

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of

Privacy and Security of Information Stored on)
Mobile Communications Devices) CC Docket No. 96-115
)
)

To: The Commission

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Danielle Coffey
Vice President, Government Affairs

Mark Uncapher
Director, Regulatory and Government Affairs

Brian Scarpelli
Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

Its Attorneys

July 13, 2012

TABLE OF CONTENTS

Executive Summary iii

I. Introduction 1

II. Existing Privacy Requirements Focus on the Areas of Greatest Customer Concern..... 3

 A. Consumer privacy protections focus on the misuse of personal information 3

 B. Consumers Benefit from Personalization-Enhancing Innovations 5

III. Voluntary Codes of Conduct Benefit Consumer with Flexibility – and Enforceability 8

IV. Carriers and Service Providers need flexibility for Network Management, Including
 Customer-Specific Data 14

V. Conclusion..... 17

Executive Summary

TIA member companies recognize the importance of consumer privacy concerns and have a strong interest in ensuring that consumers have sufficient confidence about their privacy so that they are willing to embrace new technologies and services.

The use of consumer information to design products and improve services, as well as fund free services and content, has produced substantial benefits for consumers. Americans are accustomed to making pragmatic choices about their privacy in our information economy. Mobile applications and the collection of data allow consumers to have a much more personalized experience and to engage in “automated dialogue” about their needs and interests. Additionally, many online services and mobile applications are offered online free of charge, but collect information from the user, such as age, sex and general location.

The focus of privacy protection should continue to be on how information is used, collected, and safeguarded, not on which technology is used for those functions. Technological convergence has made legal and regulatory distinctions between ‘networked’ and ‘brick and mortar’ consumer relationships irrelevant. Regulations based on invalid distinctions can fail in their purpose and do real economic harm by discouraging the adoption of network technologies. Consumers need to be given more credit for understanding their choices in opting for convenience. Regulations that greatly hinder the availability of information and implement burdensome technical safeguards would be costly to consumers in the form of less availability of free services and content and more expensive products.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of

Privacy and Security of Information Stored on)
Mobile Communications Devices) CC Docket No. 96-115
)
)

To: The Commission

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. INTRODUCTION

The Telecommunications Industry Association (“TIA”) welcomes the opportunity to provide the Federal Communications Commission (“Commission” or “FCC”) with comments regarding the privacy and data security practices of mobile wireless service providers with respect to customer information stored on their users’ mobile communications devices, and the application of existing privacy and security requirements to that information.¹ As the Commission observes in its notice, service providers’ collection and use of this information may be a legitimate and effective way to improve the quality of wireless services. At the same time,

¹ Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices, CC Docket No. 96-115. DA 12-818 (rel. May 25, 2012) (“PN”).

the collection, transmission, and storage of this customer-specific network information raises new privacy and security concerns.²

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 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.

TIA, on behalf of its members, appreciates the importance of the interplay between information privacy and innovation in the information economy. A significant benefit to consumers of the digital economy is the opportunity to use information about customers’ needs and interests to create and offer personalized products and services. TIA believes that an appropriate privacy framework should balance consumer privacy concerns with the consumer benefits arising from technological innovation and business model flexibility in communications and Internet commerce. Policy solutions should not restrict an individual consumer’s ability to choose their preferred balance between privacy and these innovations that provide convenience, speed or enhanced communication.

² *See Id.* at 1.

II. EXISTING PRIVACY REQUIREMENTS FOCUS ON THE AREAS OF GREATEST CUSTOMER CONCERN

A. CONSUMER PRIVACY PROTECTIONS FOCUS ON THE MISUSE OF PERSONAL INFORMATION

The American system of privacy protections is not the product of a single source of law. Our protections instead focus on regulating the use of sensitive information.³ Instead of a comprehensive system attempting to dictate how consumer records are maintained, our national approach addresses the areas of greatest concern. This includes laws affecting the use of financial, health, and children’s information. Beyond the restraint that consumers exercise in the use of personally identifiable information, there are numerous state and Federal laws that govern these specific uses.

In addition to the privacy rules and regulations discussed in greater detail below, as the Notice observes, certain types of information are subject to additional protections, such as those set out in the Communications Act of 1934, as Amended (“Communications Act”).⁴ Carriers subject to Section 222 of the Communications Act have a duty to “protect the confidentiality of

³ See, e.g., Health Information Technology (“HITECH”) Provisions of American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D, Pub. L. 111-5, 123 Stat. 115, codified in relevant part at 42 U.S.C. §§ 17937 and 17954). The HITECH Act directs the FTC to issue a rule requiring entities that obtain consumers’ personal information but are not subject to the Health Insurance Portability & Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996). See also, Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq* (“FCRA”). The FCRA regulates the collection, dissemination, and use of consumer information, including consumer credit information. See also the Federal Trade Commission (“FTC”), under the Federal Trade Commission Act, 15 U.S.C. § 45 (FTC Act”), 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. The FTC’s longstanding approach rests primarily on efforts to ensure (1) that consumers are afforded notice of what marketing. See Fed. Trade Commission 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 and noting that “there is a higher probability that the consumer will find the message relevant if information about past behavior helps to predict preferences.”).

⁴ See, PN, p. 4

proprietary information of, and relating to ... customers.”⁵ TIA believes that the Commission’s consideration of the breadth of Section 222 requirements should be predicated on the existing legal framework for privacy, which focuses on specific users concerns about the potential misuse of personal information. Care should be taken in order to avoid developing overly prescriptive rules for the maintenance and use of customer data.

These “information use” -based protections contain an extensive body of state and federal law to safeguard consumer privacy. However, this approach allows for a 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. “Information use” laws, such as Fair Credit Reporting legislation,⁶ give consumers access to information which may result in adverse decisions. These processes also give consumers the opportunity to amend their records with clarifying information.⁷ 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. In addition to these “information use” protections, a number of privacy self-regulation standards have emerged that are widely accepted throughout industry. The FTC has encouraged these efforts and has the Section 5 power to enforce them.

It is notable that the FTC’s recent series of cases addressing failures to maintain personal information securely does not differentiate based on the technology used to safeguard the information. The FTC brought actions against online companies that failed to secure their

⁵ 47 U.S.C. § 222(a).

⁶ *See* FCRA.

⁷ *See* FCRA at § 1681i..

networks, as well as against a hotel chain that experienced a data security breach which led to the exposure of customers' credit card information.⁸ The focus was properly on the violation and misrepresentation of the privacy protections promised to consumers, not on which technology was used to collect or store the consumer information.

The Consumer Proprietary Network Information regulations ("CPNI")⁹ administered by the FCC narrowly focuses on the information practices of telecommunications carriers. Because their scope does not reach the activities of non-carriers, carriers can potentially be held to different standards for identical information practices than others.

B. CONSUMERS BENEFIT FROM PERSONALIZATION-ENHANCING INNOVATIONS

Americans are accustomed to making pragmatic choices about their privacy in our information economy. As consumers, we can choose to pay in cash to preserve our anonymity, but we regularly volunteer to give away information about ourselves. We know that credit card purchases produce a "paper trail" of information about our lifestyle and other characteristics. We also know that by ordering products through a mail order catalog, we will get future offers for related products. Consumers need to be given more credit for understanding their choices when they opt for convenience.

⁸ See, e.g., Press Release, Federal Trade Commission, *FTC Files Complaint Against Wyndham Hotels for Failure to Protect Consumers' Personal Information* (Jun. 26, 2012), available at <http://ftc.gov/opa/2012/06/wyndham.shtm> (last visited July 13, 2012).

⁹ See 47 U.S.C. § 222 (establishing duty of every telecommunications carrier to protect confidentiality of customers' CPNI).

Networked technologies are seeking to duplicate the same personalized attention that consumers get from the best brick and mortar merchants. A traditional merchant often knows, based upon past experience or even conjecture, what a consumer wants and is able to make recommendations. Consumers value the personal attention that this requires.

In many respects, the interactive nature of networked communications is far more similar to a conversation with a brick & mortar merchant than it is with more conventional mass media electronic medium. Not only can the consumer reject the merchant's recommendations, but they can also guide the dialogue in a direction that results in a more mutually satisfactory conclusion. Online processes that replicate familiarity with consumer preferences are a positive characteristic of online commerce.

The personalization of consumer communications to customize contact and engage in an “automated dialogue” is a benefit of the Internet. Sophisticated retention of past buying patterns and other data can help a marketer personalize their contact with a customer. The openness and communications power of the Internet provides strong incentives for e-commerce companies to keep their customers satisfied. For example, search engines and other related tools compete with each other in their ability to identify and access desired content. Regulators have noted the consumer benefit of marketing personalization.¹⁰

¹⁰ See, e.g., Jon Leibowitz, Chairman, Fed. Trade Commission, 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 have concerns, however, about how their data is collected, stored, and used.”).

While some advocates dwell on one particular type of technology or service as posing a drastic threat to consumers' privacy, these fears are often hypothetical only and do not take into account new consumer benefits. Individual consumers are best suited to determine if future offers have been tailored to fit their specific interest. 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.

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. 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. Also, onerous restrictions on behavioral advertising would likely increase the volume of unwanted marketing messages. 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.

III. VOLUNTARY CODES OF CONDUCT BENEFIT CONSUMER WITH FLEXIBILITY – AND ENFORCEABILITY

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.

Industry understands that if consumers do not trust that new technologies and business models will respect their privacy preferences or keep their sensitive information secure, users will be hesitant to use such technologies. Consumer mistrust of new products and services slows consumer adoption. Consequently, the ICT industry wants 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.

Industry members are 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. Given the providers' interest in marrying strong privacy protections with consumer choice and innovation; self-regulatory regimes are a powerful tool to use in developing appropriate privacy norms. Existing voluntary self-regulation privacy initiatives have already substantially contributed to fostering consumer confidence. Future efforts offer greater flexibility in responding promptly to new concerns to better meet emerging threats.

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 below – 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 through 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.

Competitive pressures encourage the adoption of “privacy best practices” in order to assure consumer confidence. Companies that fail to meet consumer expectations can expect the word to spread quickly, much more quickly than in traditional vendor/customer environments. TIA members are strongly committed to providing their customers with an environment that discourages fraud and promotes pro-customer behavior.

Consumer surveys demonstrate that consumers are already carefully weighing choices regarding their privacy. Regulators should not place unnecessary barriers to offering consumers convenience, nor should they underestimate the capacity of consumers to make informed choices. Innovation has also increased the amount of control consumers can exercise over their personal information.

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. Since the early period of the internet's popularity, industry members have been very aggressive in recognizing emerging concerns about privacy and taking steps to institute self-regulated models:

1. At the outset of the internet, consumers were cautious about using it, particularly for commercial activities. The Online Privacy Alliance was formed in 1998 by a coalition of global companies and trade associations with the intent of fostering consumer trust and protection of their online privacy. The Alliance promoted guidelines that led to the adoption of effective Internet privacy policies by the private sector.¹¹ It also developed a framework for enforcing consumer privacy that called for objective third party monitoring of website compliance with privacy policies and provision of a mechanism for consumer complaint and resolution.
2. Shortly after that, in 2000, the Network Advertising Initiative was formed to address concerns about online advertisers' use of cookies to track consumers' web browsing in order to facilitate behavioral advertising.¹² The founding companies of NAI worked with the Federal Trade Commission to develop a self-regulatory framework to provide notice and mechanisms to alter the scope of the data tracking, including opt out systems.¹³ NAI continues to operate today and has updated its code of conduct and tracks compliance among its member organizations.

¹¹ See Online Privacy Alliance, available at <http://www.privacyalliance.org/> (last visited July 13, 2012).

¹² See Network Advertising Alliance, History, available at <http://www.networkadvertising.org/about/history.asp> (last visited July 13, 2012).

¹³ See *Id.*

Within the relatively short period in which mobile application have been a feature of the consumer wireless market, several industry led initiative have addressed specific consumer concerns:

1. Mobile Marketing Association Code of Conduct. 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.¹⁴
2. Self-Regulatory Principles for Online Behavioral Advertising. 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.¹⁵ The Principles aim to provide consumers greater transparency, choice, and control regarding the collection and use of their information for online behavioral advertising purposes. The Digital Advertising Alliance (DAA), a consortium of advertising trade groups, announced plans to expand consumer choice on privacy. The DAA plans to include a “do not track” button on web browsers that the organization’s members would honor. DAA members already support a privacy icon to give consumers the opportunity to opt out of ads.¹⁶

¹⁴ See Mobile Marketing Association, Code of Conduct (July 2008), available at <http://www.mmaglobal.com/policies/code-of-conduct> (last visited July 13, 2012).

¹⁵ See Internet Advertising Board, Self-Regulatory Principles for Online Behavioral Advertising (July 2009), available at http://www.iab.net/public_policy/behavioral-advertisingprinciples (last visited July 13, 2012)

¹⁶ See The Self-Regulatory Program for Online Behavioral Advertising, Opt Out from Online Behavioral Advertising, available at <http://www.aboutads.info/choices/> (last visited July 13, 2012).

3. Best Practices and Guidelines for Location- Based Services. 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.¹⁷ CTIA Best Practices and Guidelines (“Guidelines”) are intended to promote and protect user privacy as new and exciting Location-Based Services (“LBS”) are developed and deployed. Location Based Services have one thing in common regardless of the underlying technology – they rely on, use, or incorporate the location of a device to provide or enhance a service. Accordingly, the Guidelines are technology-neutral and apply regardless of the technology or mobile device used or the business model employed to provide LBS (e.g., a downloaded application, a web-based service, etc.). The Guidelines rely on two fundamental principles: user notice and consent.¹⁸

4. Mobile Application Rating System. CTIA and the Entertainment Software Rating Board (“ESRB”) announced in November 2011 that they have developed a rating system that mobile application storefronts voluntarily support as part of their application submission (or onboarding) process. The CTIA Mobile Application Rating System with ESRB uses the familiar age rating icons that ESRB assigns to computer and video games to provide parents and consumers reliable information about the age-appropriateness of applications.¹⁹

¹⁷ See CTIA Business Resources, Best Practices and Guidelines for Location-Based Services, http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 (last visited July 13, 2012).

¹⁸ See *Id.*

¹⁹ See CTIA, *CTIA-The Wireless Association and ESRB Announce Mobile Application Rating System* (Nov. 29, 2011), available at <http://www.ctia.org/media/press/body.cfm/prid/2147> (last visited July 13, 2012).

5. Mobile Privacy Principles. Leading mobile operators and vendors” have also worked on privacy matters through the GSM Association’s (GSMA) Mobile Privacy Initiative, which published principles regarding notice, transparency, and control for consumers over information that is collected or accessed by mobile applications. In February, the GSMA released privacy guidelines to provide for more functional and coordinated implementation of the principles across mobile platforms.²⁰

6. Also, the leading mobile platform providers agreed to abide by stricter privacy policies at the behest of the California Attorney General.²¹ As part of the agreement, the companies will give customers the option to read the privacy policy before downloading a new or updated mobile application. These companies also agreed to provide a means for customers to report applications that don’t comply with terms of service.

These efforts indicate industry’s continued commitment to ensuring consumer privacy and enhancing their trust in the ICT marketplace without the need for strong government regulation. A key factor to the continued success of these self-regulatory initiatives was the ability to target it to the relevant industry players that have a stake in effective outcomes.

²⁰ See Jennifer Baker, *Mobile Network Operators Set Guidelines for App Privacy*, PC WORLD (Feb 27, 2012 11:40 am), available at http://www.pcworld.com/businesscenter/article/250773/mobile_network_operators_set_guidelines_for_app_privacy.html (last visited July 13, 2012).

²¹ See State of Cal., Office of Attorney Gen., *Mobile Applications and the Mobile Privacy Fact Sheet*, available at <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy> (last visited July 13, 2012).

IV. CARRIERS AND SERVICE PROVIDERS NEED FLEXIBILITY FOR NETWORK MANAGEMENT, INCLUDING CUSTOMER-SPECIFIC DATA

Communications networks providing high-bandwidth applications such as VoIP, streaming video, video conferencing, and gaming, require intensive management tools.²² Increasing traffic demands and services with distinct characteristics require that service providers have the flexibility to use a robust and diverse set of traffic-management tools. Without appropriate management and diagnostic tools network operators would be hindered in meeting the typical users' expectations.²³ These methods include having visibility to the experience of individual users.

Increased network demand is not the only legitimate justification for usage and diagnostic tools. These usage and diagnostic tools will have to become increasingly sophisticated to keep pace with the growing complexity of the services be provided. For example, subscribers expect network operators to block an assortment of harmful or otherwise undesirable content, including spam, spyware, and denial of service. Users expect their specialized and managed services to work in an uninterrupted and timely fashion. There is simply little to no tolerance for latency, jitter, packet loss or lack of availability for these business or mission critical services. A misguided decision to impose data collection restrictions for network management could severely undermine the Quality of Service.

²² See Declaration of Kenneth Ko and Kevin Schneider at 19-20 (submitted with Comments TIA, GN Docket No. 09-191, WC Docket No. 07-52, at 17-22 (filed Jan. 14, 2010) (“TIA Open Internet Comments”) (“Ko/Schneider Declaration”); see also Declaration of Matt Tooley and Don Bowman (submitted with TIA Open Internet Comments) at 16-18 (“Tooley/Bowman Declaration”).

²³ See Tooley/Bowman Declaration at 4, 16; Ko/Schneider Declaration at 21. See also Preserving the Open Internet, Broadband Industry Practices, Notice of Proposed Rulemaking, 24 FCC Rcd 13064 at ¶ 136 (“it may be reasonable for a provider to take measures to counter traffic that is harmful or unwanted by users”) (“Open Internet NPRM”).

Previously, the Commission has appropriately recognized the need for reasonable network management, including practices to:

- (1) reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns;
- (2) address traffic that is unwanted by users or harmful;
- (3) prevent the transfer of unlawful content; or
- (4) prevent the unlawful transfer of content.”²⁴

The proposed definition also stated that reasonable network management consists of “other reasonable network management practices.”²⁵

Additionally, advanced network management tools can enhance public safety, public safety communications, such as with E911, and the prioritizing of emergency calls. Similarly these tools could improve communications access for communities with specialized needs. The Commission has further acknowledged that “existing mobile networks present operational constraints that fixed broadband networks do not typically encounter,” which puts greater pressure on the concept of “reasonable network management” for mobile providers, and creates additional challenges in applying a broader set of rules to mobile at this time.²⁶

More specifically, network data collection restrictions for customer specific information present a potential tension with the fact that many managed services are deliberately offered outside of the best-effort Internet due to the value or sensitivity of the content. Customer specific

²⁴ See Open Internet NPRM at ¶¶ 133–41.

²⁵ See *Id.*

²⁶ See Preserving the Open Internet Broadband Indus. Practices, *Report & Order*, 25 FCC Rcd. 17,905 ¶ 95 (Dec. 23, 2010).

information, including usage history, may assist network managers to better meet user quality of service expectations.

V. CONCLUSION

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.

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 the foregoing reasons, TIA urges the FCC to take into consideration its views in this proceeding.

Respectfully submitted,

**TELECOMMUNICATIONS INDUSTRY
ASSOCIATION**

By: */s/ Danielle Coffey*

Danielle Coffey
Vice President & General Counsel, Government
Affairs

Mark Uncapher
Director, Regulatory and Government Affairs

Brian Scarpelli
Manager, Government Affairs

**TELECOMMUNICATIONS INDUSTRY
ASSOCIATION**

10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

July 13, 2012