Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
	)	CC Docket No. 96-115
Implementation of the Telecommunications	)	
Act of 1996	)	
	)	
Telecommunications Carriers Use of Customer	)	
Proprietary Network Information and	)	
Other Customer Information	)	

Comments of the Alliance for Telecommunications Industry Solutions

The Alliance for Telecommunications Industry Solutions (ATIS) submits these comments in response to the *Public Notice* released May 25, 2012, in the above-referenced docket. In the *Public Notice*, the Federal Communications Commission (Commission) seeks to refresh the record in this proceeding, noting it last collected information in response to a 2007 *Public Notice* focused on service providers' duties to erase customer information prior to the refurbishing of equipment. The current *Public Notice* seeks comment on a number of issues related to the privacy and data-security practices of mobile wireless service providers with respect to customer information stored on users' mobile devices, including whether these practices have created data-security vulnerabilities. ATIS notes that there has been, and continues to be, significant industry-led work in the area of privacy and security. ATIS believes that these industry efforts are the most effective method to address the complex issues that arise from the continued evolution of communications networks and equipment, and urges the Commission to not disrupt this work.

ATIS is a global standards development and technical planning organization that leads, develops, and promotes worldwide technical and operations standards for information, entertainment, and communications technologies. ATIS' diverse membership includes key stakeholders from the ICT industry –wireless and wireline service providers, equipment manufacturers, broadband providers, software developers, consumer electronics companies, public safety agencies, digital rights management companies, and internet service providers. Nearly 600 industry subject matter experts work collaboratively in ATIS' open industry committees and incubator solutions programs. Technical, operational, and business priorities are also examined by ATIS through its Technology and Operations (TOPS) Council, a group established by the ATIS Board of Directors to identify and address the ICT ecosystem's needs through focused, expedited efforts.

While ATIS works on a broad array of issues, security and privacy issues permeate virtually all of ATIS' work programs and significant work is underway in many ATIS committees and forums. The ATIS Cloud Services Forum (CSF), for example, is working on a number of issues that will enhance the ability of service providers to offer secure and reliable cloud-based services. The ATIS CSF, which promotes the integration of cloud technologies and network infrastructure by developing standards and creating reusable service enablers and technical solutions, is currently examining a Trusted Information Exchange (TIE). TIE would be an end-to-end solution for the secure exchange of cloud service information.

The ATIS Network Reliability Steering Committee (NRSC) also addresses privacy and security issues in its work to enhance network reliability. A key focus of the NRSC is the development of industry Best Practices, which are industry practices that are developed through rigorous deliberation and expert consensus and proven through actual implementation. Among the existing industry Best Practices are many that focus on cyber security and privacy, including

Best Practice 8-8-8769. This Best Practice, which focuses on the protection of personally identifiable information, notes that service providers should protect such information against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data. This Best Practice also notes that policies for personal information protection should be clearly identified and enforced.[1]

The ATIS Network Performance, Reliability and Quality of Service Committee (PRQC) has a strong focus on network reliability and security. The PRQC develops standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. One of the technical reports that has been developed by the PRQC is *Security for Next Generation Networks -- An End User Perspective* (ATIS-0100010). This report, which provides an overview and guidelines for security in next generation networks, addresses data confidentiality requirements:

> In order to achieve at least the same level of data confidentiality protection that is present in TDM systems, NGN must implement services which ensure data confidentiality. These mechanisms must ensure that the information in a Network system and transmitted information is accessible for reading or modification only by authorized parties. These confidentiality mechanisms must also provide an appropriate level of "back-traffic" (i.e., stored encrypted traffic) protection that will protect the information for the desired length of time.[2]

The ATIS Packet Technologies and Systems Committee (PTSC) also has active work programs underway that are focused on network security. As the ATIS committee that develops standards and technical reports related to services, architectures, and signaling, the PTSC focuses on a number of security issues, including end-to-end user authentication and signaling security

[1] The full text of this Best Practice may be viewed on the ATIS Industry Best Practices website at: http://www.atis.org/bestpractices.

[2] *Security for Next Generation Networks -- An End User Perspective* (ATIS-0100010), Section 6.5.2.

and identity management/security.

Finally, ATIS notes that significant work is being completed by the ATIS TOPS Council Cyber Security Focus Group (CS-FG). The CS-FG has developed a phased, end-to-end approach to analyzing the cyber security landscape, starting with the core network and moving to the edge. It has defined functional domains encompassing chips and handsets, regulatory issues, trust and identity management, reference architecture, and service assurance. This approach will ensure end-to-end compatibility with each domain to avoid divergent approaches and lack of end-to-end Quality of Experience. This work is currently underway and will be progressed in phases with the first phase addressing both machine-to-machine and international regulatory issues. As part of this work, the CS-FG will develop of a common set of cyber security/data privacy policies and protocols that, at a minimum, conform to North American regulatory requirements, with the goal of developing a unified model that addresses cybercrime at a sufficiently high level, while allowing country-specific flexibility.

As explained above, there is significant industry work underway to address security and privacy issues. ATIS believes that these industry efforts are the most effective method to address the complex and evolving issues, including those pertaining to data security and privacy. ATIS therefore urges the Commission not to disrupt this industry-led work.

Respectfully submitted,

Thomas Goode
General Counsel
Alliance for Telecommunications Industry
Solutions
1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 628-6380

July 13, 2012