are obvious, expected, legitimate, or not potentially harmful to consumers, including, for example, product and service fulfillment, communication with the consumer, first-party direct marketing, internal research and development, risk control and compliance, and protection of the company's interests. While not a comprehensive list, these examples are categories of processing that are necessary and/or legitimate and consistent with the reasonable consumer's expectations. There is no point, therefore, in listing them. Moreover, if they are stripped from the policy, the policy is more likely to provide the consumer with information that is of interest to her. This is exactly the approach followed by the financial regulators in their model GLBA privacy form, which briefly describes a financial institution's "everyday business purposes" and then focuses on various types of sharing of customer information for marketing purposes.

²⁰ *Id.* at 31.

Moreover, the requirement that a financial institution provide its customers with a GLBA 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.²¹ 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.²² The model was developed over the course of five years, in which the agencies conducted qualitative and quantitative testing with consumers. The agencies' stated 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."²³ As a result, the financial regulators have gone to great lengths to develop a model privacy notice that they believe is understandable, a unique challenge that should not be overly simplified, while reaffirming that a properly tailored notice that is periodically provided to consumers is appropriate and strikes the right balance.

Nonetheless, if Commerce's recommendations were to become enforceable, then, by way of example, a covered company would have to provide a notice detailing what information it collects, the purposes for which it uses that information, and with whom it will be shared, at every online and offline point of collection. To do so, a company would have to identify each point of information collection, across all channels in which it, its employees, and agents acting on its behalf collect personal information. This point should not be overly simplified. In fact, this would present a monumental undertaking. For example, if a bank were covered, a bank would need to identify every single type of situation in which it collects information, including, for example, when a consumer speaks with a loan officer to ask a question, whenever a consumer provides information to customer service, when a consumer reports a lost or stolen credit card and when a security guard interviews a witness to an accident at a bank branch.

There are potentially tens of thousands of instances in which information hypothetically could be collected and used by a single company. Assuming that these instances could be identified and listed in a somewhat-clear fashion that is both understandable and meaningful to consumers (an unlikely assumption), these notices then would have to be provided repeatedly through a website, by e-mail, by telephone, and on paper. For companies, such as banks engaged with individuals across various online and offline channels, providing such notice would be impracticable and the costs and challenges would be dramatic and particularly onerous. It is difficult to imagine how some companies could even provide such a notice and how most consumers could actually decipher and understand such a notice. For example, imagine a consumer receiving a privacy "package" in the mail that lists countless hypothetical collection and use scenarios; then, imagine receiving similar privacy packages from a hundred other companies. It is also difficult to imagine what meaningful benefits this would provide consumers, particularly where consumers do not "shop" based on privacy interests.

²¹ 15 U.S.C. § 6802(a).

²² See 74 Fed. Reg. 62,890 (Dec. 1, 2009).

²³ *Id.* at 62,893.

To the extent that notice is required, we believe that companies should be provided with flexibility in terms of when and how they are permitted to provide consumers with any required notices, particularly if the Proposed Framework is extended to personal information collected offline. Specifically, we encourage Commerce to affirmatively state that a company should not be required to provide a consumer with a hard copy of its notice at the point of each offline information collection, such as in a retail outlet, or at a cocktail party or over the telephone. Instead, we recommend that a company have the option of posting a publicly available copy of the notice, such as one posted on its website or a customer service desk in a physical outlet. This approach would not only result in obvious efficiencies, but it would also avoid obstacles to the free flow of information, as a company would not be prohibited from interacting with a consumer before it is able to provide him or her with a copy of its notice.

Under the current GLBA privacy notice structure, banks and other financial institutions incur significant mailing and printing costs each year to provide their customers with annual privacy notices. For example, a large bank holding company may send its customers literally in excess of a hundred million notices each year, at a cost exceeding tens of millions of dollars. If you imagine a scenario in which the Proposed Framework applies to virtually every consumer-oriented business in the country, trillions of notices would be mailed each year (*i.e.*, it is not hard to imagine the average American receiving at least 100 notices a year). The mailing costs alone for these notices would very high, let alone the other costs in connection with the preparation and delivery of those notices, including, for example, legal costs and the diversion of a company's resources. These additional costs to business must not be underestimated and could have a significant impact on new business development and jobs and our ability to compete globally.

C. Choice Should be Limited to Where It Matters

We believe that a company should not have to provide choice with respect to practices that are consistent with the provision of a product or service to the consumer, generally considered legitimate, or otherwise immaterial. According to Commerce, the "individual participation" FIPP provides that companies should, "to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance" of personal data.²⁴ The Proposed Framework does not set out the circumstances under which a company would be required to obtain such consent; however, we urge Commerce to carefully consider this issue.

In particular, and consistent with our recommendations with respect to the disclosures required for privacy notices, we believe that a company should not have to obtain consumer choice for many types of data processing, including the following:

- *Processing that is commonly accepted by the consumer.* For example, a consumer buying a product online will expect that his or her personal information will be used to charge a credit card and deliver the product. She will also understand that the company will use her personal information to communicate about the purchase (*e.g.*, to notify her that the item has shipped or to advise of a delay) and will share it with a delivery company or the U.S. Postal Service so that the product can be delivered. Because these uses are commonly accepted (and implicit in the request for the

²⁴ *Id.* at 26.

product), choice should not be required. Specifically, any consumer choice to limit these disclosures and uses would be fundamentally inconsistent with the consumer's initial request for the product.

- *Processing that is legitimate or immaterial to a reasonable consumer's decision to share his or her data.* Some data uses and disclosures, while not necessarily obvious to consumers, are not only legitimate, appropriate, and important to business operations, legitimate governmental interests and our economy more generally, but also immaterial to a reasonable consumer's decision to share his or her personal data with a company. Accordingly, they should not be subject to consumer choice. They include, by way of example, disclosures to service providers, servicing the consumer's account, internal analytics, internal research and development, fraud prevention, audits, legal compliance, and disclosures to governmental authorities or law enforcement.²⁵ Providing consumers with choice with respect to these types of processing would have significant unintended negative consequences. For instance, internal research and development provide many benefits, such as new or improved products and services. Giving consumers the ability to decline to have their information (such as their feedback or the products they have purchased) used for these purposes would stifle companies' ability to innovate. Similarly, no benefit can come of a consumer's ability to choose whether to have his or her information used for fraud prevention, which provides value for merchants, banks, the consumer, and the financial institution. In fact, U.S. law requires that financial institutions collect and use personal information from their customers for "know-your-customer" and anti-money laundering and anti-terrorist financing purposes, thus providing individuals with choice in this area would be counter productive and would create a direct conflict of obligations.

If these, as well as other types of processing that may not have been expressly described above, are not excluded from the categories of processing over which consumers have specific choice, consumers will be overwhelmed with choices (including about a myriad of potential uses) from the various companies with which they do business, asking them whether or not they agree to multiple data uses and disclosures for which consent should not be necessary, and in fact would be counter productive. Our suggested approach would ensure that consumers are only provided choice when the choice really matters. For example, choice may be appropriate with respect to the disclosure to unaffiliated third party for the third party's marketing activity.

D. The Costs Associated with Broad Access and Correction are Significant

If Commerce's recommendations were to become enforceable, a covered company would have to provide individuals with access to their information and the ability to update and correct it. This requirement would call for the implementation and maintenance of systems to track all personal information held by an organization in a form that is searchable and updateable. The costs associated with this would be significant, even for online companies. For an organization, that still relies heavily on paper and offline collection of data, the cost of

²⁵ The OCC's GLBA privacy regulations provide a useful list of the categories of disclosures that it found to be legitimate and not subject to consumer choice. *See* 12 C.F.R. §§ 40.13, 40.14.

developing such a system would be astronomical. For example, many larger companies are organized by product line, and individuals often interact with multiple business units or across multiple countries. Those business units frequently have separate databases. Thus, if a parent company received an access request, it would require either checking every database of every division or business unit to provide accurate information or it would require significant investment in infrastructure to create a global system that incorporated all data from all business units. In addition, organizations would be required to ensure that they have employees trained and available to respond to access requests. Some industries would have to adopt measures to verify individuals' identities before providing the requested access.

Moreover, in light of the growing issue of identity theft, specific procedures would need to be developed to verify the identities of individuals requesting access. In addition, the need to match access requests with information relating to consumers would likely cause many companies that do not currently collect sensitive identifiers, such as Social Security numbers, to do so.

E. Privacy Impact Assessments (“PIAs”) Should Not be Mandated

We believe that PIAs should not be mandated and that the government should not require that PIAs be published. In some instances, PIAs may provide a company with a valuable internal tool to identify and mitigate risks that certain practices and technologies may pose to privacy. While Commerce may consider encouraging their use, it should not be mandated. It does not make sense to conduct a PIA for every new practice or technology; rather, a PIA is likely only to be appropriate when there is a serious risk of negative and unknown consequences to privacy. For example, when the consequences are already known and certain measures and procedures are commonly applied to address them, a PIA is unnecessary. The frequency and use of PIAs should be determined by the company itself so that it does not become another costly and unnecessary administrative burden.

In addition, imposing a requirement to make PIAs public would discourage their use and possibly compromise their integrity. First, bad actors could access and use a company's PIA to exploit the weaknesses in its security operation (as described in the PIA itself). Second, if PIAs are made public, companies would be discouraged from making honest assessments to identify risks and creating risk mitigation techniques. The public-disclosure aspect, however, is likely to create a disincentive to innovation and the creation of new technologies. Their value as a powerful internal tool enabling a company to manage and mitigate its risks would be severely undermined. For example, requiring public disclosure of PIAs would present a real risk of requiring the disclosure of proprietary business information, including trade secrets, which would expose a company to competitive disadvantages and deter innovation. In the banking context, the government recognized the need to maintain confidentiality of bank examinations for purposes of encouraging full and complete disclosure and evaluation and to protect the banking system. Confidentiality of internal assessments is essential to their value as a risk mitigation tool.

IV. Commerce Should Discourage Restrictions on the Movement of Data Globally

Citing the EU-U.S. Safe Harbor and the APEC Pathfinder project as appropriate models, Commerce is seeking to establish and promote global “interoperability” by creating another

form of the EU “adequacy” approach. Some of the growing number of countries around the world that have adopted omnibus privacy laws also restrict the cross border transfers of personal data, and some countries restrict the transfer of data to countries that do not provide an “adequate” level of protection. An “adequacy approach” requires global organizations to put in place complex and overly bureaucratic programs and arrangements that, particularly given their cost, do little to provide meaningful privacy protections, and instead, complicate and add costs to the use of personal data for legitimate business purposes. In the EU, companies have expended sometimes significant resources to implement and then maintain model contracts programs, which are filed and updated, but have no practical effect or benefit to individuals.

Many of the laws that restrict cross border data transfers that are based on the EU adequacy model, are ill suited for today’s globally interconnected world in which data flows in multiple directions simultaneously and national borders become meaningless. The adequacy model of the EU has been fairly criticized as it appears to require “equivalence” rather than “adequacy,” thereby failing to take into consideration different legal and cultural operation mechanisms in other countries. This results in a hodgepodge of contractual arrangements or consent obligations that do little to provide meaningful privacy protections.

The APEC Framework was designed to be a model for countries that do not have privacy laws (as an alternative to the EU’s data privacy regime) and to facilitate cross border data transfers by eliminating unnecessary restrictions. It now appears that instead of facilitating cross border transfers, the APEC Pathfinder Project is creating a new free-standing, detailed and prescriptive data privacy regime that Commerce is seeking to put in place across the U.S. economy, which is inconsistent with the way privacy principles operate in the U.S. and would frustrate the free flow of commerce.

The new comprehensive international regime supported by Commerce in APEC as well as the proposed new domestic data privacy Framework proposed by Commerce, would apply to all companies in the U.S., across all industry sectors, and relate to all types of personal data. Such an approach undercuts the stated goals of U.S. policy and deviates from the original intent of the APEC cross border initiative in a manner that would impose unnecessary and onerous new burdens on organizations in the U.S., and go well beyond the current obligations on other APEC member economies and, in some instances, the EU, and impose unnecessary burdens on global commerce in general.

Such an outcome is unnecessary and harmful both domestically and internationally. The APEC Framework recognized that nations may make different choices and have different approaches regarding the protection of certain information even when they agree on the broad principles that apply. For example, based on the sensitivity of the data, the U.S. has chosen to provide more protection for customers of financial institutions and health care providers than for other types of customers and data. It also allows organizations to provide information to the government for a variety of purposes. The APEC Framework recognizes that these choices should be honored, rather than overridden. The APEC Framework simply requires that local law be “broadly compliant” with the APEC Principles. As the APEC Framework states, “[it] is not intended to impede governmental activities authorized by law when taken to protect national security, public safety, national sovereignty or other public policy” and “[i]n view of the differences in social, cultural, economic and legal backgrounds of each member

economy, there should be flexibility in implementing these Principles.”

Instead, the approach emerging within APEC is to require organizations to demonstrate compliance with the APEC Privacy Principles at the organizational level, rather than at the country level. While we question whether this approach will work for many organizations operating in other sectors, it is also problematic for organizations that are already subject to comprehensive sectoral regulation. For example, many of the APEC economies already regulate financial institutions with respect to privacy and data security, and it would be more efficient for these economies rather than individual companies to demonstrate broad compliance with the APEC principles at the economy level. Organizations could then demonstrate that they are in compliance with their home economy’s laws through flexible existing means. The APEC principles should provide a country/governmental standard that organizations can implement as appropriate. The APEC principles should not govern organizations directly, bypassing the country/governmental level altogether.

Despite the adoption of the APEC Framework and the ongoing efforts of the Pathfinder project, more economies in the region have opted to enact a style of privacy legislation which is likely to create barriers to cross border transfers. Prior to the adoption of the APEC Framework in 2005, eight of the twenty-one economies in APEC had either omnibus or sectoral privacy laws in place (*i.e.*, Australia, Canada, Chile, Hong Kong, Japan, Korea, New Zealand, and the United States). None of these eight countries had rules that prohibited transfers to countries that did not provide adequate protection. After the adoption of the APEC Framework and the ongoing implementation of the Pathfinder project, four more countries (Malaysia, Mexico, Russia, and Taiwan) adopted omnibus privacy laws and three of these four adopted laws that either prohibit transfers to countries that do not provide adequate protection or give the regulator the ability to impose such restrictions, contrary to intent of the APEC Framework. Two more APEC economies (the Philippines and Thailand) are contemplating omnibus privacy laws that would also restrict cross border transfers. Thus, rather than facilitate cross border transfers within a compliant community, the APEC Framework has instead encouraged countries with no data protection laws to adopt restrictive laws that impose barriers to data flows.

In contrast, an appropriate model based on the current U.S. financial sector approach to cross border data has the potential to offer appropriate protection irrespective of the jurisdictions to which the data may travel. Rather than conduct an assessment of how an organization or economy measures up to a set of principles or FIPPs, which is an approach similar to that required by the EU, an alternative approach would be to determine if there are sufficient enforcement mechanisms in place in the home jurisdictions of responsible organizations in the event that the organizations fail to live up to their data protection obligations, or if they act unfairly based on the home jurisdiction standards. As discussed above, they apply to banks wherever they may handle such consumers’ financial information. That is, the U.S. privacy laws applicable to financial institutions do not differentiate based on where a bank may handle that consumer financial information (*e.g.*, within the U.S. or outside of the country).

Moreover, these obligations apply to banks even when the banks rely on third-party service providers to handle information on their behalf (even outside of the country).²⁶

Organizations need an appropriate solution to the existing cross border transfer issue. Simply adopting the EU adequacy approach, which has been the subject of much criticism, is not the solution. Such an approach will only add yet another conflicting law to the growing number of data privacy laws that currently exist and will result in additional cost and bureaucracy on organizations without a corresponding benefit to consumers. Consequently, Commerce should consider augmenting the Pathfinder initiative with a privacy and data security concept embodied in existing U.S. law rather than an “interoperability” that is really another form of “adequacy”.

V. Commerce Should Support A National Standard Security Breach Notification Law

We support a federal data breach notification law that preempts state laws. Disparate state laws that impose myriad actual or potentially conflicting notification requirements that result in high costs, inordinately complex compliance obligations and do not serve the public interest. These effects are frequently felt by banks that are subject to GLBA security breach notification requirements, but that are not uniformly exempted from state security breach notification laws. A common national standard would avoid creating confusing and conflicting obligations and promote the public interest.

In this regard, the goal of a notification law should be to define a reasonable and balanced notification trigger that ensures that individuals receive notice when there is a significant risk of substantial harm, but that does not result in over-notifying and desensitizing individuals to these important notices. The primary purpose of providing notices to individuals is to enable them to take steps to mitigate the risk of substantial harm that might result from a breach. Thus, any individual notification requirement should be risk-based. Notification should focus on situations where there is a significant risk that identifiable, unencrypted sensitive data compromised in a breach will be used to commit identity theft or to make fraudulent transactions using an individual’s account. A determination of whether a particular incident poses a risk of significant harm should be based on an assessment of the circumstances surrounding the incident. While notification of affected individuals should occur as soon as reasonably possible after an organization determines the nature and scope of the breach, restores the reasonable integrity of the data system and determines that there is likelihood of substantial harm, it should be permitted to be delayed at the request of a law enforcement agency that is carrying out its own investigation.

* * * *

²⁶ See, e.g., 12 U.S.C. § 1861 *et seq.* (the Bank Service Company Act, which provides the functional regulators with the authority to examine a bank’s service providers); Office of the Comptroller of the Currency Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers (May 15, 2002).

Once again, the Forum appreciates 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,

A handwritten signature in black ink that reads "John R. Dearie". The signature is written in a cursive style with a large, stylized initial "J" and "D".

John R. Dearie
Executive Vice President for Policy
Financial Services Forum