MORRISON | FOERSTER

1290 AVENUE OF THE AMERICAS
NEW YORK, NY 10104-0050

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP
NEW YORK, SAN FRANCISCO, LOS ANGELES, PALO ALTO, SACRAMENTO, SAN DIEGO, DENVER, NORTHERN VIRGINIA, WASHINGTON, D.C.
TOKYO, LONDON, BRUSSELS, BEIJING, SHANGHAI, HONG KONG

January 28, 2011

Writer's Direct Contact
212.506.7213
MWugmeister@mofo.com

Via E-Mail privacynoi2010@ntia.doc.gov

COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK

Report Of The Commerce Department's Internet Policy Task Force

COMMENTS OF THE GLOBAL PRIVACY ALLIANCE

The Global Privacy Alliance ("GPA")[1] appreciates the important role the Department of Commerce (Commerce) has played over the years to promote electronic commerce policies that both encourage growth and innovation as well as build trust with respect to consumer protections, privacy, and security in the online world. As the Commerce report points out, U.S. Internet policy has avoided fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust in this area. In addition, there is a clear recognition that U.S. laws and policies, backed up by strong enforcement, provide effective commercial data privacy protections and that the companies driving the digital economy have demonstrated a willingness to develop and abide by their own best practices. According to Commerce, there is evidence to suggest that consumers may lack information necessary to make informed choices, which undermines consumer trust and inhibits the adoption of new services. By issuing its green paper, Commerce seeks to foster a discussion about ways to strengthen the existing commercial data privacy framework in the United States.

[1] The GPA is comprised of a cross section of global businesses from the financial services, automobile, aerospace, consumer products, pharmaceutical, computer and computer software, communications, and electronic commerce sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

In particular, Commerce is seeking comment on whether baseline commercial data privacy principles, such as comprehensive Fair Information Practice Principles (FIPPs) should be enacted by statute or other means and, if so, which FIPPs should receive high priority. Members of the GPA take privacy obligations very seriously and work actively within their global organizations and the business community at large to encourage responsible privacy practices that enhance consumer trust as well as preserve the free flow of information. Based on its members' extensive experience complying with numerous omnibus privacy statutes around the world, the GPA commends Commerce on recognizing the difficulty in creating an omnibus approach and appreciates the recognition that any privacy solution must be flexible in light of the complexity and variation among organizations.

Morrison & Foerster LLP on behalf of the Global Privacy Alliance (GPA) is pleased to offer the following comments and observations on the issues raised by Commerce in its green paper.

EXECUTIVE SUMMARY

I. EXISTING U.S. PRIVACY LANDSCAPE IS BROAD AND VARIED

The U.S. approach to privacy has been to regulate business practices when there is a demonstrated need, resulting in the adoption of legislation that is tailored to address specific harms. Accordingly, the landscape of U.S. privacy law is broad and varied, focused on protecting sensitive information and limiting inappropriate disclosures of information, while avoiding unnecessarily broad regulation.

II. AN OMNIBUS APPROACH TO PRIVACY

The GPA commends Commerce on recognizing the difficulty in creating an omnibus approach and appreciates the recognition that any privacy solution must be flexible in light of the complexity and variation among organizations and must take into consideration the costs of compliance.

> *Maintain Existing Regimes for Already-Regulated Industries.* Experience in the U.S. has shown that, even within one sector, such as financial services or healthcare, it can take years and substantial efforts on the parts of regulators, industry, and other stakeholders to achieve an appropriately tailored privacy framework. These regimes should not be cast aside for a broader and untested legislative framework. We encourage Commerce to make more explicit that any new legislative framework should be able to encompass existing sectoral privacy rules.
>
> *Encourage Voluntary, Enforceable Privacy Codes.* The development of voluntary, enforceable privacy codes of conduct in specific industries should be encouraged, as appropriate to the industry, data type, and/or processing activity. This approach reflects the reality that FIPPs are not "one-size-fits-all" and require tailoring. The U.S. Government should identify those contexts or data types for which FIPPs are needed, rather than assuming that they are needed for all types.

III. FAIR INFORMATION PRACTICE PRINCIPLES

Commerce should focus on obligations that will produce tangible consumer benefits, such as those intended to protect against real harms to the consumer, rather than focus on protecting abstract privacy rights.

> ***Notice.*** We agree with Commerce that consumers are better served by privacy policies that are clear and concise. More thought should be given, therefore, to how to impose a notice requirement that will produce results in practice that are

meaningful and beneficial to consumers. Regulators could, in consultation with industry and other interested stakeholders, develop a list of those use and disclosure categories that are obvious, accepted, legitimate, and not potentially harmful to consumers. Alternatively, the appropriate regulators could create a list of those uses and disclosures that require notification.

Choice. Choice is clearly appropriate when information will be used for something that is not commonly accepted or there is a risk of material harm to the consumer. While choice is appropriate in some situations, we suggest that a company should not have to provide consumer choice for certain types of data processing, such as processing that is commonly accepted based on context and processing that is legitimate and immaterial to a reasonable consumer's decision to share his or her data. Our suggested approach would ensure that consumers are given a choice when the choice really matters.

Access. Access and correction rights should be focused on situations when the use of inaccurate information will have an adverse effect on consumers. Commerce should consider situations, similar to the FCRA when tailoring an access and correction right so that the proper balance is struck.

Procedures for Ensuring Compliance/Accountability. Ensuring compliance with policies and procedures are key components of any compliance program. The practices and procedures required to ensure compliance with the FIPPs will likely vary from one sector to another, therefore, any new accountability requirements should be finely targeted.

Privacy Impact Assessments (PIAs). PIAs are valuable tools. Their use should be encouraged, but it should not be mandated. In addition, imposing a requirement to make PIAs public would discourage their use and possibly compromise their integrity. The value of PIAs as a powerful internal tool enabling a company to manage and mitigate its risks would be severely undermined by a publication requirement.

IV. SCOPE OF THE PROPOSED FRAMEWORK

Before proceeding with the proposed Framework or any other approach, we urge Commerce to carefully consider its scope. In particular, we recommend that it clarify the extent to which offline data, publicly available information, business information, and the activities of service providers should be covered.

Offline Data. We recommend that Commerce clarify that it will be limited to online personal information.

Publicly Available Information. Because such information is already in the public realm, businesses should not be required to incur the costs of adopting privacy protections for it.

Information Collected And Used In A Business Context. Commerce should consider defining "commercial data privacy" to only be limited to information collected from or about individuals in connection with personal, family, or household purposes. The use of professional information for legitimate business purposes does not adversely affect individuals' privacy rights. Organizations and individuals should be free to use professional information.

Employee Data. Organizations collect personal information from their employees to fulfill their employer obligations and carry out legitimate business activities. When information is collected, used, and disclosed for such purposes, applying the full complement of FIPPs would unnecessarily burden legitimate human resources activities.

Service Providers. We recommend that Commerce consider the role of service providers carefully and expressly clarify that FIPPs do not apply to service providers or a narrower set of FIPPs obligations would only apply. Application of the full complement of FIPPs directly to service providers would cause practical difficulties and inefficiencies, in part because service providers do not have their own relationships with consumers.

V. GLOBAL INTEROPERABILITY: ACCOUNTABILITY VS. ADEQUACY

Adequacy. This adequacy model is ill suited for today's globally interconnected world in which data flows in multiple directions simultaneously, and national borders become meaningless. Moreover, this model is not sufficiently flexible in that it requires equivalence rather than adequacy and, therefore, fails to take into consideration different legal and cultural norms in other countries.

Accountability. The accountability model has the potential to offer uniform and consistent protections without regard to the jurisdictions to which the data may travel. A key question that remains to be answered fully, however, is what does it mean to be an accountable organization and, more importantly, what measures are available in the organization's home jurisdiction to enforce the obligations should the organization fail to remain accountable for personal information that is entrusted to it. We believe that the focus for accountability should be to determine if there are sufficient enforcement mechanisms in place in the home jurisdictions of the

"accountable" organizations in the event that they fail to live up to their data protection obligations in other countries or if they act unfairly based on the home jurisdiction standards. Codes of conduct, trustmarks and accountability agents should also be considered in addressing this burgeoning complexity.

APEC. While the U.S. Government should continue its efforts in the Pathfinder project to encourage the development and deployment of cross border privacy rules (CBPRs), we urge Commerce to focus its efforts on persuading those countries that have enacted cross border data privacy restrictions to provide an exception from local cross border rules for organizations that agree to adopt CBPRs to govern transfers from one jurisdiction to another. CBPRs should not become an additional layer of rules that merely supplement a country's existing cross border privacy rules.

VI. SUPPORT FOR A FEDERAL BREACH NOTIFICATION LAW

We support a federal data breach notification law, with an appropriate risk-based notice trigger, that preempts state laws. Disparate state laws that impose a myriad of actual or potentially conflicting notification requirements do not serve the public interest.

DETAILED ANALYSIS

I. EXISTING U.S. PRIVACY LANDSCAPE IS BROAD AND VARIED

The U.S. model for regulating business practices is rooted in a recognition that overly broad regulation adversely affects companies and, in turn, consumers and the economy. This has led to a reluctance to regulate business practices absent a demonstrated need, resulting in the adoption of legislation that is tailored to address specific harms. This approach has been followed with respect to 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 that follow from the free flow of information. 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,[2] focused on protecting sensitive information and limiting inappropriate disclosures of information, while avoiding unnecessarily broad regulation.

II. AN OMNIBUS APPROACH TO PRIVACY

Based on its members' extensive experience with numerous omnibus privacy statutes around the world, the GPA commends Commerce on recognizing the difficulty in creating an omnibus approach and appreciates the recognition that any privacy solution must be flexible in light of the complexity and variation among organizations.

---

[2] 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).

A. Need for Flexibility

It is impractical to apply FIPPs across all sectors, data categories, and data uses.

Data collection, use, and disclosure requirements can vary widely from one sector to another, so it would be difficult to apply FIPPs uniformly across every industry sector and data type and use. Since there is not just one right answer, as discussed below, applying obligations such as notice, choice, and access across every sector, every medium, every type of data, and every type of processing, an appropriate balance must be struck. Lawmakers, regulators, and self-regulatory bodies, therefore, must have flexibility in determining which rights and obligations are appropriate for different situations.

Lawmakers in the U.S. have, in fact, taken this approach to date. Congress has determined, for example, that information collected online from children deserves greater protection than information collected online from adults. Consequently, it passed the Children's Online Privacy Protection Act to require that websites obtain a parent's informed consent prior to collecting information from children.[3] The Act also gives the parent ongoing control over how the information is used and disclosed. The California legislature has also acted with respect to certain types of data processing. Its "Shine the Light" law imposes certain notice and choice obligations on companies that share their customers' personal information with third parties, for those parties' own direct marketing purposes.[4] These types of flexible and balanced approaches should be considered as the Framework proposed by Commerce is considered.

B. Finding the Correct Balance

There should be an appropriate balance between extending meaningful privacy protections to consumers and regulatory burdens on organizations.

Any framework must strike an appropriate balance between extending meaningful privacy protections to consumers and imposing regulatory burdens on organizations. Careful consideration must be given to the costs associated with an omnibus legislative regime to ensure that innovation and jobs are not sacrificed at the expense of privacy protections that do not provide tangible consumer benefits. This is especially important in the new economic environment in which the U.S. must compete efficiently with other countries and where reducing regulatory burden is important to our economic growth. The red tape associated with many privacy laws in the EU, for example, with respect to database registration and approval processes for data collection and transfer, contributes to the decision by some

[3] 15 U.S.C. § 6501 *et seq*.
[4] Cal. Civ. Code § 1798.83.

companies to move operations outside of the EU to countries that have less onerous data protection laws.

C. Maintain Existing Regimes for Already-Regulated Industries

Commerce should make more explicit that any new legislative framework should be able to encompass existing sectoral privacy rules.

Commerce states at the outset of its green paper that "[c]onsistent with our focus on commercial data privacy, we make no recommendation with respect to [fed government info, financial, health, education."[5] Experience in the U.S. has shown that, even within one sector, such as financial services or healthcare, it can take years and substantial efforts on the parts of regulators, industry, and other stakeholders to achieve an appropriately tailored privacy framework. The Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA) and Health Insurance Portability and Accountability Act (HIPAA) are examples of laws regulating the financial and health care sectors that have struck an appropriate balance between regulation and innovation.[6] These regimes should not be cast aside for a broader and untested legislative framework. We encourage Commerce to make more explicit that any new legislative framework should be able to encompass existing sectoral privacy rules.

Financial privacy laws have been the subject of Congressional and regulatory debate and refinement over the past 40 years. For example, in late 2009, the federal agencies responsible for enforcing the Gramm-Leach-Bliley Act (GLBA) [7] issued a model privacy notice for financial institutions to use in meeting their notice requirements under the Act.[8] The model notice was developed over the course of five years, during which the agencies conducted extensive qualitative and quantitative consumer testing to ensure that the notice would be understandable to consumers.[9] This experience suggests that it is no quick and easy feat to impose an appropriate privacy framework even within one industry sector. Similarly, the development of HIPAA took several years to develop, but nonetheless has been the subject of increased criticism.

---

[5] Green Paper, pp. 4-5.
[6] Federal protections for consumer financial information are also contained within the Electronic Funds Transfer Act, the Equal Credit Opportunity Act, and the Fair Credit Billing Act. Together, these laws subject financial institutions to a detailed array of privacy obligations and limitations. They have been designed to complement each other, based on an understanding of the ways in which financial institutions operate.
[7] 15 U.S.C. § 6801-6809.
[8] *See* 74 Fed. Reg. 62,890 (Dec. 1, 2009).
[9] *Id*. at 62,893.

D. Encourage Voluntary, Enforceable Privacy Codes.

The development of voluntary, enforceable privacy codes of conduct in specific industries should be encouraged, as appropriate to the industry, data type, and/or processing activity. This approach reflects the reality that FIPPs are not "one-size-fits-all" and require tailoring; however, adherence to a code of conduct or the full FIPPs should not be the only options, as some industry sectors, data types, and processing activities do not warrant regulation.

Under its proposed Framework, Commerce appears to suggest that a company that declines to participate in its industry's "voluntary" code of conduct would then be subject to enforcement by the Federal Trade Commission (FTC) for failure to comply with the full set of FIPPs (presumably, as established by legislation).[10] Each option (code compliance and the risk of FTC enforcement) critically fails to leave room for the possibility that data processing by certain industry sectors does not warrant regulation, that there might be valid reasons that an organization elects not to adopt its industry code, and that there are certain types of data that simply should not be regulated. Commerce acknowledges that FIPPs are general and, therefore, "there may be contexts in which certain [of them] do not apply, leading to a waste of resources when businesses must demonstrate compliance with each principle."[11] Indeed, there may be contexts in which none of the FIPPs apply, such as to professional contact information or publicly available information. It thus seems that the more appropriate and efficient approach would be to identify those contexts or data types for which FIPPs are needed, rather than assuming that they are needed for all types.[12]

III. FAIR INFORMATION PRACTICE PRINCIPLES

The following examples are provided to illustrate some of the issues that would likely arise if the obligations contained in the proposed Framework were to become statutory requirements. We urge Commerce to focus on obligations that will produce tangible consumer benefits, such as those intended to protect against real harms to the consumer, rather than focus on protecting abstract privacy rights. Not all types of data need protection, and not all types of data processing call for regulation. We encourage Commerce to follow consistent U.S. precedent to impose data restrictions only when there is a specific, identifiable harm. Commerce should also balance consumer protections with cost and regulatory burdens that could prevent businesses from growing and from competing effectively.

---

[10] "FTC approval of a voluntary enforceable code of conduct as sufficient would establish a presumption that an entity that demonstrates compliance with the code would not be subject to an enforcement action under FIPPs-based commercial data privacy legislation. For companies that do not align themselves with a voluntary code of conduct, the default would be for the FTC to enforce the FIPPs through a transparent and predictable process." Green Paper, p. 44.

[11] *Id.* at 41.

[12] We note that in the EU the development of industry codes of conduct have been available since the Directive was implemented in 1998. To date there have been only two codes of conduct adopted and approved.

A. Notice

There are a number of situations in which providing notice to consumers may be appropriate, such as when information may be used for a purpose that is not commonly accepted or when there is the potential for material harm to a consumer. As Commerce considers whether to implement a notice obligation, it is essential that the U.S. not make some of the key mistakes made by other countries in establishing overly broad and prescriptive notice obligations. As Commerce has recognized, most consumers do not read privacy notices because they are far too detailed and lengthy;[13] moreover, most of the uses described do not affect an individual's choice about whether to provide personal information to the organization. Thus, we agree with Commerce's suggestion that we strive for clear and concise privacy notices.[14]

Requiring companies to identify each point of information collection, across all channels in which it, its employees, and agents acting on its behalf collect personal information is counter productive and would undercut Commerce's laudable goal of encouraging notice that is useful to consumers to make important decisions. If a notice obligation were overly broad, organizations would need to identify when information is collected in connection with sales transactions in a retail store, when an organization searches the internet for potential speakers at a conference, whenever a customer provides information to customer service, or when a security guard interviews a witness to a slip and fall accident. There are potentially thousands of instances in which information could be collected. In addition, a company would need to identify all of the ways in which information is used. Imagine the uses that a corner convenience store would need to include in such a notice:

> to provide a product, to process payment, to provide customer service, to contact a consumer if a special request has been made, to respond to inquiries, to conduct sweepstakes or contests, to improve services, to determine which items are most popular, to send postal mailings and coupons, to conduct market research, to engage in fraud protection, to investigate accidents in the store, to contact witnesses, to obtain insurance, to defend lawsuits, to investigate and prevent theft, to respond to requests from law enforcement, to respond to requests from government authorities, to protect the privacy, safety or property of the store, to share with third parties in the event of a merger or corporate transaction.

Now imagine an organization that deals with individuals across multiple channels and multiple businesses. Such a notice would be so long and detailed that it would completely undercut its utility.

---

[13] Green Paper, p. 32.
[14] *Id.* at 33.

An added complication is the manner in which notice would be delivered. Assuming that all uses for every channel could be identified and listed in a clear and understandable fashion, notices then would have to be provided through a website, by e-mail, by telephone, and on paper. For an e-commerce company that solely operates a website, delivering a notice might be fairly straightforward because there is one channel through which information is collected and that same channel can be used to provide notice. For organizations that operate through multiple channels (online, by telephone, in retail settings, at trade shows, in person interviews), however, the challenges in finding appropriate ways to deliver a notice so that consumers would have notice when personal information is collected would be significant. Similarly cloud computing and "smart" machines such as your refrigerator, present challenges that we have not yet even begun to contemplate. It is difficult to articulate how companies could provide such a notice and how many individuals could actually decipher and understand such a notice. In fact, the sheer volume of information disclosed in a "comprehensive" notice and the likely irrelevance of a great deal of it to most consumers would likely cause many to simply disregard the notice.

In discussing the FIPPs' "purpose specification" and "use limitation" principles, Commerce gives the example of an ISP that wants to collect customer usage records to prepare bills, detect fraud, and settle billing disputes. It would state those three purposes in its privacy notice, and, according to Commerce, those would be the only three ways in which the records could be used.[15] If the ISP later had a business need to use the records internally for security purposes, it would, in Commerce's view, not be permitted to engage in such use without first providing customers with notice of it and, perhaps, obtaining their consent to the use – even though the use "has the clear potential to bring privacy and security benefits to the ISP and its customers."[16]

Areas for Further Consideration.

We agree with Commerce that consumers are better served by privacy policies that are clear and concise.[17] More thought should be given, therefore, to how to impose a notice requirement that will produce results in practice that are meaningful and beneficial to consumers. One possible approach might be to permit companies the flexibility to describe their data uses via something less than a granular list. In fact, the most effective notice may be one that does not even list the obvious or expected categories of information use. Commerce could, in consultation with industry and other interested stakeholders, develop a list of those use and disclosure categories that are obvious, accepted, legitimate, and not potentially harmful to consumers. The list would include, for example, product and service fulfillment, communication with the consumer relating to the product or service, first-party

[15] Green Paper, p. 38.
[16] *Id.*
[17] Green Paper, p. 33.

direct marketing, internal research and development, legal compliance, fraud prevention, and protection of the company's interests. While not a comprehensive list, these examples are categories of processing that are necessary and/or legitimate. There is no point, therefore, in listing them in a notice. Moreover, if they are stripped from the notice, the notice will be far more concise and straightforward and, most importantly, provide the consumer with the facts he or she really needs to decide whether or not to share his or her data (*i.e.*, the facts that are most material to that decision). Of course, any use or disclosure that does not fall within one of the agreed-upon categories and that is likely to be material to consumers should be included in the policy. One obvious example is the sharing of consumer data with third parties for their own direct marketing use.

HIPAA provides a useful example. Health care regulators spent considerable energy trying to find the right balance between providing useful information and overwhelming consumers. HIPAA's notification requirements relating to privacy and security policies and procedures do not require enumeration of every conceivable use or disclosure of individually-identifiable health information that may be made without individual authorization. Instead, HIPAA requires only summary information about the general types of uses and disclosures that are permitted by regulation.[18] Some covered entities are even expressly excused from providing a notice of privacy practices to the individuals whose information they handle.[19]

Alternatively, the appropriate regulators could create a list of those uses and disclosures that require notification. Such a list might include the use or disclosure of sensitive health information, disclosure of information relating to an individual's specific purchases or transactions, use of geo-location information, collection and use of information from and about an individual for online behavioral advertising purposes, disclosure of a customer's information to third parties for those parties' own commercial purposes, and use of data relating to an individual's purchasing behavior to determine the prices to charge him or her or whether certain products or services will be made available to him or her. The obvious benefit of this alternative is that it could evolve over time and is not limited to a specific technology, platform, or period of time. Two years ago, for example, no one was concerned about geolocation data, but that has quickly changed. Having a list of those uses, disclosures, or types of data that must be included in a notice could be readily updated by guidance from the appropriate regulator.

B. Choice

Many countries around the world, as well as U.S. regulators, have struggled with finding the right balance between giving individuals choice over how their information is used and burdening both consumers and businesses with an overly prescriptive regime. Choice is

[18] *See* 45 C.F.R. § 164.520(b).
[19] 45 C.F.R. § 164.500(b)(1).

clearly appropriate when information will be used for something that is not commonly accepted or there is a risk of material harm to the consumer. In some countries, however, the consumer experience on the web has become so cumbersome that consumers must consent to four different notices before he or she can enter a website. Such overly complicated choice is bad for both consumers and companies. Commerce should consider for what types of uses or disclosures choice should be required: for example, disclosures to all third parties regardless of use or only for disclosures for marketing purposes? What type of choice should be required – opt-in or opt-out? For example, would a company that sells computers have to give individuals the right to have information not shared with an affiliate that runs the warranty program? Would employers have to allow employees to opt out of sharing information with service providers, such as payroll and benefit providers? Would individuals have the right to opt out of sharing among affiliated companies when sharing information is necessary to provide 24/7 customer service? Would organizations have to provide individuals with the right to opt out of receiving postal mail? These are very difficult questions that require serious discussion among all stakeholders and are unlikely to result in a single answer that applies across all sectors for all data types.

Areas for Further Consideration.

While choice is appropriate in some situations, consistent with our recommendations with respect to the disclosures required for privacy notices, we suggest that a company should not have to provide choice for the following types of data processing:

- *Processing that is commonly accepted by the consumer based on context.* For example, a consumer buying a product online will understand that his or her personal information will be used to charge a credit card and deliver the product. He or she will also understand that the company will use personal contact information to communicate about the purchase (*e.g.*, to notify the consumer 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 by the consumer, consent should be inferred by the request for the product.

- *Processing that is legitimate and 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, but also immaterial to a reasonable consumer's decision to share his or her personal data with a company.[20] Accordingly, they should not be subject to

[20] The inclusion of a "materiality" component is consistent with federal law's approach to consumer protection generally (as enforced by the FTC). Disclosures that are "material" must typically be called out to consumers; if a disclosure is not "material," then there is no need to treat it specially.

> consumer choice.[21] They include, by way of example, disclosures to service providers,[22] servicing the consumer's account, internal analytics, internal research and development, fraud prevention, audits, legal compliance, and disclosures to governmental authorities or law enforcement.[23] Permitting consumers to opt out of (or requiring them to opt into) these types of processing would have negative consequences to both organizations and consumers. It is beneficial to organizations and consumers to prevent fraud, provide efficient customer service, and cooperate with law enforcement. Internal research and development provides 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.

If these types of processing 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 choice should not be necessary. Our suggested approach would ensure that consumers are asked only given choice when the choice really matters: that is, when the company proposes to use personal data in a way that is not covered above.

C. Access

Access and correction rights should be focused on situations when the use of inaccurate information will have an adverse effect on consumers. The FCRA is one example of where the significant benefit to the consumer of providing a method for consumers to obtain information and correct it when it will be used for credit or employment decisions outweighs

---

[21] For illustrative purposes, imagine a consumer's slip-and-fall accident at a retailer's store. In this scenario, the retailer is likely to collect personal information from the consumer to appropriately address the consumer's situation. The retailer, however, may also use information that it has previously collected from the consumer outside of the incident (*e.g.*, sales receipts on the day in question or video tapes of the stores premises). In turn, the retailer may provide this information to emergency personnel contacted by the retailer, its insurance company, a government safety inspector, and even its attorneys or a court in litigation in connection with the incident. While a consumer may not expect to suffer an injury at a retailer, the collection and sharing of information described in this example is legitimate, appropriate, and important to business operations. To the extent that the retailer uses information that it has separately collected in connection with the incident, it would seem immaterial to a reasonable consumer's decision to share that information with the retailer.

[22] Giving consumers the ability to opt out of the disclosure of their data to service providers would deprive companies of the efficiencies associated with outsourcing. It could also incent companies against data uses for which they need a service provider, which could result in fewer offerings to or benefits for consumers. In its Financial Privacy Rule, the FTC does not subject the sharing of financial data with service providers to consumer choice. 16 C.F.R. § 313.13(a).

[23] The FTC's Financial Privacy Rule provides a useful list of the categories of disclosures that it found to be legitimate and not subject to consumer choice. *See* 16 C.F.R. §§ 313.13 and 313.14.

the costs to business of providing such a system. Commerce should consider other similar situations when tailoring an access and correction right so that the proper balance is struck.

A requirement to provide individuals with broad access to their information, and the ability to update and correct it, begs the question of whether the consumer benefits outweigh the cost and effort required to implement and maintain systems needed to provide such access. If an omnibus access and correction right were implemented, organizations would need systems capable of tracking all personal information they hold in a form that is searchable and updateable. As organizations continue to outsource, store data in "the cloud" and adopt distributed information management systems, providing access is not quite so easy. The cost of providing expansive access rights would be high, particularly for organizations collecting and using offline data that have multiple channels for data collection online or have any distributed models across organizations or geographies. 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. For an organization, such as a law firm, that still relies heavily on paper and offline collection of data, the cost of developing such a system would be prohibitively expensive. 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. As Commerce considers these issues, perhaps there should be a limitation on any access right based on the burden of providing the information (as there is in some EU countries) or perhaps organizations should be able to require a fee for access requests that are require extensive effort.

In addition, there are legitimate reasons for denying access in certain situations, so careful consideration must be given to establishing appropriate access exceptions. In the law firm context, for example, the need to comply with legal privilege obligations has to be carefully weighed against the right for individuals to be granted access. Similar concerns would arise in connection with other providers of professional services, such as accountants. In addition, exceptions have to be built in for requests that might expose the privacy rights of other individuals or trade secrets.

D. Procedures for Ensuring Compliance/Accountability

Ensuring compliance with policies and procedures are key components of any compliance program. The practices and procedures required to ensure compliance with the FIPPs will likely vary from one sector to another. While employee training and accountability are essential in some industries and for some data types, the requirement should not be

ubiquitous across all industries for all data types.[24] As pointed out by Commerce, in order to audit or monitor data processing, there has to be a clear understanding of what information is being handled. In an organization that relies heavily on non-electronic data, the complexities of tracking all data would be significant. Given the substantial costs associated with the hiring of qualified employees to conduct or oversee regular audits, the handling of the recordkeeping that would result, and requisite employee training, it will be important to provide sufficient flexibility so that organizations may select compliance procedures and accountability standards that are most appropriate to their particular data collection and use activities. Many organizations already are struggling to keep up with recordkeeping obligations pursuant to other laws, such as the Sarbanes-Oxley Act; therefore, any new accountability requirements should be finely targeted.

E. Privacy Impact Assessments (PIAs)

Commerce proposes that companies be required to conduct PIAs to identify, evaluate, and mitigate risks arising from the use of personal information in new practices or technologies. PIAs are valuable tools. Their use should be encouraged, but it should not be mandated. PIAs are not appropriate for every new practice or technology; rather, a PIA is appropriate only when there is a serious risk of negative and unknown consequences to privacy. When the consequences are already known and certain measures and procedures are commonly applied to address them, a PIA is unnecessary and should not be required. In addition, the frequency 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. PIAs are useful precisely because they identify the risk and then the company works to fix the problem, a benefit that would be lost if companies were forced to disclose the reports.[25] Finally, a requirement that PIAs be publicized could expose a company's trade secrets. The public-disclosure aspect is likely to create a disincentive to their use, as well as to innovation and the creation of new technologies. For example, publication could risk disclosure of a company's proprietary methods of targeting customers, including how it filters online and offline lists and determines who receives certain messages. Commerce may have an interest in knowing that

[24] For example, the Massachusetts data security regulations impose audit and employee training obligations only to sensitive categories of data, such as name plus Social Security number, driver's license number, or financial account number. *See* 201 Mass. Code Regs. §§ 17.01-17.05.

[25] By way of analogy, bank examiners' reports are both detailed (and therefore useful) and protected against disclosure.

the company reaches its results legally, but it does not have to know – or permit others to know – the particular algorithms and methods used to get to those results. The value of PIAs as a powerful internal tool enabling a company to manage and mitigate its risks would be severely undermined by a publication requirement.

IV. SCOPE OF THE PROPOSED FRAMEWORK

Before proceeding with the proposed Framework or any other approach, we urge Commerce to carefully consider its scope. In particular, we recommend that it clarify the extent to which offline data, publicly available information, business information, and the activities of service providers should be covered.

A. Offline Data.

It is not entirely clear whether Commerce intends for the Framework to apply to personal information collected offline. While the very title of the Framework ("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," arguably suggest that the intended scope may be broader. We believe that it is critical for Commerce to clarify the framework's intended scope. We recommend that Commerce limit it to online personal information.

If the Framework extends to personal information collected offline, then companies will need flexibility in how they are permitted to provide the required notice. Specifically, in that case, 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 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 directing consumers to a publicly available copy of the notice, such as one posted on its website or a customer service desk in a physical store.[26] 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.

B. Publicly Available Information.

The Framework covers "commercial data privacy" but it is unclear if this would include publicly available information. It should not. Because such information is already in the

[26] Japan's Personal Information Protection Law (Article 18) provides the flexibility of notifying individuals directly or through a public announcement (e.g., an announcement posted on a website or displayed in a location in a store where it will be easy to see).

public realm, businesses should not be required to incur the costs of adopting privacy protections for it.

C. Information Collected And Used In A Business Context

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 may make it reasonable to assume that Commerce intends for the Framework to apply only to information obtained from an individual in connection with personal, family, or household purposes (*i.e.*, a "consumer" interaction). There are also references, however, to "individual" privacy, which could be read to cover personal data beyond that collected from a consumer. We request Commerce to consider defining "commercial data privacy" to only information collected from or about individuals in connection with personal, family, or household purposes. Thus, for example, information about an individual in his or her capacity as a representative of an entity and used in the context of a business-to-business relationship would be excluded.

An exemption for professional information is appropriate and, as noted below, is consistent with the rules of a number of other countries. The use of professional information for legitimate business purposes does not adversely affect individuals' privacy rights. Individuals acting in their professional capacity, and their employers, expect and want their information (such as the contact information found on business cards and company websites) to be shared easily with others. Indeed, individuals usually disclose their professional contact information for the purpose of making such information available to be freely used. The growth of sites such as LinkedIn is a perfect example of the desire by individuals to freely share such information. Imposing the same notice and choice obligations, for example, as those that apply to consumer data would restrict the sharing of information that permits organizations to maintain their everyday operations and would consequently hamper efficiency.

Consider the following examples:

- An individual gives his or her business card to another individual at a conference or meeting. The recipient should not be expected to provide the individual with his or her company's privacy notice or obtain the individual's consent before taking the business card and adding the details to his or her rolodex or electronic address book.
- Similarly, when an individual sends an email inquiry to a company in his or her capacity as the representative of an organization, the company should not have to send the individual a privacy notice and obtain the individual's consent to use his/her email address so the company can respond to the query.
- If an organization is seeking an expert to provide advice, the organization should be able to search the internet and collect that information as it makes its decision without

having to provide notice to each potential expert whose advice it might seek. The reason individuals post professional information publicly, such as on the internet, is so that other people can easily find it and use it.

In the business context, individuals have less of an expectation of, and less concern with, privacy because the information collected from and about them does not pertain to their personal, home, or family lives. For these reasons, extending the Framework's protections to such information is unnecessary.

Some countries' omnibus data protection laws also exempt business information. For example:

- Spanish legislation excludes processing operations regarding legal entities and files that only record data of individuals providing services in organizations (their name, functions or jobs performed, postal or e-mail address, and professional telephone and fax numbers).[27]
- Canada's legislation currently excludes name, title, business address, and business telephone number of an employee of an organization from the definition of personal information (business e-mail address and fax number are not currently excluded).[28] Recently proposed amendments would remove this exclusion and would expressly permit business contact information to be used without consent, solely for the purposes of communicating or facilitating communication with the individual in relation to their employment, business, or profession. Under the proposed amendments, "business contact information" would include an individual's name, position name or title, work address, work telephone number, work fax number, work e-mail address, and similar information.

Organizations and individuals, therefore, should be free to use professional information.

D. Employee Data

Organizations collect personal information from their employees to fulfill their employer obligations and carry out legitimate business activities. When information is collected, used, and disclosed for such purposes, applying the full complement of FIPPs would unnecessarily burden legitimate human resources activities. For example, a mechanism to exercise choice (*e.g.*, give employees the right to opt out) with respect to the collection, use and disclosure of

[27] Article 2 paragraphs 2 and 3 of the Spanish Royal Decree 1720/2007 of December 21, which approves the Regulation implementing Organic Law 15/1999**,** of December 13, on the Protection of Personal Data.
[28] Personal Information Protection and Electronic Documents Act (PIPEDA), available at http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html

employee personal information should not be required when the employer must use this information to carry out reasonable and/or legitimate business activities and operate the business efficiently. Consequently, we believe that different rules should apply to employee data than apply to consumer data. While it is extremely important to protect employee personal information, choice should not be required to collect, use, and disclose employee data for legitimate and/or reasonable purposes within the context of the employment relationship and any subsequent retiree relationship. "Reasonable purposes within the context of the employment relationship" may vary depending on the business and industry sector of the organization; however, if an organization wishes to collect, use, and disclose employee data for purposes beyond those that are legitimate and/or reasonable within the context of the employment relationship, then employee choice may be appropriate. Similarly, to require employers to provide notice when personal information is to be used for employment related or business operation (*e.g.*, normal business and administrative functions required to operate the business efficiently) purposes would not serve the interests of employees or organizations. Employers use employee information for commonly used and accepted purposes such as:

> Managing work activities and personnel generally, including recruitment, appraisals, performance management, promotions and succession planning, rehiring; administering salary, and payment administration and reviews, wages and other awards such as stock options, stock grants and bonuses, healthcare, pensions and savings plans, training, leave; managing sickness leave, promotions, transfers, secondments; honoring other contractual benefits; providing employment references, loans; performing workforce analysis and planning; performing employee surveys; performing background checks; managing disciplinary matters, grievances and terminations; reviewing employment decisions; making business travel arrangements; managing business expenses and reimbursements; planning and monitoring of training requirements and career development activities and skills; creating and maintaining internal employee directories; facilitating communication with employees and their designated contacts in an emergency; ensuring business continuity; protecting the health and safety of employees and others; operating, managing, and safeguarding the IT and communications infrastructure, systems, office equipment and other property; managing product and service development; improving products and services; managing company assets; allocating company assets and human resources; strategic planning, project management, compilation of audit trails and other reporting tools; maintaining records relating to business activities, budgeting, financial management and reporting; managing mergers, acquisitions, sales, re-organizations or disposals and integration with purchaser; complying with legal and other requirements, such as income tax and national insurance deductions, recordkeeping and reporting obligations; compliance with government inspections and other requests from government or other public

authorities; responding to legal process such as subpoenas; pursuing legal rights and remedies; defending litigation and managing any internal complaints or claims; conducting investigations and complying with internal policies and procedures.

The average employee notice provided in countries that have a notice requirement is five single spaced pages long. The usefulness to employees of such a notice has been questioned by many privacy practitioners, consumers groups and data protection authorities. The burden on employees in providing such lengthy notices has to be considered, the administrative and other costs associated with providing such an all encompassing notice and the benefits of such a notice must all be considered when determining how to apply the FIPPs to employee data.

E. Service Providers

The 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 respectfully recommend that Commerce consider the role of service providers carefully and expressly clarify that FIPPs do not apply directly to service providers or a narrower set of FIPPs obligations would only apply.

Application of the full complement of FIPPs to service providers would cause practical difficulties and inefficiencies. Because service providers do not have their own relationships with consumers, it would be very difficult for them to provide, for example, 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. Moreover, we believe that this is consistent with consumer expectations.

Additionally, not all service providers provide the same role. Some play a more significant role in managing or hosting personal information, and it may be appropriate, depending on the role of the service provider, to expect the service provider to take on a greater role with respect to access or accuracy, for example.

In the health care area, despite the comprehensive protection given to individually-identifiable health information by HIPAA, covered entities are nonetheless permitted to disclose such information to their business associates without any requirement to first seek

individual authorization or choice.[29] Even after extending many of HIPAA's regulatory requirements to business associates and significantly increasing the privacy and security obligations of both covered entities and business associates, a relatively free exchange of individually-identifiable health information between these entities remains permissible.[30] The same principles should apply to the regulation of personal information generally, including information that is far less sensitive. Accordingly, we urge Commerce to either exempt service providers from the scope of its Framework or, at least, subject them to a narrower set of FIPPs obligations.

V. GLOBAL INTEROPERABILITY: ACCOUNTABILITY VS. ADEQUACY

A. International Landscape

In the U.S., Commerce, the FTC and other regulatory agencies have sought to educate industry and the public about FIPPs, encourage voluntary adoption of meaningful privacy protections by industry, and require organizations to live up to their public commitments to protect privacy or face enforcement actions for unfair and deceptive practices under Section 5 of the FTC Act or to similar provisions in other laws.[31]

In contrast, a growing number of countries around the world have adopted omnibus privacy laws. These laws, however, vary widely with respect to the personal data covered, the permissible uses and disclosures, and specific obligations such as notice, choice, and database registration. Most of these laws also restrict the cross border transfers of personal data to countries that do not provide an "adequate" level of protection. To comply with these disparate laws, global organizations must put into place a complex and overly bureaucratic set of programs and arrangements that, particularly given their cost, do little to provide

[29] 45 C.F.R. § 164.502(e)(1)(i).
[30] *See* Sections 13401 & 13404(a) of the Health Information Technology for Economic and Clinical Health Act as set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009.
[31] For example, a bank that fails to live up to its public commitments related to privacy or that fails to comply with the myriad privacy requirements that apply to banks can be subject to enforcement actions under the Federal Deposit Insurance Act ("FDIA"). In this regard, banks are subject to detailed and rigorous examination and supervision by their functional regulators, including with respect to the various privacy requirements to which they are subject. *See, e.g.*, 12 U.S.C. § 481 (directing Office of the Comptroller of the Currency to examine "all the affairs of" every national bank). If a bank's functional regulator believes that the bank has engaged in an unsafe or unsound practice or has violated the law, the functional regulator may bring an enforcement action under the FDIA against the bank, including, for example, to obtain an injunction or civil money penalties. 12 U.S.C. § 1818(b).

meaningful privacy protections and instead complicate and add costs to the use of personal data for legitimate business purposes.[32]

B. Accountability and the APEC Privacy Framework

The APEC Privacy Framework was developed several years ago to encourage the adoption of privacy regimes in those APEC economies that did not have privacy rules in place and to ensure that such rules would not interfere with the transfer of personal data among the APEC economies. Toward that end, the APEC Framework specifically included a principle on accountability. The purpose of the accountability principle is to enable organizations to establish a consistent and more uniform privacy protection regime for their data processing activities and eliminate the need for artificial distinctions between domestic and international transfers and use of information. Allowing an organization to apply a consistent set of rules for domestic and international transfers appropriately reflects the way in which personal information is used today and is likely to result in meaningful privacy protection for consumers. In exchange, organizations are expected to remain responsible for the protection of personal information under their control without regard to the jurisdictions to which the personal information may be transferred. Thus, if information is transferred locally or across the globe, an organization is expected to ensure that it is properly protected.

Despite the adoption of the APEC Framework and the ongoing efforts of the Pathfinder project, an initiative designed to develop a system that provides for accountable cross border transfers, more economies in the region have opted to enact privacy legislation that is likely to make cross border transfers more difficult. Prior to the adoption of the APEC Framework in 2005, eight of the 21 economies in APEC had either omnibus or sectoral privacy laws in place (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. Subsequent to the adoption of the Privacy Framework and the ongoing implementation of the Pathfinder project, four more countries (Malaysia, Mexico, Russia, and Taiwan) adopted omnibus privacy laws and three of the 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 the 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 encourage cross border transfers in a manner that encourages accountability, the APEC framework has instead encouraged countries with no data protection laws to adopt restrictive laws that limit data flows.

[32] For example, EU organizations must establish, maintain, and continuously update an extensive array of model contracts which must be filed with the data protection authorities; such contracts have no practical effect or benefit to individuals.

C. Cross Border Privacy Rules (CBPRs)

While the U.S. Government should continue its efforts in the Pathfinder project to encourage the development and deployment of cross border privacy rules (CBPRs), we urge Commerce to focus its efforts on persuading those countries that have enacted cross border data privacy restrictions to provide an exception from local cross border rules for organizations that agree to adopt CBPRs to govern transfers from one jurisdiction to another.[33] CBPRs should not become an additional layer of rules that merely supplement a country's existing cross border privacy rules. Rather, the entire purpose of CBPRs is to enhance cross border data flows and to remove impediments such as adequacy or similar restrictions that may apply locally. Without this quid pro quo (*i.e.*, companies are accountable in exchange for being relieved of cross border limitations), the concept of accountability becomes meaningless. If companies will be compelled to comply with local cross border restrictions in addition to being accountable for personal information globally, there is no incentive for organizations to be accountable. Rather, the goal should be to encourage organizations to be responsible for personal information no matter where it is transferred. This approach will yield the greatest protection for the consumer, while at the same time allowing organizations to take appropriate steps to protect information without over regulation. As demonstrated by Canada and Japan, an accountability model offers the best solution to bridging disparate approaches to data protection around the world.

D. EU Adequacy Model

Many of the laws that restrict cross border data transfers are based on the EU adequacy model, which is ill suited for today's globally interconnected world in which data flows in multiple directions simultaneously, and national borders become meaningless. In particular, the adequacy model is not sufficiently flexible in that it requires equivalence rather than adequacy and, therefore, fails to take into consideration different legal and cultural norms in other countries. This conclusion is borne out by the fact that very few countries have been found "adequate" by the EU.

Moreover, the adequacy model creates an enormous bureaucratic burden for the transferring organization, the receiving organization, and the national data protection authorities (DPAs) that is not sustainable in the long-term. From a regulatory perspective, this model requires tremendous oversight of an ever increasing number of businesses engaged in cross border commerce and vast amounts of data flowing in all different directions. The DPAs simply do not have the resources to review all of the data transfers or to enforce these rules. From the organization's perspective, the adequacy mechanisms are unclear or require a complicated

[33] *See* Miriam Wugmeister, Karin Retzer, and Cynthia Rich, "Global Solution For Cross-Border Data Transfers: Making The Case For Corporate Privacy Rules," 38 Geo. J. Int'l L. 449 (Spring 2007)

array of contracts, consents, and/or regulatory approvals without increasing privacy protection. Organizations that are less risk adverse simply ignore the rules, while those organizations that do their best to comply with the letter of the law are placed at a competitive disadvantage. Compliance with cross border data transfer rules are viewed as a tax that organizations must pay lawyers and DPAs in order to run their businesses. The individual ultimately suffers the most because the resulting hodgepodge of rules that organizations must put in place to satisfy this maze of complicated cross border rules do little to adequately protect their personal data and discourage organizations from remaining accountable for protection of that data.

E. Accountability vs. Adequacy

In contrast, the accountability model has the potential to offer uniform and consistent protections without regard to the jurisdictions to which the data may travel. A key question that remains to be answered fully, however, is what does it mean to be an accountable organization and, more importantly, what measures are available in the organization's home jurisdiction to enforce the obligations should the organization fail to remain accountable for personal information that is entrusted to it. In addition, if the bureaucratic obligations present in countries with an adequacy model were lifted, far more attention could be paid by DPAs to ensuring that appropriate steps are taken to actually protection personal information. One could argue that the reason enforcement is so much more robust in the U.S. is because we have far less focus on formal cross border limitations and much more focus on ensuring that companies live up to the promises that they make. It is clear from the discussion resulting from the European Commission's ongoing review of the EU Data Protection Framework that the EU's approach has placed far too much emphasis on form over substance, and the resulting bureaucratic formalities are not producing the desired results. As a result, the EU is now proposing to add an accountability obligation onto existing data controller obligations in the hopes that it would force data controllers to assume more responsibility for compliance.

Accountability is not a monolithic concept, but rather accountability can be established through multiple paths. 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 economy level. This approach may work for organizations operating in unregulated sectors but is problematic for those organizations that are already subject to comprehensive sectoral or other regulations. For example, many APEC economies have regulated how financial institutions collect, use, and share personal information. Because many of the APEC economies already regulate financial institutions with respect to privacy and data security, economies rather than companies should have to demonstrate broad compliance with the APEC principles at the economy level and organizations demonstrate

that they are in compliance with their home economy's laws through flexible existing means, including exam processes.

F. Options to Consider

We believe that the focus for accountability should be to determine if there are sufficient enforcement mechanisms in place in the home jurisdictions of the "accountable" organizations in the event that they fail to live up to their data protection obligations in other countries or if they act unfairly based on the home jurisdiction standards. The FTC has successfully used its Section 5 authority under the FTC Act to prosecute organizations that fail to live up to their stated privacy policies or who have acted unfairly. As a result, whether or not the organization is subject to a set of privacy rules becomes less relevant; what matters more is whether it lives up to the rules it has committed publicly to follow and whether there is true enforcement. Where the US has regulated, it has required those organizations to be accountable. The privacy obligations applicable to banks apply wherever they may handle consumer financial information. That is, the U.S. privacy laws do not differentiate based on where a bank may handle consumer financial information (*e.g.*, within the U.S. or outside of the country). Moreover, these privacy 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).[34] Given the U.S. experience with this model, the federal government should strongly consider such a model as it focuses on the Framework.

Given the significant increase in data flows both domestically and internationally, regulators are not positioned to effectively police all data collection and use activity within, much less beyond their jurisdiction. Codes of conduct may help address the concept of globally applicable rules, but one omnibus regulatory entity may not be the best enforcement paradigm. Trustmarks and accountability agents should also be considered in addressing this burgeoning complexity. Such trust agents do not replace the authority with ultimate responsibility but rather create a supplemental path that allows companies to more effectively handle validation of core practices, while also providing customers with an easy and well supported path of complaint and redress.

It would be far easier if all countries and organizations could simply adhere to a common set of privacy rules; however, even if such rules could be established, it would take years to accomplish a global consensus regarding a single set of privacy rules. Organizations need a more immediate solution to the existing cross border transfer issue. Simply adopting the EU adequacy approach is not the solution. Such an approach will only add yet another conflicting law to the growing number of laws that currently exist and will result in more

[34] *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).

compliance burden on organizations without a corresponding benefit to consumers. Consequently, we urge Commerce to broaden its existing approach to accountability, look beyond the Pathfinder initiative, and consider augmenting the Pathfinder initiative with privacy and data security concepts embodied in existing U.S. law.

VI. SUPPORT FOR A FEDERAL BREACH NOTIFICATION LAW

We support a federal data breach notification law, with an appropriate risk-based notice trigger, that preempts state laws. Disparate state laws that impose a myriad of actual or potentially conflicting notification requirements do not serve the public interest. Moreover, these disparate laws result in both higher costs and uneven individual protection. A common national standard would avoid creating confusing and conflicting obligations and promote the public interest.[35]

A. Breach notification should be predicated upon a significant risk of substantial harm and should allow for flexible timing and method of notification.

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. In addition, because notifications to individuals and public authorities serve different purposes, there should be different triggers and obligations for each group.

Individuals. The primary purpose of providing notices to individuals is to enable them to take steps to mitigate the risk of 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. Such data would include, for example, Social Security number and financial account or credit or debit card data, together with any password or pin number that can be used to access the underlying 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, it should be permitted to be delayed at the request of a law enforcement agency that is carrying out its own investigation. Finally, a law should be

[35] *See* the GPA's paper on "Breach Notification Legislation -- Key Elements to Consider." A copy is provided as a separate attachment to this submission.

flexible with respect to the method of notification. The method used should depend on the particular circumstances surrounding the company's relationship to the potentially affected individuals, the manner in which it typically communicates with them, and the type and scope of the breach.

Public Authorities. The primary purpose of public reporting is to enable the authorities to identify persistent or systemic problems and take action as needed to address them. Given these objectives, notification about a security breach believed to affect only a few individuals would not be appropriate. Frequent reporting about relatively minor security breaches will overwhelm the public agencies responsible for consumer protection and data security regulation, whose resources are most likely already stretched thin. Consequently, only major breaches (*e.g.*, those affecting more than 5,000 individuals) should be reported or made public in some way. The method of notification should reflect the specific needs of the public authorities, but should not be so burdensome as to cause delay in notifying individuals.