Before the
National Telecommunications and Information Administration
Washington, DC 20230

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

To: National Telecommunications and Information Administration

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Danielle Coffey
Vice President, Government Affairs
TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

TABLE OF CONTENTS

SUMMARY 2

DISCUSSION 3

I. TIA Members Support Privacy Protections for Consumers. 3

a. Consumer Privacy is Important to the Adoption of Technological Advances. 3

b. TIA Members Support the Current Privacy Framework Based on Notice, Choice, and Data Security, which, Coupled with Robust Enforcement, will continue to be Effective in Protecting Consumer Privacy. 4

c. Where Additional Protections are Necessary, Self-Regulatory Regimes are an Effective and Flexible Complement to Government Regulation. 5

II. It is Vital That Consumer Privacy Protections Maintain Flexibility for Different Business Models and Technologies to Promote Innovation, Which Will Ultimately Benefit Consumers and Our Economy. 6

a. Consumer Demand for Technological Innovation has Resulted in Greater Consumer Choice and Significant Benefits to Consumers and the Economy. 6

b. Unduly Burdensome Restrictions Related to Consumer Privacy May Impede Technological Innovation and Reduce Consumer Choice. 7

c. Privacy Regulation Should be Technology Neutral 7

III. The United States Leads the World in Technological Innovation, Due In Part to Flexible and Balanced Privacy Laws. When Looking to Privacy Laws and Regulations in Other Countries as Models, it is Important to Focus on Models that Preserve Flexibility while Protecting Privacy 8

a. Highly Restrictive Privacy Requirements may Hamper Innovation 8

b. APEC's Privacy Framework and the Cross Border Privacy Rules Represent an Appropriate Model For Protecting Privacy While Preserving The Flexibility Necessary For Innovation. 9

CONCLUSION 11

Before the
National Telecommunications and Information Administration
Washington, DC 20230

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

To: National Telecommunications and Information Administration

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA") hereby submits comments to the National Telecommunications and Information Administration ("NTIA") in the above-captioned proceeding. TIA, on behalf of its members, appreciates NTIA's interest in the important area of the interplay between information privacy and innovation in the Internet economy. TIA believes that an appropriate privacy framework balances consumer privacy concerns with the consumer benefits arising from technological innovation and business model flexibility in communications and Internet commerce. Thus, as explained below, TIA supports the privacy framework now in place in the United States, which focuses on notice, choice, appropriate data protection, and robust enforcement. To the extent NTIA believes that additional protections are required, it should work to facilitate the expansion of self-regulatory regimes, which have already proven successful in structuring providers' conduct, rather than supporting new prescriptive requirements, which would threaten innovation and undermine consumer welfare. Moreover, any modifications to the existing privacy framework must be technology-neutral, focusing on how information is used and protected, rather than the specific means by which it is collected and used.

TIA represents the global information and communications technology ("ICT") industry through standards development, advocacy, trade shows, business opportunities, market intelligence and world-wide environmental regulatory analysis. Its 600 member companies manufacture or supply the products and services used in the provision of broadband and broadband-enabled applications. Since 1924, TIA has enhanced the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications. Members' products and services empower communications in every industry and market,

including healthcare, education, security, public safety, transportation, government, the military, the environment and entertainment.

Summary

Effective privacy protections are important for consumers and the ICT industry, particularly in an era of rapid technological change. Consumers will only adopt new information and communications technologies if they trust that their personal privacy preferences will be respected and that their personal information will remain secure. Innovations in information use and technology, coupled with effective privacy protections, have greatly enriched consumer choices and experiences and benefitted our economy.

There is an extensive body of state and federal law to safeguard consumer privacy, including Section 5 of the Federal Trade Commission Act. This provides a strong but flexible privacy framework based on consumer notice and choice, as well as reasonable security measures to protect consumers' personal information from unauthorized access or release. Certain types of information are subject to additional protections, such as those set out in the Communications Act of 1934, as Amended ("Communications Act") and the Health Insurance Portability and Accountability Act ("HIPAA"). By accounting for consumer demands, sensitivity of information, and other relevant factors, this existing framework has proven effective in addressing privacy challenges arising from innovations in information use and technology.

Industry has strong incentives to protect consumer information, particularly sensitive consumer information, and thus self-regulation has been an effective complement to governmental action, particularly for new and evolving technologies. Examples of self-regulation include the Mobile Marketing Association Code of Conduct, the Better Business Bureau Self-Regulatory Principles for Online Behavioral Advertising, and CTIA-The Wireless Association Best Practices and Guidelines for Location-Based Services. Industry members are well positioned to understand technological and business needs and to propose solutions that protect consumer privacy while allowing market and technical innovations to continue.

Appropriate collection, sharing, and use of consumer information provide many benefits to industry, the economy, and consumers. It is thus vitally important that privacy protections maintain flexibility for different business models and technologies to ensure that these benefits continue. Businesses may collect and use information to provide more convenient services or to improve products or customer service. Information about consumers may also be used for marketing purposes, which permits more targeted marketing and also underwrites the provision of free content and services on the Internet and other channels thereby making services more affordable for all consumers.

Of course, the collection, sharing, and use of consumer information also raise concerns about privacy. Consumers are concerned that their personal data may be collected without their knowledge, used in a way they do not expect or desire, or misused to invade their privacy. They may also be placed at risk of harms such as identity theft if their personal information is not secured adequately. Privacy protections should provide users clear notice about what information will be collected, how it will be used, and by whom, as well as reasonable security for their personal information. These protections should not, however, replace consumers' *own*

choices, which may favor innovations that provide convenience, speed, or easier communication. Such protections also should not dictate which technologies may be used, as long as consumers receive appropriate notice and can exercise choice about how these technologies collect, use, and share their information.

Finally, privacy protections should not impose onerous requirements on business or consumers, which may retard the development or uptake of new technologies and services to the detriment of consumers and our economy. For example, although the European Privacy Directive 95/46/EC has benefits in terms of applying a unified approach that reduces confusion about which standards apply, it is also highly bureaucratic and its burdens may outweigh the privacy benefits for individuals. By contrast, the Asia-Pacific Economic Cooperation ("APEC") Privacy Framework and the Cross Border Privacy Rules reflect an approach to privacy regulation that protects privacy while preserving the flexibility necessary for innovation. TIA members applaud the Department of Commerce's leading role in the APEC process and the development of these Rules.

Discussion

I. TIA Members Support Privacy Protections for Consumers.

Industry, including the ICT industry, needs information about customers' needs and interests to create and offer products and services that best meet those needs and interests – services and products which, in turn, produce substantial benefits for consumers. As the ability to collect, use, and store information about consumers has increased, however, so have consumers' concerns about privacy. It is in the interest of the ICT industry to ensure that consumers have sufficient confidence about their privacy so that they are willing to embrace new technologies and services and, based on their preferences, to share their information in exchange for benefits such as greater convenience, increased safety, or enhanced communications.

a. Consumer Privacy is Important to the Adoption of Technological Advances.

The use of consumer information to design products and improve services, as well as to fund free services and content, has produced substantial benefits for consumers.[1] Consumers justifiably

[1] *See, e.g.*, Jon Leibowitz, Chairman, Fed. Trade Comm'n, Keynote Address at the National Cable & Telecommunications Association Cable Show 2010 (May 12, 2010) (stating that targeted advertising is "usually good for consumers, who don't have to waste their time slogging through pitches for products they would never buy; good for advertisers, who efficiently reach their customers; and good for the Internet, where online advertising helps support the free content everyone enjoys and expects"); *see also* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 112 (2008) ("It is not obvious, however, that better information about consumer behavior increases the amount of marketing. It clearly leads to more targeted
(continued on next page)

have concerns, however, about how their data is collected, stored, and used.[2] If consumers do not trust that new technologies and business models will respect their privacy preferences or keep their sensitive information secure, however, they will be hesitant to use such technologies, thus foregoing benefits for themselves and ultimately slowing innovation.[3] It is thus in the interest of the ICT industry to ensure that consumers have sufficient confidence about their privacy so that they are willing to embrace new technologies and services and, based on their preferences, to share their information to receive benefits such as greater convenience, increased safety, or enhanced communications.[4]

b. TIA Members Support the Current Privacy Framework Based on Notice, Choice, and Data Security, which, Coupled with Robust Enforcement, will continue to be Effective in Protecting Consumer Privacy.

There is no single source of privacy law in the U.S. The Federal Communications Commission ("FCC") administers Consumer Proprietary Network Information ("CPNI") regulations[5] that protect certain subscriber information held by communications providers and Congress has also enacted sector-specific laws governing sensitive personal data, such as HIPAA's protections for health records.[6] The FTC, however, provides general oversight for much of the collection, use, and sharing of consumer information for most businesses through application of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices.[7] The FTC's longstanding approach rests primarily on efforts to ensure (1) that consumers are afforded notice of what

---

marketing -- there is a higher probability that the consumer will find the message relevant if information about past behavior helps to predict preferences.").

[2] *See* Fed. Trade Comm'n Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology*, at 1 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (discussing consumer concerns over personal data collection).

[3] *See, e.g.*, Ctr. for Democracy & Tech., *Health Information Privacy: Current Trends, Future Opportunities*, at 1 (Mar. 2010), *available at* http://www.cdt.org/files/pdfs/FTCRoundtableTestimony.pdf (citing survey data suggesting that consumers who do not trust privacy and security protections for electronic health records will not use them and noting that this may affect individual patient care and overall public health).

[4] *See, e.g., Data Accountability Act and Informed P2P User Act: Hearing on H.R. 2221 and H.R. 3224, Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (May 5, 2009) (statement of Federal Trade Commission) ("If companies do not protect the sensitive consumer information that they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace.").

[5] *See* 47 U.S.C. § 222 (establishing duty of every telecommunications carrier to protect confidentiality of customers' CPNI).

[6] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264(c)(2), 110 Stat. 2033–34 (1996); Social Security Act, 42 U.S.C. § 1320d-2 (2009).

[7] Federal Trade Commission Act, 15 U.S.C. § 45.

information is collected about them and how it will be used (notice), (2) that they can choose whether to allow collection and use of their personal information (choice), and (3) that the entity that collects personal consumer information uses reasonable measures to secure it against accidental or unauthorized access or release (security).

TIA members support this framework of notice, choice, and security. Consumers should be able to access clear descriptions of the types of personal data collected and the purpose for which that data is being used and to exercise choice about whether to permit their personal information to be collected and used as described. In addition, any company that collects and maintains such information must take reasonable security measures to guard against unauthorized access to it. Finally, robust enforcement of privacy protections is very much in the interest of the ICT industry to guard against consumers losing confidence in the market and failing to embrace new communications technology. In fact, the self-regulatory programs that TIA members support that are described in the following subsection all use a framework based on notice, choice, and security backed up by enforcement to ensure accountability.

c. Where Additional Protections are Necessary, Self-Regulatory Regimes are an Effective and Flexible Complement to Government Regulation.

Industry members are necessarily sensitive to consumers' demands. They are also well positioned to understand providers' technological and business needs and to propose privacy-protective solutions that offer an effective sector-wide response while allowing market and technical innovations to continue.[8] Given the providers' interest in marrying strong privacy protections with consumer choice and innovation, self-regulatory regimes are a powerful tool for use in developing appropriate privacy norms. Self-regulation also offers greater flexibility in responding promptly to new concerns to better meet emerging threats.

Accordingly, the ICT industry has participated in a variety of self-regulatory efforts to address privacy concerns and enhance consumer confidence in new technologies and business models. For example, many TIA members follow the Mobile Marketing Association Code of Conduct, which requires companies to provide consumers notice about how their information will be used; choice (based on obtaining customer consent, offering customization by consumers, and requiring constraint by marketers); and security for consumer information.[9] TIA Members have also participated in the development of the cross-industry Self-Regulatory Principles for Online Behavioral Advertising issued by the Better Business Bureau and leading advertising industry associations.[10] The Principles aim to provide consumers greater transparency, choice, and

---

[8] *See, e.g.*, Leibowitz, *supra* note 1 ("We know that those of you in the industry are much better positioned to understand the threats to consumer privacy – and to put in place the technical safeguards that I believe we all want.").

[9] Mobile Mktg. Ass'n, *Global Code of Conduct* (July 2008), *available at* http://mmaglobal.com/codeofconduct.pdf.

[10] Better Business Bureau et al., *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available at* http://www.bbb.org/us/Storage/0/Shared%20Documents/online-ad-

(continued on next page)

control regarding the collection and use of their information for online behavioral advertising purposes. In addition, CTIA has also promulgated Best Practices and Guidelines for Location-Based Services, which are based on the fundamental principles of user notice and consent regarding their location information and which aim to facilitate consumer use of new and exciting location-based services.[11]

II. It is Vital That Consumer Privacy Protections Maintain Flexibility for Different Business Models and Technologies to Promote Innovation, Which Will Ultimately Benefit Consumers and Our Economy.

It is crucial for policymakers not to focus exclusively on the privacy risks associated with new technologies and services, thereby overlooking the tremendous increase in consumer welfare such technologies can offer, including some capabilities that actively promote consumers' privacy interests. Because many useful products and services rely on consumer information, it is vital to strike a careful balance so that privacy-based restrictions do not unduly burden industry's ability to offer these products, services, and capabilities.

a. Consumer Demand for Technological Innovation has Resulted in Greater Consumer Choice and Significant Benefits to Consumers and the Economy.

Consumers have embraced new technologies and business models that provide improved capabilities and greater value. For example, all of the applications and services that are the subject of self-regulation discussed above – mobile marketing, targeted advertising, and location-based wireless services– offer consumers enormous benefits. These include improved personal safety and security through easy access to maps and directions and the ability to locate children and friends throug location-based services; more efficient shopping and searches through advertising that is better targeted to the recipient's interests; and savings and convenience through offers such as mobile coupons provided through mobile marketing. There are also innovative business models that use consumer information to support an array of new goods and services, often provided to consumers free of charge. For example, search engines give users access to a universe of information at speeds and scales that were previously unimaginable. In addition to benefits to individual consumers, the collection of data in anonymized form can provide societal benefits, such as epidemic detection and other medical insights, or improvements in urban planning.

Innovation has also increased the amount of control consumers can exercise over their personal information. New technologies often offer a consumer the opportunity to choose the level of

---

principles.pdf. *See also* Leibowitz, supra note 1 (expressing support for self regulation in this area).

[11] CTIA-The Wireless Ass'n, *Best Practices and Guidelines for Location-Based Services* (Apr. 2008), *available at* http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf.

information gathering with which he or she is comfortable. For example, many search engines allow users to delete cookies or to opt out of behavioral targeting. Technological innovation can also actively improve consumer privacy through a variety of ways. Everyday examples range from being able to use a mobile phone rather than a home or office phone to have a private conversation, to the opportunity to use a search engine to gather information about a medical or psychological condition without having to ask an individual. A more advanced example is the ability of health information technology to limit access to electronic medical records to authorized users and to create a tracking system indicating when records have been accessed and by whom.[12]

b. Unduly Burdensome Restrictions Related to Consumer Privacy May Impede Technological Innovation and Reduce Consumer Choice.

Privacy regulations that greatly hinder the availability of information would be costly to consumers, who would receive fewer of the resulting benefits, such as improved services and products and greater convenience. For example, free services and content may become less widely available or suffer a reduction in quality because a critical source of their funding — targeted advertising—may become less valuable.[13] Also, onerous restrictions on behavioral advertising would likely *increase* the volume of unwanted marketing messages, imposing exactly the harm avoided by the highly popular "Do Not Call" rule.[14] Finally, if members of the ICT industry are required to implement burdensome technical safeguards as part of their product specifications, the costs will invariably be passed on to consumers, which will likely raise the price of new products and thereby deter adoption.

c. Privacy Regulation Should be Technology Neutral.

As noted above, the current privacy framework is based on providing the consumer notice about what information is collected and how it will be used, choice about whether to provide personal information, and security for the personal information that is collected. This framework is based on the consumer's expectations about how his or her personal information will be treated[15] and

---

[12] *See* D. Gilman and J. Cooper, *There Is a Time to Keep Silent and a Time to Speak, The Hard Part Is Knowing Which Is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. TECH. L. REV. 279 (forthcoming 2010) (discussing impact of information technology on health care industry).

[13] This effect is not simply speculative; the FTC is conducting an inquiry into the future of journalism, spurred by the decreasing ability of advertising to fund the news reporting function of newspapers. *See* FTC Workshop: New Media Workshop, http://www.ftc.gov/opp/workshops/news/index.shtml (last visited June 2, 2010) (describing FTC workshop entitled "How Will Journalism Survive the Internet Age.").

[14] Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 (1994).

[15] *See, e.g.*, Fed. Trade Comm'n Staff Report, *supra* note 2, at iii (noting that principles do not need to cover "first party" behavioral advertising because such activity by and at single website "is more likely to be consistent with consumer expectations.").

thus the focus of privacy protection should be on how information is used, collected, and safeguarded, not on which technology is used for those functions. For example, if a consumer chooses to provide personal information online pursuant to a privacy policy that promises that such information will not be shared with third parties for marketing purposes, it matters little to the consumer if the privacy promise is broken through a cookie that collects the information as he types it in, through a technology that intercepts the message while it is traveling over the network, or through the later release of that information from the recipient's database. Privacy protection should focus on how information is used and protected, rather than the means of information collection, whether it is through cookies, deep packet inspection, or paper records.

It is notable that the FTC's recent series of cases addressing failures to maintain personal information securely did not differentiate based on the technology used to safeguard the information. The FTC brought actions against companies that failed to secure their networks, as well as against a drug store chain that disposed of pill bottles with sensitive medical information by throwing them into the trash.[16] The focus was properly on the violation of the privacy protections promised to consumers, not on which technology was used to collect or store the consumer information.

III. The United States Leads the World in Technological Innovation, Due In Part to Flexible and Balanced Privacy Laws. When Looking to Privacy Laws and Regulations in Other Countries as Models, it is Important to Focus on Models that Preserve Flexibility while Protecting Privacy.

U.S. industry has been at the forefront of innovation in information and communications technology. As detailed above, the existing U.S. privacy framework based on notice, choice, and security has permitted the development of innovative consumer products that provide safety, convenience, and easy communications, as well as business models that offer consumers access to informative and diverse content and useful services at no cost.

a. Highly Restrictive Privacy Requirements may Hamper Innovation.

One straightforward way to reduce threats to privacy is to make the costs of information gathering, usage, and sharing prohibitive. Privacy protections must be balanced, however, to ensure that consumers and society continue to receive many of the benefits provided by information and communications technologies and that providers retain the ability to develop innovative methods of funding free content and services.

The European Privacy Directive 95/46/EC is a central example of privacy protection that contains some useful elements but also some elements that are unnecessarily burdensome. The Privacy Directive generally prevents the collection and processing of personal information unless

[16] *See Genica Corp*., FTC File No. 082 3113, Decision and Order (Mar. 2009); *DSW Inc*., FTC File No. 052 3096, Decision and Order (Mar. 7, 2006); *CVS Caremark Corp.*, FTC File No. 072 3119, Decision and Order (June 18, 2009).

the subject has provided unambiguous consent, and it also imposes significant use and retention standards on entities that collect or process personal data. Like the U.S. privacy framework, it contains the elements of notice, choice, and security, and one of its main benefits is that it applies a unified approach that reduces confusion about which standards apply to what activities. The Privacy Directive also imposes substantial costs on businesses, however, such as compliance and opportunity costs, that are ultimately borne by consumers.[17] Notably, a recent study commissioned by the European Information Commissioner's Office found that the Directive has become outdated in terms of technology, reflects an insufficient focus on harms and risks, is seen as bureaucratic, burdensome and too prescriptive, focuses on process rather than outcomes, and has become a rigid control mechanism over otherwise unobjectionable data processing.[18]

Unfortunately, examples of well-intentioned but overly burdensome regimes are not limited to Europe. A second cautionary example of the risks of onerous privacy protections is in the area of health information technology, where studies suggest that burdensome consent requirements have retarded hospitals' adoption of health information technology, with associated negative effects on patient health outcomes.[19]

b. APEC's Privacy Framework and the Cross Border Privacy Rules Represent an Appropriate Model For Protecting Privacy While Preserving The Flexibility Necessary For Innovation.

The APEC Privacy Framework, which was endorsed by APEC ministers in 2005, is an example of a successful international model that protects privacy while preserving the flexibility

---

[17] *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 20 (2000) ("There are, in short, identifiable costs to recognizing stringent data privacy rights, both in terms of efficiency and equity. For businesses, these costs include compliance, transaction, operating, and opportunity costs. Businesses ultimately factor these costs into the prices charged consumers. The prices of goods and services on the EU market are, in principle, higher on average than they would be without the EU data privacy requirements.").

[18] Neil Robinson et al., Info. Commissioner's Office, *Review of EU Data Protection Directive: Summary* (May 2009), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf. *See also* European Privacy Officers Forum, *Submission on the Review of the Data Protection Directive* (2009), *available at* http://www.huntonfiles.com/files/webupload/EPOF_Submission_on_DP_Directive_Dec_09.pdf (stating that European privacy notification requirements have become excessively bureaucratic and require considerable resources to manage, which is disproportionate to benefit brought to individuals.).

[19] *See* Gilman & Cooper, *supra* note 12, at 328-29 (discussing study documenting relationship between increased infant mortality and privacy requirements that suppress adoption of electronic health records by healthcare providers).

necessary for innovation.[20] The Framework takes into account the enormous benefits new technologies and business models offer consumers, government, and the economy, and seeks to enable data transfers, while "recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region." The Framework includes the principles of notice where reasonable, collection by lawful and fair means, use of the information only for the purposes collected unless consent for other uses is given, choice where appropriate, data accuracy and consumer access, reasonable security, and accountability. The Framework also supports imposing remedies that are commensurate with the extent of the actual or potential harm to individuals resulting from privacy violations.

The APEC Privacy Framework also supports the cooperative development by APEC members of Cross Border Privacy Rules that adhere to the Framework's principles. The Framework encourages the members to work with stakeholders in this process to create effective privacy protections without creating unnecessary barriers to cross-border information exchanges, including unnecessary administrative and bureaucratic burdens for business and consumers.

TIA members recognize that the Department of Commerce, along with other U.S. agencies, has been instrumental in working with counterparts across the APEC economies to develop a system in the APEC region that ensures the protection of consumers through accountable cross-border flows of personal information while facilitating business access to the benefits of electronic commerce. TIA members particularly commend the Department of Commerce for including opportunities for the business community to engage and provide input throughout the APEC Cross Border Privacy Rules development process. This collaborative effort has been essential given the pace of innovation in electronic commerce.[21] When the U.S. hosts APEC next year, TIA members stand ready to help showcase the success of the APEC Privacy Framework and the potential of the Cross Border Privacy Rules to address data privacy issues across APEC member economies.

---

[20] Asia-Pacific Economic Cooperation, *Privacy Framework* (2005), *available at* http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1.

[21] In particular, TIA members support the U.S. Government's efforts within the APEC E-Commerce Steering Group in organizing capacity building workshops on data protection legal regimes for important emerging APEC economies, including the Philippines, Vietnam, and Indonesia. Such workshops provide an important avenue for government and industry best practices and information sharing.

Conclusion

TIA welcomes NTIA's inquiry on the interaction between consumer privacy and technological innovation and, for the foregoing reasons, urges NTIA to support privacy protections that maintain flexibility for different business models and technologies, including technology neutrality, and thereby promote innovation.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: /s/ Danielle Coffey_____
Danielle Coffey
Vice President, Government Affairs
TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240