Before the
DEPARTMENT OF COMMERCE

In the Matter of	)	
	)	
Information Privacy and Innovation in the Internet Economy	)	Docket No. 100402174-0175-01
	)	RIN 0660-XA12
	)	
	)	
	)	

COMMENTS OF VERIZON AND VERIZON WIRELESS

Verizon and Verizon Wireless ("Verizon") appreciate the opportunity to provide input to the Department of Commerce ("Department") Internet Policy Task Force as it launches its Privacy Innovation Initiative. In its Notice,[1] the Department has appropriately recognized the importance of establishing an environment consistent with longstanding information use practices and individual privacy expectations while encouraging innovation and increased participation in the Internet.

At Verizon, protecting the privacy of customer information is an important and well-established priority. Consistent with the Notice's focus, Verizon recognizes that consumers will use the full capabilities of its communications products, services, and networks only if they trust that Verizon will respect their privacy preferences and use their information in accordance with their expectations. Verizon remains committed to maintaining strong and meaningful privacy protections for consumers as communications technologies and services rapidly advance.

[1] Department of Commerce, *Information Privacy and Innovation in the Internet Economy*, Notice of Inquiry, 75 FR 21226 (2010) ("Notice").

Fundamentally, privacy protections should include a clear disclosure of what information is being collected, how it is used, and with whom it is shared. Consumers should also have ready access to tools that allow them to control the use of their information for certain purposes. In recent years, privacy requirements that attempt to apply these principles have proliferated in the form of state and federal laws and regulations, international in-country and region-specific requirements, and self-regulatory programs. However, as the Department has acknowledged in the Notice, the existence of multiple approaches and requirements can complicate consumers' ability to understand how their information is being protected and companies' ability to implement all applicable rules, especially where rules may conflict or where technologies and services converge such that jurisdiction is difficult to determine.

Accordingly, a unified approach to privacy protection that incorporates the principles of consumer transparency and control and applies them equally – regardless of the particular technology or business model used in the collection of such data – would improve consumer knowledge while creating efficiencies for companies. Such an approach would allow businesses to devote greater resources towards innovative business models, to the benefit of consumers who could take advantage of new services with a clear understanding of the data security and privacy controls available to them.

As such, the Department should continue to identify and examine whether domestic and foreign privacy laws conflict with each other in a manner that imposes undue compliance burdens for business or where barriers to commerce exist in specific states or countries. The Department should promote flexible programs that meet consumers' privacy expectations while allowing for continued innovation in the

information economy. In addition, the Department should encourage the development and use of tools that enhance individuals' ability to control their private information and support programs that increase consumer education around privacy protections and controls.

DISCUSSION

I. The Harmonization of International, Federal, and State Privacy Requirements Would Benefit Consumers and Businesses.

A. International Laws

In the international environment, privacy laws tend to be based on the location of the data subject or where the data collection occurs. Yet these bases for differing laws make little sense in today's business environment. Verizon, which operates in 159 countries on six continents, serves customers on its own network and also manages network capacity obtained from dozens of other carriers on behalf of its business and multinational customers. To most efficiently serve its customers, Verizon, like many other multinational businesses, deploys central servers and host computers that facilitate remote access by authorized persons located around the world. As a result, the notion of "where data collection occurs" is difficult to fix for purposes of a national law's definition, and there are substantial administrative burdens attendant to deploying services under this type of collection-based privacy system.[2]

Moreover, existing national and multi-national legal treatments of cross-border data flows – and related privacy implications – vary greatly and impact both privacy

[2] The extent of this problem is increasingly apparent in the context of cloud computing. Cloud computing involves the exchange of data in the IP cloud among myriad systems and databases within that cloud and therefore does not lend itself to geographic and jurisdictional certainty.

compliance and businesses' approaches to service deployment. In some cases, this balkanization impedes communications, trade, the free flow of information, and certain business activities. The EU Data Protection Directive was enacted to remove such obstacles to the flow of data among member states, but has requirements that differ from those in the rest of the world.

Attempts to overcome jurisdictional differences – through bi-lateral and multi-lateral agreements and commercial terms – have been slow to develop and are not always uniformly effective. One of the seminal efforts in this area was the Department's negotiation of the EU-U.S. Safe Harbor Framework to ease compliance with 1995 EU Data Protection Directive.[3] This Framework has been successful in facilitating global commerce for some industries transferring data between the U.S. and EU. However, the Safe Harbor rules cover only some commercial organizations, while other entities, including telecommunications service providers, are not presently eligible and must implement European standard commercial terms (or certain other approved terms) between and among entities collecting or processing data in the EU.

Moreover, the Safe Harbor rules only address data flows between the U.S. and EU countries. For organizations that engage in multi-regional data transfers, there is no single privacy paradigm that provides a global set of rules and protections. This gap can be a substantial obstacle to innovation and the advancement of new services.

[3] The Safe Harbor Framework consists of seven privacy principles, 15 frequently asked questions and answers (FAQs), the European Commission's adequacy decision, the exchange of letters between the Department and the European Commission, and letters from the Department of Transportation and Federal Trade Commission on their enforcement powers. The documents are listed and published at http://www.export.gov/safeharbor/eu/eg_main_018493.asp.

The recently developed Binding Corporate Rules (BCRs) also serve as an important tool for compliance with national data protection rules under the EU Directives. BCR negotiation and implementation remain, however, member state-by-member state tasks, without the benefit of mutual recognition among national data protection authorities for nationally-approved BCRs.

Finally, the Asia Pacific Economic Cooperation (APEC) Privacy Framework requires that a company bind itself publicly to adhere to agreed principles for cross-border flows of personal information. APEC's use of flexible principles designed to facilitate cross-border transfer among APEC member countries is a welcome development for U.S. companies seeking to do business globally. The Department's role in developing the APEC Cross Border Privacy Rules and working with its counterparts across APEC economies on a project to implement the framework, known as Data Privacy Pathfinder, has been particularly helpful to the business community. The Pathfinder's illustration of how APEC's principles should be applied benefits both national authorities and entities seeking to conduct cross-border data transfers.

However, the utility of the APEC Framework will only be as strong as national governments' willingness to promote the adoption of its principles and follow through with compliance. While the concept of a mechanism to bridge disparate national laws through cross-border accountability has promise, as a non-legal instrument, it does not offer the certainty often sought by multi-national businesses.

B. U.S. Federal Laws and Self-Regulation

In the United States, privacy laws have evolved primarily from concerns about specific types of information and its collection and use in specific industry segments or

sectors. This approach seeks to protect particular categories of data for which sensitivity and risk are believed to be the highest. For instance, laws governing health, financial, and communications information were enacted to provide heightened treatment for this sensitive information.

The sectoral approach, however, may lead to consumer confusion. Consumers may become accustomed to certain aspects of the sector-specific requirements they encounter, such as medical privacy notices with which they are presented when they visit a doctor or credit card privacy statements they receive in the mail. In most cases, though, consumers lack a clear sense of what particular information is protected under which set of rules or what their rights are with respect to the use of their data by the specific entities covered by the applicable sectoral privacy rule.

Moreover, the sectoral approach can cause an uneven application of rules. When the same information is gathered and used in provisioning similar services, but the privacy obligations that apply to individuals' information are different based on how specific sectoral laws define "covered entities," consumers can be harmed. For example, the Communications Act's definition of "telecommunications carrier" was adopted almost 15 years ago – long before the explosive growth in Internet-related communication applications, services, and tools. Requiring that only certain competitors comply with the Act's and the FCC's robust privacy requirements, while allowing others to avoid them altogether, distorts competition. The resulting cost advantage could translate to a lower price that would drive consumers to these companies. Yet these same consumers would likely mistakenly believe that the same privacy protections they have available to them when their information is held by a "telecommunications carrier" would

continue.

To avoid this harm to competition and consumers, the privacy protections afforded to the collection and use of data deemed sensitive in a specific sector should be required of all parties collecting or using that sensitive data, regardless of nominal sector. The notion of a "covered entity" based on traditional industry silos is outdated and has the end result of regulating the same service in different ways. These differences and the consequent inconsistency in privacy protections are generally unknown to consumers.

While the sectoral laws in the United States have responded to specific areas of concern, effective self-regulatory programs have developed in other areas and complement those laws. Examples of such programs include the BBB Advertising Review Services,[4] the CTIA Best Practices and Guidelines for Location-Based Services,[5] and the recently released Self-Regulatory Principles for Online Behavioral Advertising.[6] These self-regulatory programs promote innovation while maintaining privacy protections as a mainstay of new services or technologies. Self-regulatory programs leverage the particular expertise of industry players that understand the way in which consumer information is collected and used and what controls can best afford consumer privacy protection while allowing market and technical innovations to continue. Self-regulation also offers greater flexibility for industry to respond effectively to new privacy

---

[4] BBB Advertising Review Services, http://www.bbb.org/us/Advertising-Review-Services (last visited June 11, 2010).

[5] CTIA Best Practices and Guidelines for Location-Based Services, http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf (April 2, 2008).

[6] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising*, http://www.iab.net/media/file/ven-principles-07-01-09.pdf (July 2009).

concerns, helping consumers avoid emerging threats.

C. State Laws

Privacy laws and regulations that establish controls around the collection, use, or protection of customer information exist in nearly every state. State legislatures have forged state-specific data breach notification laws and have been active in areas including data security, data retention and destruction, use and display of social security numbers, and privacy-protective marketing practices. Not surprisingly, the legal requirements of the many state-specific laws vary. For example, while state laws requiring consumer notification in instances where sensitive data has been breached are largely consistent in their desired outcomes, 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.

Businesses like Verizon that have a wide geographical footprint must ensure they comply with *all* applicable state requirements simultaneously. Businesses approach the multiplicity of state privacy laws by choosing the most restrictive requirements across the board, implementing different rules for different states, or using some combination of these approaches. Regardless of the approach selected, these variations raise businesses' costs and increase the difficulty of compliance without necessarily improving customers' privacy protections.

In addition to compliance, businesses must closely follow and participate in, to the extent possible, the legislative processes around state privacy laws in all of the jurisdictions where they do business. State legislatures have been actively modifying existing privacy laws and developing new laws. Over 100 state data-security and privacy

laws have been enacted in the past five years. When state legislative sessions are in progress, it is not unusual for Verizon to be monitoring or engaged in discussion on twenty different privacy-related bills. When new legislation becomes law in a given state, businesses must conduct a comprehensive reevaluation of their privacy policies and practices. Such significant inefficiencies would be averted by the harmonization of state privacy laws.

II. The Department Should Promote Innovation and Consumer Education.

The Department should support the development of privacy-enhancing technologies and processes that further consumer understanding and engagement in decisions about the use of their personally identifiable information. For instance, identity services are being developed that enable online authentications and help consumers manage their privacy and information use and sharing preferences. As the FCC recognized in its National Broadband Plan, trusted "identity providers" could help consumers manage their data in a way that maximizes the privacy and security of the information. Through the development of appropriate safe harbor provisions, services that maintain identity management and authentication components could be acknowledged as trusted intermediaries. Such services would safeguard information by following strict guidelines, audit mechanisms, and reporting obligations to help consumers manage their online identities across Websites and application providers to better utilize new technologies and services they choose. And consumers would benefit from the innovations that businesses can provide on top of the identity and profile data that consumers are willing to share.

The Department should also encourage businesses to consider privacy principles

and appropriate consumer privacy controls as they design and develop products and services, rather than retro-fit protections after problems have arisen and consumer privacy has been compromised. Verizon strives to build privacy controls into new products and services within the development process so that controls are as effective and comprehensive as possible.

CONCLUSION

Verizon supports the Department's goals as it examines the impact of the current privacy framework on Internet commerce and innovation. In light of the compliance complexities required of businesses from the myriad international, federal, and state privacy requirements, and the need for greater consumer understanding of privacy protections and controls, the Department should promote a unified approach to privacy that recognizes and incorporates the flexibility offered by self-regulatory programs. The Department should play a leadership role in the international environment to ensure that U.S. privacy positions are represented as new approaches to privacy are considered in other parts of the world. Finally, the Department should emphasize the importance of consumer outreach and education and foster better understanding of general consumer privacy programs and controls.

Respectfully submitted,

Karen Zacharia
Mark J. Montano
VERIZON
1320 North Courthouse Road
9th Floor
Arlington, VA 22201
(703) 351-3158

Attorneys for Verizon

John T. Scott, III
Verizon Wireless
1300 I Street, N.W.
Suite 400-West
Washington, DC 20005
202.589.3760

Attorneys for Verizon Wireless

Michael E. Glover
Of Counsel

June 14, 2010