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

February 18, 2011

Writer's Direct Contact
212.506.7213
MWugmeister@mofo.com

Via Online Delivery at https://ftcpublic.commentworks.com/ftc/consumerprivacyreport/

PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS

Preliminary FTC Staff Report
FTC File No. P095416

COMMENTS OF THE GLOBAL PRIVACY ALLIANCE

The Global Privacy Alliance (GPA)[1] appreciates the important role the Federal Trade Commission (Commission) has played over the years to protect consumer privacy. By issuing its preliminary staff report, the Commission seeks input on a proposed framework to balance consumers' privacy interests with innovation that relies on consumer data to develop new products and services.

In particular, the Commission is seeking comment on whether and how certain baseline commercial data privacy principles, such as comprehensive Fair Information Practice Principles (FIPPs), should be imposed upon businesses. 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 the Commission on recognizing the challenges associated with policymaking on privacy issues. The GPA also appreciates the Commission's recognition that privacy solutions must be flexible in light of the complexity and variation among organizations and its desire to avoid solutions that would hinder business innovation.

[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.

Morrison & Foerster LLP, on behalf of the GPA, is pleased to offer the following comments and observations on the issues raised by the Commission staff in its preliminary report.

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 SHOULD BE FLEXIBLE AND ADAPTABLE

The GPA commends the Commission on recognizing the significant challenges associated with policymaking on privacy issues and appreciates the recognition that privacy solutions must be flexible in light of the complexity and variation among organizations and must take into consideration the costs of compliance.

Apply a Flexible and Balanced Approach to FIPPs. An appropriate balance must be struck before obligations such as notice, choice, and access are applied across every sector, every medium, every type of data, and every type of processing. Lawmakers, regulators, and self-regulatory bodies must have flexibility in determining which rights and obligations are appropriate for different situations. This is consistent with the approach taken by U.S. lawmakers to date.

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 framework. We encourage the Commission to make explicit that existing sectors with privacy laws should be exempt from any new framework.

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, including notice, choice, access, and reasonable

retention, are not "one-size-fits-all" and require tailoring. The Commission should identify those contexts or data types for which FIPPs are needed, rather than assuming that they are needed for all types.

III. SCOPE OF THE PROPOSED FRAMEWORK

Before proceeding with the proposed framework, we urge the Commission to carefully consider its scope. In particular, we recommend that it take into account the potential ramifications of its current definition of covered information. We also recommend that the Commission clarify the extent to which publicly available information, business information, and the activities of service providers should be covered. Finally, we urge the Commission to take a flexible approach with respect to offline data.

Consumer Data Linked To A Device. Including such data within the scope of the proposed framework is overly broad. It would implicate a wide variety of "smart" machines, presenting numerous challenges in applying the framework, including many challenges that cannot yet be contemplated. To avoid hampering the free flow of information, as well as the imposition of unnecessary costs on businesses and consumers, we recommend that the Commission consider a more narrowly tailored scope.

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. The Commission should consider expressly limiting the scope of the framework 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.

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

Flexibility for Offline Data. If the final framework extends to consumer data collected offline, then companies will need flexibility in how they are permitted to

comply with applicable FIPPs. For example, a company should not be required to provide a consumer with a hard copy of its notice at the point of collection; rather, it should be able to direct consumers to a publicly available copy of the notice, such as online or in a retail location. A flexible approach would result in obvious efficiencies and avoid obstacles to the free flow of information.

IV. FAIR INFORMATION PRACTICE PRINCIPLES

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

Notice. We agree with the Commission 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. The Commission 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 and therefore need not be described in privacy notices. Alternatively, it could create a list of those uses and disclosures that require notification.

Choice. Choice may be 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 would have an adverse effect on consumers. When tailoring an access and correction right, the Commission should ensure that the proper balance is struck (as with the Fair Credit Reporting Act). Broadly applicable access obligations would raise costs for businesses and, therefore, consumers.

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 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. As the Commission recognizes, their use should be encouraged. It should not be mandated.

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.

[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).

II. AN OMNIBUS APPROACH TO PRIVACY SHOULD BE FLEXIBLE AND ADAPTABLE

Based on its members' extensive experience with numerous omnibus privacy statutes around the world, the GPA commends the Commission for recognizing the significant challenges associated with policymaking on privacy issues and appreciates the recognition that privacy solutions must be flexible in light of the complexity and variation among organizations.

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, an appropriate balance must be struck before obligations such as notice, choice, and access are applied across every sector, every medium, every type of data, and every type of processing. 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 taken into account as the proposed framework 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 regime to ensure that

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

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

C. Existing Regimes Should Be Maintained

The Commission should make explicit that any new framework should encompass existing sectoral privacy rules.

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.[5] These regimes should not be cast aside for a broader and untested legislative, regulatory, or self-regulatory framework, and the Commission should make explicit that existing sectors with privacy laws should be exempt from any new framework.

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 Commission and the other federal agencies responsible for enforcing the GLBA[6] issued a model privacy notice for financial institutions to use in meeting their notice requirements under the Act.[7] 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.[8] 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] 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.

[6] 15 U.S.C. § 6801-6809.

[7] *See* 74 Fed. Reg. 62,890 (Dec. 1, 2009).

[8] *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.

III. SCOPE OF THE PROPOSED FRAMEWORK

Before proceeding with the proposed framework, we urge the Commission to carefully consider its scope. In particular, we recommend that it clarify the extent to which publicly available information, business information, and the activities of service providers should be covered.

A. Consumer Data Linked To A Device

The proposed framework covers "consumer data that can be reasonably linked to a specific consumer, computer, or other device."[9] The Commission proposes to apply its framework to all such data, which would result in an extremely broad scope. In particular, the framework's applicability to consumer data linked to a "device" would implicate a wide variety of "smart" machines, such as refrigerators, television-top boxes, cars, and products that have not yet been imagined. We agree that businesses should be encouraged to take privacy and data security into account in the early stages of product development; however, the application of the entire proposed framework to such a broad range of data would present a host of challenges, including many that cannot yet be contemplated. For instance, it is difficult to imagine how businesses would provide notice to and obtain choice from their customers in connection with all devices, or how they would provide customers with access to the data obtained through their use of the device. These requirements would not only impede the free flow of information, but they would also impose costs on businesses (and, consequently, on their customers), without countervailing benefits to consumers. Moreover, consumers would be inundated with privacy notices, leading them to likely disregard them. For these reasons, we recommend that the Commission consider a more narrowly tailored scope for any final framework.

B. Publicly Available Information

As noted above, the proposed framework covers "consumer data that can be reasonably linked to a specific consumer, computer, or other device." It is unclear if this would include

[9] Preliminary Staff Report, p. 41.

publicly available information. It should not. Because such information is already in the 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 proposed framework covers "consumer data that can be reasonably linked to a specific device." The use of the word "consumer" makes it reasonable to assume that the Commission 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); however, this is not entirely clear. We therefore request that the Commission expressly limit the framework's scope to 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).[10]
- 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).[11] 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. Service Providers

The proposed framework does not address its applicability to 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 the Commission consider the role of service providers carefully and expressly clarify that the framework does not apply directly to service providers or that only a narrower set of FIPPs obligations apply.

---

[10] 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.

[11] 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.

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.[12] 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.[13] The same principles should apply to the regulation of personal information generally, including information that is far less sensitive. Accordingly, we urge the Commission to either exempt service providers from the scope of its framework or, at least, subject them to a narrower set of FIPPs obligations.

E. Flexibility For Offline Data

If the final framework extends to consumer data collected offline, then companies will need flexibility in how they are permitted to comply with applicable FIPPs. With respect to notice, for example, we encourage the Commission 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 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

[12] 45 C.F.R. § 164.502(e)(1)(i).
[13] *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.

store.[14] 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. Similar considerations should be applied to other FIPPs.

IV. 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, regulatory, or self-regulatory requirements. We urge the Commission 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 the Commission to follow consistent U.S. precedent to impose data restrictions only when there is a specific, identifiable harm. The Commission should also balance consumer protections with cost and regulatory burdens that could prevent businesses from growing and from competing effectively.

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 the Commission considers the issues surrounding privacy notices, it should seek to avoid some of the key mistakes made by other countries in establishing overly broad and prescriptive notice obligations. As the Commission has recognized, many privacy notices are far too long and difficult to navigate.[15] 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 the Commission's suggestion that we strive for clear and concise privacy notices.

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 the Commission'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

[14] 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).
[15] Preliminary Staff Report, p. 70.

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.

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.

Areas for Further Consideration.

We agree with the Commission 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. 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. The Commission 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 direct marketing, internal and market 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 effort 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.[16] Some covered entities are even expressly excused from providing a notice of privacy practices to the individuals whose information they handle.[17]

Alternatively, the Commission 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

[16] *See* 45 C.F.R. § 164.520(b).
[17] 45 C.F.R. § 164.500(b)(1).

types of data that must be included in a notice could be readily updated by guidance from the Commission.

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 may be 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 a consumer 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. We therefore believe that the Commission is right to consider the types of uses or disclosures for which 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 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, we agree with the Commission that a company should not have to provide choice for 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, no choice should be required.

We recommend that the Commission, in its revised framework, further conclude that a company should not have to provide choice for 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. Accordingly, they should not be subject to consumer choice.[18] They include, by way of example, disclosures to service providers,[19] servicing the consumer's account, internal analytics, internal research and development, fraud prevention, audits, legal compliance, and disclosures to governmental authorities or law enforcement.[20] 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 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 to obtain and correct personal information, when it is used for credit, insurance, or employment decisions, outweighs the

---

[18] 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 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.

[19] 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 Commission does not subject the sharing of financial data with service providers to consumer choice. 16 C.F.R. § 313.13(a).

[20] The Commission'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.

costs to business of providing such a system. The Commission should consider 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 becomes more difficult. 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 that 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 the Commission 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 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

The Commission's "privacy-by-design" proposal would require a company to develop, implement, and enforce a comprehensive privacy program. The practices and procedures required to ensure compliance with such a program 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.[21] In addition, 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

As part of its "privacy-by-design" proposal, the Commission proposes that companies be required to conduct privacy impact assessments (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.

*** * ***

The GPA appreciates the opportunity to comment on this important matter. If you have any questions, or if we can otherwise be of assistance, please do not hesitate to contact me at 212.506.7213.

[21] 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.