Via email to: privacynoi2010@ntia.doc.gov

January 28, 2011

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

Re: Department of Commerce Notice of Inquiry
Information Privacy and Innovation in the Internet Economy
Docket No. 101214614–0614–01

INTRODUCTION AND EXECUTIVE SUMMARY

The Department of Commerce Internet Policy Task Force's "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" Green Paper represents a constructive and important effort to help ensure the Internet's continued role in U.S. innovation, prosperity, education, and political and cultural life.[1] Verizon[2] looks forward to continued work with the Department and other stakeholders to promote meaningful privacy protections that safeguard the privacy of personal information while allowing technological innovation to continue to thrive. As the Green Paper recognizes, consumer trust is vital to the Internet's continued growth and advancement.

The framework proposed in the Green Paper – with its focus on promoting enforceable voluntary industry codes of conduct that implement baseline Fair Information Practice Principles (FIPPs) – holds promise for achieving these goals. Industry self-regulation is uniquely suited and has a proven ability to effectively address complex issues raised by rapidly advancing technologies and the expanding number of business entities and practices involved in Internet commerce. The same substantive standards should apply to all relevant business practices,

[1] http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf ("Green Paper").

[2] "Verizon" refers to Verizon Wireless and to the wholly owned subsidiaries of Verizon Communications Inc.

regardless of the technologies or entities involved. Privacy and data protection practices should be informed by the nature and sensitivity of the data involved as well as the nature of the data's use (or re-use).

The Green Paper correctly emphasizes the importance of promoting widespread industry participation in effective self-governance programs. Industry codes of conduct should include strong accountability and enforcement components such that industry takes responsibility, in the first instance, to enforce its own codes. And the Federal Trade Commission (FTC) should backstop such industry enforcement mechanisms by, under appropriate circumstances, using its authority under Section 5 of the Federal Trade Commission Act.[3] A safe harbor model for firms that participate in self-governance programs would be a powerful motivator to encourage all companies to adopt industry standards.

Given the cross-border nature of the Internet, it is also important to ensure that the proposed federal privacy framework, employing a combination of carrots and sticks to maximize good faith adherence to effective privacy practices, is not undermined by state laws or regulations. Accordingly, the Department correctly raises the question of federal preemption of state laws. A unified national privacy framework would help ensure consistent consumer expectations regarding privacy matters, and that such expectations are consistently respected by all entities engaged in a given practice. It would also eliminate conflicts of law and facilitate the ability of companies to meet their privacy obligations without undue complexities and burdens. This builds confidence and trust in Internet commerce and in the businesses that transact on the Internet. Congress should also consider – and the Department of Commerce should support – eliminating legal uncertainties inherent in the existing panoply of state data breach notification laws, and in the 1980's-era Electronic Communications Privacy Act (ECPA).[4]

The Green Paper rightly cautions against government-imposed, prescriptive privacy regulation. Regulatory history teaches that in an environment of rapid technological change, prescriptive regulation would likely have unintended negative consequences such as stifling investment and innovation. It is important that any specific recommendations made in the Green Paper be carefully applied to avoid unintended consequences. For example, while specifying information collection and use purposes and limitations may have value in informing consumers of data use practices, a careful balance must be found so that such a requirement avoids becoming overly burdensome for the entities that have to create them and the consumers who would need to read them. Likewise, requiring businesses to provide consumers with "privacy impact assessments" (PIAs) on a product-by-product basis raises concerns.[5] While PIAs make sense in some contexts, these complex technical documents would not be helpful as customer-facing documents. To the contrary, publicizing the inner workings of companies' data security environments could have negative security and competitive implications.

The privacy framework set forth in the Green Paper has strong potential to assist the U.S. government as it works with other countries to promote increased cooperation among privacy enforcement authorities and to increase global interoperability of privacy frameworks based on

[3] 15 U.S.C. § 41.

[4] 18 U.S.C. § 2510.

[5] *See* Green Paper at 34-36.

broadly accepted privacy principles. The Green Paper correctly concludes that the U.S. should continue to support the APEC Data Privacy Pathfinder project as a model for the kind of principles that could be adopted by groups of countries with common privacy values and objectives but sometimes diverging privacy legal frameworks.[6]

DISCUSSION

I. THE U.S. SHOULD ADOPT AN APPROACH TO PRIVACY THAT INCORPORATES VOLUNTARY CODES AND SHOULD ENCOURAGE THIS MODEL INTERNATIONALLY.

A. Promoting Self-Regulation, and Avoiding Prescriptive Rules, Will Help Avoid Unintended Negative Outcomes.

The Green Paper correctly recognizes that the diversity of business models and organizations in the Internet ecosystem "counsel against attempting to develop comprehensive, prescriptive rules," especially given that "a hallmark of the digital economy is the wide variety of rapidly evolving products, services, and content that are often made available free of charge in part through the use of personal data."[7] An effective privacy framework must therefore maintain the ability to flexibly address diverse and evolving practices and technologies.

Since its inception, the general policy approach of the U.S. government towards the Internet has been driven by the recognition that government regulators cannot, when faced with complex industries and technologies, effectively and timely promote consumer welfare without active participation by the private sector and consumers themselves. Instead, U.S. Internet policy has historically stressed the dual importance of avoiding top-down government regulation and encouraging the private sector to play a leadership role in Internet administration.[8] That approach has worked well with respect to the broad range of complex technical issues that have presented themselves as the Internet has evolved. Indeed, the dramatic rise of the Internet has been due largely to successful self-governance by responsible stakeholder action through technical standards bodies, self-regulatory codes based on industry-developed best practices, and

---

[6] *See* Green Paper at 53.

[7] *Id*. at 32.

[8] For example, the White House's 1997 "Framework for Global Electronic Commerce" stated:

> For electronic commerce to flourish, the private sector must continue to lead. Innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry.… Accordingly, governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet. Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them.

http://clinton4.nara.gov/WH/New/Commerce/read.html (Washington, D.C., July 1, 1997).

ongoing public-private sector dialogues around specific issue areas.[9] Embracing that longstanding policy approach is crucial in the privacy area because rules based on static assumptions about technology and markets become quickly obsolete – and worse, lead to unintended negative consequences such as stifling investment and innovation.

In the privacy area, voluntary industry codes of conduct (with the FTC as a backstop) are uniquely suited to buttress existing privacy law, regulation, and self-governance programs. They ensure that consumers – empowered by transparent privacy standards and knowledge about which firms are complying with them – can evaluate the practices of providers with which they choose to do business. Accordingly, reliance on industry self-governance with respect to privacy practices should be the predominant model going forward.

B. U.S. Foreign Policy Should Promote a Unified Global Privacy Infrastructure by Supporting FIPPs-Based Frameworks.

Verizon agrees that it is time for the U.S. government to "renew [its] commitment to leadership in the global privacy policy debate."[10] The U.S. should promote development of a unified international privacy infrastructure that not only increases cooperation among privacy authorities around the world for purposes of enforcement and creation of seamless cross-border compliance solutions, but that also supports mutual recognition of fundamental privacy principles in participating countries' national legal frameworks. Verizon agrees with the broad consensus that the APEC Privacy Framework – the concept of a mechanism to bridge disparate national laws through cross-border accountability – bears promise and should be promoted. However, as with any multinational initiative designed to promote mutual respect for baseline principles across national laws, the utility of the APEC Framework will only be as strong as the participating national governments' willingness to promote the in-country implementation of its principles and to follow through with appropriate accountability mechanisms. As a non-legal instrument, absent additional efforts by national member governments the APEC Framework cannot offer the certainty often sought by multinational industry.

The U.S. government should also remain closely engaged with the European Commission (EC) as the EC updates its Data Protection Directive of 1995 (95 Directive).[11] As the EC continues its review of the 95 Directive, greater harmonization among the myriad European national interpretations of the Directive is of paramount importance, including the minimization of national "gold-plating" of data protection requirements, increased emphasis on flexible cross-

---

[9] Examples include the Internet Engineering Task Force, the Internet Society, the Internet Corporation for Assigned Names and Numbers, the Internet Assigned Numbers Authority, and the recently created Broadband Internet Technical Advisory Group.

[10] Green Paper at 6.

[11] The Electronic Communications Data Protection Directive, (2002/58/EC, OJ L 201, 31.07.2002) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT, a progeny of the 95 Directive applying its principles in the context of online services, was recently revised in the context of the European Electronic Communications Regulatory Framework review. The revisions to the 2002 Directive, addressing needed changes to such areas as opt-in/out and security breach notification, underscore the degree to which changes in online services necessitate revisiting the EU privacy fundamentals in the 95 Directive.

border compliance solutions, and consideration of broader global trade implications of European Union (EU) privacy directives. Such regionally-focused changes would assist in alleviating some of the often-cited extraterritorial implications of the 95 Directive. Further, it will be particularly important from a multinational perspective for the U.S. government to work cooperatively with the EU (and with other jurisdictions) toward development of data protection policies consistent with the FIPPs-based approach set forth in the Green Paper and in these comments. As the American Chamber of Commerce explained in its recent comments to the EC, such a unified approach should focus on data protection practices, not on the specific technology used to collect or store the data, or the particular entities involved.[12]

II. THE PROPOSED PRIVACY FRAMEWORK RIGHTLY PROMOTES INDUSTRY-DEVELOPED CODES OF CONDUCT.

A. Responsible Internet Businesses Embrace Privacy Practices that Ensure Consumer Confidence and Trust.

Verizon employs some of the strongest privacy practices in the industry because its reputation for trust is an important business imperative and a competitive asset. Privacy is an integral part of Verizon's culture and is engrained in its business practices and policy positions. The concept of "privacy by design" is not new to Verizon. Verizon has incorporated privacy considerations into its product planning, development and implementation processes for decades.[13] Data collection and use are essential considerations in these processes, as are data protection and security measures. For example, Verizon-provided location-based services such as VZ Navigator or Family Locator[14] have built in controls which require consumers to decide where and when to turn on the location-tracking features associated with these services on their devices.[15]

The company's privacy programs have long included an emphasis on clear communications with consumers about the information we collect, how it is used, and choices regarding certain uses of their information. Strong data security and privacy compliance programs as well as redress mechanisms are integral to company operations. Employees must complete privacy training, and safeguarding customer privacy is built into the Verizon employee Code of Conduct. Verizon also requires that its vendors and agents maintain privacy and security protections that align with our standards.

---

[12] *See* American Chamber of Commerce to the European Union, *Amcham EU's response to the Commission communication on a comprehensive approach on data protection in the European Union*, www.amchameu.eu (follow "Position Papers" to "DEC—Final POP on data protection") (Jan. 14, 2011).

[13] One relatively early example is the deployment of caller identification technology by Bell Atlantic (a Verizon predecessor) in the 1980's. When Verizon rolled out the product, the company ensured customers had the option to block the Caller-ID capabilities.

[14] VZ Navigator is a mobile device application that allows subscribers to get turn-by-turn directions to a destination, search local places of interest, and search and get a map of a particular location. Family Locator, formerly known as Chaperone, helps subscribers securely determine and receive updates on the location of family members' cell phones via a website or cell phone.

[15] In addition, customers may choose from a variety of parental control tools to protect children's privacy by blocking unwanted calls and messages, creating trusted numbers, or avoiding objectionable content.

Verizon listens and responds to its customers and other important stakeholders regarding privacy issues and concerns. For example, Verizon successfully led resistance to calls for a wireless white pages directory. It also led the industry in insisting on appropriate legal processes before online subscribers' identifying information could be provided to copyright holders alleging copyright infringement. More recently, Verizon updated its privacy policy to consolidate the privacy policies of multiple affiliates, giving consumers a one-stop shop for learning about the company's privacy policies. The updated policy is structured in a layered format designed to assist consumers' ability to find the information they are most interested in, and to understand the information at the level of detail different customers desire. Verizon is proud to have received numerous accolades for its strong commitment to privacy.[16]

Many companies understand it is in their interest to implement strong privacy practices because there is a collective benefit that accrues from the growth that occurs when consumers are confident about using Internet services and capabilities. The entire ecosystem benefits when consumers understand who has access to their information and how it will be used, are comfortable that their information will be adequately protected, and are empowered to make meaningful choices about the collection and use of their private information. Over a decade ago, the imperative to ensure that consumers could evaluate the data practices of businesses operating on the Internet led to the development of online privacy policies. Privacy seal programs such as those administered by TRUSTe and BBBOnline began to serve as widely recognized trust marks for consumers who look to do business with trusted entities and for businesses that choose to incorporate the privacy best practices associated with these voluntary regimes.

Over time, as technology and data use practices have evolved, consumers have expressed increased levels of concern about online advertising as complex data practices emerged. In response to the FTC's recommended best practices for online behavioral advertising, a broad representation of the Internet advertising ecosystem is now actively implementing a comprehensive set of Self-Regulatory Principles for Online Behavioral Advertising.[17] This regime, which covers thousands of different firms involved in online behavioral advertising, establishes specific requirements for entities that collect, use or share data for online behavioral advertising purposes. For example, advertisements delivered using online behavioral advertising techniques will carry a uniform icon that leads to a consistently-worded notice about the ad and the information used to deliver it, as well as a mechanism for the consumer to opt-out of the ad campaign and any similar campaigns from firms participating in the campaign. The program also includes accountability and enforcement mechanisms to ensure compliance. Verizon was an

---

[16] *See, e.g.*, "Verizon Named to Dow Jones Sustainability North America Index for the Second Straight Year," http://newscenter.verizon.com/press-releases/verizon/2010/verizon-named-to-dow-jones.html (Sep. 20, 2010) (noting that some Verizon's highest-scoring areas were for its work in privacy protection); "Consumers Rank Verizon as Most Trusted Communications Company to Protect Customer Privacy, in Ponemon Institute Survey," http://newscenter.verizon.com/press-releases/verizon/2010/consumers-rank-verizon-as.html (Feb. 26, 2010).

[17] *See* Self-Regulatory Program for Online Behavioral Advertising, http://www.aboutads.info/ ("Self-Regulatory Principles"). The program addresses the principles set forth in the FTC *Staff Report on Self-Regulatory Principles For Online Behavioral Advertising*, http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (Feb. 2009).

active participant in the development of these principles, and is now deploying the icon and consumer notice provisions that the principles set forth on applicable Verizon advertisements.

Industry has shown its commitment to developing, and its ability to develop, robust codes of conduct that implement baseline government-approved principles.[18] The U.S. government should support and promote such strong self-regulatory programs and should encourage broad-based support and adherence to them.

B. Properly Implemented Green Paper Recommendations Can Promote Widespread Adherence to Effective Privacy Practices.

The U.S. government should embrace a privacy framework that promotes voluntary codes of conduct and that combines "carrots" *and* "sticks" to maximize the participation of industry stakeholders in such codes. The principal "carrot" to incentivize firms to embrace industry codes should be a safe harbor mechanism protecting firms that participate in good faith. As far as possible, enforcement mechanisms should look to industry accountability programs as the first line of defense. The "stick" should be government enforcement under Section 5 of the FTC Act.

The Department should establish the Privacy Policy Office (PPO) contemplated by the Green Paper. The PPO should work with industry stakeholders and the FTC to develop a set of baseline FIPPs that would form the basis of voluntary codes of conduct that contemplate emerging privacy issues.

1. The Privacy Framework Must Focus on Data Practices and Must Be Neutral With Respect to Technologies and Entities.

In order for a privacy framework to effectively work, two principles must be met. First, the voluntary codes must be designed to apply to data *practices*. Second, the codes must be neutral, or apply equally, with respect to particular technologies or business entities. While different industry segments may need to implement privacy requirements in ways appropriate to their operations, all relevant stakeholders must be required to adhere to the same standards for protecting privacy. For example, if customer consent is required for the use of data for a particular purpose, the appropriate method for obtaining the consent may depend on a number of variables including the entity's business practices or the medium through which an entity collects the data (e.g., a call center, Web site, or retail store), but the *level* of consent should not vary. Failure to consistently apply the framework to all relevant entities and practices would result in inconsistent data protection and unfair business advantages or disadvantages. Inconsistent data protections might result in consumer confusion and would leave consumers unable to navigate or understand what levels of protection and control are afforded to them in like circumstances.

---

[18] Industry has also launched best practices programs in other areas where technologies and practices implicate consumer privacy. For example, CTIA has issued its "Best Practices and Guidelines for Location-Based Services," which requires location-based service providers to inform mobile users on how their location data will be used, to disclose and protect location-based data, and to empower consumers to decide whether or not to authorize disclosure. *See Best Practices and Guidelines for Location-Based Services, Version 2.0,* http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf (Mar. 23, 2010).

Unfortunately, inconsistent privacy protection requirements presently exist and consumers are likely to be unaware that privacy protections afforded to them by certain communications companies and cable operators are not required from other entities that may collect and use the same types of data. For example, the Cable TV Privacy Act of 1984[19] has privacy protection requirements that apply to the collection, use, and sharing of information obtained over cable systems, but that do not apply if a company collects the same data via other means (e.g., a broadband connection). Under 47 U.S.C. § 551, cable operators that fail to adhere to specific notice and consent requirements are subject to private rights of action which can include punitive damages and attorneys' fees – but consumers who choose to get their television viewing content from non-cable entities do not receive the same protections, even where the same data is collected. Any national privacy framework should remedy such inconsistencies to ensure that consumers can expect the same level of protection regardless of the entity with which they do business. Likewise, the framework must avoid creating any new inconsistencies.

2. Appropriate Enforcement is an Important Component of Self-Regulation.

Industry-based voluntary codes should include strong accountability and enforcement mechanisms. For example, firms supporting the Self-Regulatory Principles for Online Behavioral Advertising described above will be subject to accountability programs administered by the Direct Marketing Association and the Council of Better Business Bureaus (CBBB) to confirm that they are complying with their obligations. One aspect of the accountability program is a complaints-driven process modeled after certain self-regulatory programs operated by the National Advertising Review Council of the CBBB. Under these models, divisions such as the Children's Advertising Review Unit (CARU) and the Electronic Retailing Self-Regulation Program (ERSP) review complaints and act as arbitration bodies. They advise participating firms to modify advertising or discontinue advertising as necessary to comply with truth in advertising standards, and where necessary refer matters to the FTC for enforcement action if concrete steps are not taken to achieve compliance. This complaint-based model is not the only tool in use to confirm that "a private sector organization's data use is consistent with its obligations."[20] Under the Online Behavioral Advertising Self Regulatory program, the CBBB is also instituting a technology-based monitoring program under which it confirms that participants have appropriately implemented the icons and links required by the Principles.

Government enforcement provides an important backstop to industry self-governance. There may be firms that, while taking advantage of the trust created by industry self-governance, seek to profit by not adhering to industry-developed standards or by purporting to adhere to them but not doing so in good faith. The FTC should, where appropriate, prosecute such conduct because it is those bad actors that put consumers at risk and damage confidence in the overall ecosystem. The FTC has authority under Section 5 of the FTC Act to investigate and bring enforcement actions against firms that engage in "unfair or deceptive" acts. For example, the

[19] 47 USC Sec. 551.

[20] Green Paper at 71.

FTC has brought enforcement actions against purveyors of spam and spyware[21] and those companies that inadequately protected the security of consumer data.[22]

The FTC should have sole responsibility for enforcing the proposed national policy framework. Spreading enforcement responsibilities across different government agencies would reduce the ability of FTC enforcement officials to ensure consistency, legal certainty, and administrative efficiency. For the same reasons, the framework should not authorize private enforcement actions. Doing so would create substantial risks of inconsistent enforcement, and may deter stakeholders from participating in codes of conduct. The uncertainty associated with contending with private rights of action would substantially reduce the effectiveness of the self-governance framework.

3. Safe-Harbor Provisions Will Promote Broad Good Faith Participation in Self-Regulatory Regimes.

Creating a safe harbor for companies that adhere to industry-developed privacy standards is essential. As the Green Paper observes, such a safe harbor provision will reinforce the industry's incentives to develop self-governance practices that address emerging issues, and to follow such practices.[23] A safe harbor rewards companies that play by the rules, and properly subjects those that do not to disciplinary action.

4. Flexibility Is a Key Advantage of Policies that Promote Industry Self-Regulation.

The enhanced FIPPs contemplated by the Green Paper must remain sufficiently flexible such that codes of conduct can be implemented in a manner that contemplates new and emerging codes of conduct with enough flexibility to address particular privacy issues or contexts. Overly prescriptive or overly detailed FIPPs would defeat the viability of the Green Paper's dynamic framework and should be avoided.[24]

Also, given the importance of preserving flexibility within industry-specific FIPPs implementations, a government "seal of approval" is not needed. An ex ante "seal of approval," or a rule that approves industry standards after they have been in use for a specified period of

---

[21] *See e.g.*, FTC Press Release, "Judge Agrees with FTC, Orders Spammers to Pay More Than $2.5 Million and Stop Selling Bogus Weight-Loss and Anti-Aging Products," http://www.ftc.gov/opa/2008/02/sili.shtm (Feb. 4, 2008); "Spyware Seller Settles FTC Charges; Order Bars Marketing of Keylogger Software for Illegal Uses," http://www.ftc.gov/opa/2010/06/cyberspy.shtm (June 2, 2010).

[22] *See e.g.*, FTC Press Release, "ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress," http://www.ftc.gov/opa/2006/01/choicepoint.shtm (Jan. 26, 2006).

[23] Green Paper at 43.

[24] The Green Paper states that "[a] baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans." *Id*. at 58. Flexible codes of conduct can be crafted to avoid conflicts, and can be modified to the extent conflicts may arise.

time,[25] would reduce the very flexibility that makes the suggested framework ideal for addressing privacy practices and technologies as they arise in different contexts.

C. Developing Appropriate Privacy Principles.

1. Enhancing Transparency: Issues Raised by the Privacy Impact Assessment Concept.

As the Green Paper observes, existing privacy policies, disclosure notices, and notice-and-choice models sometimes fail adequately to inform consumers and empower them to make informed choices about their privacy preferences.[26] In keeping with its longstanding commitment to privacy as a consumer trust issue, Verizon understands that consumers deserve clear and easy access to notice of what information is collected and how it is used and shared with others, and provides consumers with ready access to tools that provide them the ability to control certain uses of their information. In developing and implementing new products and services, effective and comprehensive privacy controls must be considered and put in place at introduction. As discussed previously, Verizon sought to increase transparency when introducing its revised privacy policy by creating a one stop shop for information about privacy practices across Verizon's lines of business, products and services, with clear information allowing consumers to set their marketing preferences. Verizon has also begun implementing the enhanced transparency measures required by the Self-Regulatory Principles for Online Behavioral Advertising. We continually look for ways to more clearly inform our customers and Web site visitors about our privacy practices and their choices.

With regard to enhanced transparency, the Green Paper suggests that businesses might prepare and disclose privacy impact assessments (PIAs) in connection with new products or services. "If prepared in sufficient detail and made public, PIAs could create consumer awareness of privacy risks in a new technological context, where norms are not yet clear."[27] Verizon agrees that the studies cited referring to PIAs associated with radio frequency identification (RFID) and smart grid technology provide businesses with useful information about the privacy implications of emerging technologies and, as such, are useful in encouraging businesses to think through the privacy implications of adopting emerging technologies. However, there is no basis for using PIAs outside of the government context as consumer-facing documents. Regular publication of PIAs for consumer review would be impractical and counterproductive.

PIAs are complex assessments intended for technical audiences, primarily in the public sector. As currently required,[28] PIAs are used as a change management tool for federal government employees working on a program or accessing a system to understand how to best integrate privacy protections while working with personally identifiable information (PII). The PIA template in use by the Department of Homeland Security (DHS), for example, calls for a comprehensive rendering of the lifecycle of personal information, in all its forms, in every

[25] *Id*. at 53.

[26] *Id.* at 31-33.

[27] Green Paper at 34-35.

[28] *See* Section 208 of the E-Government Act of 2002 (codified at 44 U.S.C. § 3501).

primary and derivative use, detailing both relationships and responsibilities, as well as risks and mitigations, including descriptions of the statutory and regulatory authority for operating the project; the authority to collect the information at issue; enumeration of all types of PII to be used in native or derivative form; explanation of where the information comes from (e.g., identification of all sources, including identification of commercial partners); how and why the information will be used; record retention schedules; administrative (e.g., training) uses; and technical and physical controls.[29] Whatever importance PIAs have in the governmental context, these exhaustive documents are too complex and difficult to understand to have utility as consumer-facing documents.

Moreover, a number of issues arise with publication of the detail required by a PIA. To broadcast the internal workings of an information security environment is to give would-be wrongdoers a roadmap to data flows and the architecture of a firm's data defenses. Business confidentiality and competitively sensitive information could be compromised by publication of PIAs including potential disclosure of trade secrets or business plans. In addition, the commercial relationships between a company and its information suppliers are often themselves confidential.

When new technologies emerge, like smart grid and RFID, consumers should be made aware of the privacy impacts of the technologies. The reports cited in the Green Paper show that such an educative role is being filled by government and trade associations. Disclosing to consumers product-by-product PIAs relating to private sector businesses, however well intended, would not play a similarly productive role.

2. Purpose Specifications and Use Limitations Should be Proportional to Data Sensitivity and Use.

The Green Paper proposes that firms seek to better align consumer expectations and actual information practices by stating specific reasons or objectives for collecting personal information, and then using the information only for the specific ways enumerated, and no others.[30] Verizon agrees that consumers should know why information is collected and how it is used, but there is a tension between the level of specificity required by a detailed, complete purpose specification listing and the simple, clear notices most preferred for consumer notification of privacy practices.

Customer information is usually collected for myriad purposes, such as service order processing, installation, authentication and verification, service delivery, maintenance and repair, product development and improvement processes, inventory control, network management, marketing, advertising and sales initiatives that might provide consumers with coupons, package offerings, or information about available service enhancements or options. Information is also used to establish credit worthiness, to collect unpaid balances, to prevent fraud or security risks, and is required by legal obligations. Specifying the details of every possible use of information

[29] *See* DHS, Privacy Impact Assessment Guidance, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf.

[30] Green Paper at 37-40.

for service delivery and operations alone is likely more information than a consumer has the ability or desire to digest.

The nature of any data protection practice (in this case, the level of specificity in the notice) should be informed by what a consumer would reasonably expect. It is not appropriate – or beneficial – to overwhelm the consumer with detailed use specification notices for uses that reasonable consumers would expect and would not find objectionable. Indeed, a highly detailed notice listing dozens of purpose specifications could be used as a vehicle to "slide in" certain uses that *should* be more clearly communicated to the consumer but that may go unnoticed amidst the flood of detail. Thus, appropriate purpose specifications and use limitations should be proportional to the form and type of data involved, its sensitivity, and the particular uses, and be constructed to deliver useful information to consumers as they choose to interact with a company.

3. Industry Self-Governance Should Include Evaluation and Accountability Mechanisms.

The Green Paper also correctly identifies accountability as an important means of ensuring the value of a FIPPs-based framework.[31] As discussed above, industry self-governance initiatives have sought to develop enforcement mechanisms by establishing accountability agents that employ various techniques – ranging from self assessments, to complaint arbitration, to the use of monitoring technology, to combinations of these approaches and others – to ensure compliance with industry codes. Appropriate accountability programs should be a part of each enforceable, voluntary code of conduct developed through the processes outlined in the framework. It is important that an enhanced accountability FIPP not include overly prescriptive requirements for auditing or monitoring of data protection and privacy practices given the diversity of entities and practices to which FIPPs must apply.

III. CONSUMERS AND BUSINESSES WOULD BENEFIT FROM UNIFIED NATIONAL STANDARDS

A. State Breach Notification Laws.

The Green Paper correctly recognizes the burdens placed on businesses to comply with state data breach notification laws in existence today. While state laws requiring consumer notification in instances where sensitive data has been breached are largely consistent in their desired goal, detailed requirements, such as the trigger for notification, the timing of notification, the content of notification, the manner of notification, and the regulatory entities that must be notified, often differ. The challenge facing businesses is that they must ensure compliance with *all* applicable state requirements *simultaneously*.[32] These variations raise businesses' costs and increase the difficulty of compliance without necessarily improving individuals' privacy

[31] *Id*. at 40-41.

[32] There are at least 49 different breach notification laws throughout the US, which cumulatively comprise dozens of different elements.

protections. Accordingly, any national policy framework for security breach notification should preempt the divergent state laws.[33]

A federal framework should not adopt the terms found in certain state laws under a "lowest common denominator" approach. Rather, the development of the national framework should be viewed as an opportunity to take a fresh look to determine what requirements make the most sense for businesses and individuals alike. To that end, the security breach notification framework should appropriately address the following three issues.

Definition of information subject to the notification requirements. It is important that any breach notification requirements only apply to information that truly represents a risk of identity theft. "Personal information" should be carefully defined in the framework so that it covers commonly accepted sensitive information, such as an individual's government issued identification number or financial account information. At the same time, the definition should exclude information that is publicly available through the Internet or public records or of little sensitivity, such as random business identifiers.

Risk/harm analysis. Notice to customers should be required when the entity that possesses the data determines that there is a reasonable risk of identity theft, fraud, or other unlawful conduct arising from the breach. This standard, which already exists in a majority of state laws, would encourage entities that possess data to develop and widely deploy protective measures, such as encryption, data anonymization or other technological security measures that render data indecipherable and unusable by data thieves. Because individuals would only be notified of a breach when their data is at risk for misuse, they would be more likely to take the notices seriously, watch diligently for identity theft, and take other measures to protect themselves. On the other hand, receiving multiple unnecessary or irrelevant notices might lead consumers to ignore all such notices, including one that might represent a true risk of harm.

To the extent an entity determines that there is a reasonable risk of harm from a data breach, each affected individual should receive notice, regardless of the number of records accessed. However, entities should be required to report to the government only those breaches of sufficient scope where regulators or law enforcement may have an interest in reviewing the circumstances of the breach.

Timeliness of notification. While it is important that individuals receive timely notice if a breach has occurred, an equally important goal is for entities to investigate the breach, restore the integrity of the data system, and identify affected individuals so that notices are meaningful and arm individuals with the facts they need to take appropriate action. Because data breaches vary in size and complexity and may present significant challenges in determining their nature and scope, a one-size-fits-all requirement of *x* days from the day an entity learns of a breach for notice to be provided should be avoided. Instead, entities should be required to make notice in a timely fashion, without undue delay subject to the actions necessary to respond to the breach.

[33] Indeed, given the widespread adoption of inconsistent state laws, federal legislation would be irrelevant if it does not preempt the patchwork of state laws.

B. State Privacy Laws Should Not Be Permitted to Unravel the Unified Federal Privacy Framework.

The Green Paper seeks comment on how narrow or broad the preemptive effect of a national FIPP-based commercial data privacy policy should be.[34] Federal preemption is required for a national privacy framework so that enforceable industry codes maintain consistency. Even minor differences in state laws that seek to implement FIPPs could present an undue burden on entities that serve a multi-jurisdictional customer base without any substantive benefit to consumers. In fact, consumers benefit when they have a consistent and reliable set of practices that apply regardless of the state where they work, live, vacation or travel for any reason. Specifically, state enforcers should not be permitted to disregard the safe harbor provisions of a federal framework, because deviations from a consistent set of practices would reduce the incentives for firms to adopt voluntary codes of conduct. For the same reason, states should not be permitted to pass prescriptive legislation that "ratchets up" the substantive privacy standards set forth in the federal framework or in the voluntary codes of conduct. While there may be some superficial appeal to the notion that federal law should be "no less protective"[35] than existing state laws, such a philosophy would be misguided. A thoughtful and balanced approach that is protective of consumers while allowing entities that serve those consumers to focus their efforts on a single, consistent set of obligations is the correct federal framework, and the balance it creates should be preserved.

Of course, most if not all states have unfair and deceptive trade practices or consumer protection laws similar to Section 5 of the FTC Act, and state attorneys general already have authority to enforce those laws. Thus, companies are already subject to potential state enforcement action to the extent they fail to comply with their own privacy policies or with industry codes of conduct they have adopted.

C. Congress Should Consider Revising the Electronic Communications Privacy Act (ECPA).

The Green Paper indicates that the Department should review ECPA "with a view to addressing privacy protection in cloud computing and location-based services."[36] ECPA is a complex statute that seeks to balance various interests, and any revisions should be done carefully. With that in mind, legislators should consider ways to ensure ECPA and its state counterparts do not present unnecessary obstacles to companies seeking to provide customers the services that they want, including cloud and location-based services.

The key principles of technological neutrality and aligning data practices with consumer expectation discussed throughout these comments should also inform revisions to ECPA. Compliance with ECPA's requirements should not depend on the nature of the technology, but rather on the nature of the information sought and on Congressional determinations about consumers' reasonable expectations of privacy. Asymmetrical requirements should be avoided;

---

[34] Green Paper at 61-63.

[35] *Id*. at 74.

[36] *Id*. at 63.

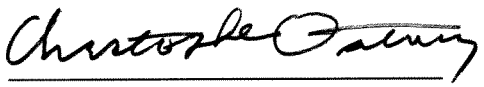
companies with similar types of consumer data should be subject to the same standards, including equivalent standards for obtaining consumer consent when seeking to use the data for equivalent purposes.

Uncertainty about the application of ECPA may impede innovation and hinder the application of new technologies by businesses.[37] Some of this uncertainty is due to the patchwork of state regulations, which although created with the best intentions of complementing federal regulation, has had the unintended consequence of creating confusion. As noted above, state variations, even where they attempt to maintain consistency, are not suitable for the creation of a balanced, effective framework. Although the framework of the federal wiretap laws has served as a general model for many states, some states have modified it in ways that create ambiguities, including ambiguities about the nature of the consent needed in different contexts. Additionally, as many of these laws were initially crafted for the telephone network, they become more difficult to apply to Internet-based communications. Any revisions to ECPA should seek to reduce such ambiguities and ensure more symmetrical and more consistent consent requirements across all states.

CONCLUSION

The privacy framework set out in the Green Paper represents the right approach for ensuring that the Internet will continue to thrive as consumers – empowered by widespread adherence to industry-developed privacy standards – drive the deployment of new products and services with confidence their privacy preferences and expectations are respected. Consumers will be well served by a policy promoting enforceable, flexible industry codes of conduct that implement technologically-neutral baseline FIPPs.

Respectfully submitted,



Kathleen G. Zanowic
Chief Privacy Officer
VERIZON
1320 North Court House Road, 9th Floor
Arlington, Virginia 22201
(703) 351-3156

Magnolia Mansourkia
Karen Zacharia
Christopher Oatway
VERIZON
1320 North Court House Road, 9th Floor
Arlington, Virginia 22201
(703) 351-3199

John T. Scott, III
VERIZON WIRELESS
1300 I Street N.W., Suite 400 West
Washington, DC 20005

[37] *Id.* at 65 n.186.