

**Before the  
Federal Communications Commission  
Washington, D.C.**

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

---

**COMMENTS OF THE INTERNET COMMERCE COALITION**

---

Jim Halpert  
Sydney White  
500 8th Street, NW  
Washington, D.C. 20004  
(202) 799-4441

July 13, 2012

## **I. Introduction**

The Internet Commerce Coalition (ICC) welcomes the opportunity to comment on the Commission's questions regarding application of the CPNI framework to the privacy and security of mobile devices.

The ICC's members include leading Internet and e-commerce companies and trade associations: Amazon.com, AOL, AT&T, CareerBuilder, Comcast, eBay, Google, Monster.com, Verizon, TechAmerica and US Telecom. Our members are committed to transparency regarding their data practices, and to protecting the privacy and security of customer information.

The Commission asks legitimate questions regarding the privacy and security of information stored on user mobile devices. While raising these questions is appropriate, expanding CPNI regulation and the concept of CPNI itself to attempt to address this issue would regulate a sliver of the complex mobile eco-system in a way that would be asymmetrical, ineffective and inappropriate. Nor can the Commission's jurisdiction over CPNI collected by the carriers be extended, directly or indirectly, to third parties.

The NTIA multi-stakeholder process has been launched only this week and has begun by addressing transparency in the mobile environment -- on a mobile ecosphere-wide basis. Subsequent topics are likely to include uses of and the security of personal information in the mobile environment. The White House determined in its April 2012 Privacy Report<sup>1</sup> that the best way to advance privacy in the networked environment is through cross-industry multi-stakeholder initiatives and in across-the-board baseline privacy legislation. Indeed, that Report supported simplifying the thicket of medium-specific communications sector privacy, rather than making it more complex by adding to stove-piped regulations, such as the CPNI rules.

---

<sup>1</sup> "Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy."

The storage of information on an end user device that is simply accessible to a carrier is very different than CPNI stored by the carrier on its systems. To the extent data is stored on the end user device to measure and maintain service quality, generally it does not “relate[] to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier” and is not “made available to the carrier by the customer...” *See* 47 U.S.C. § 222(h)(1)(A). Rather, when used to maintain or enhance quality of service, it fits directly within the “context” of the carriers’ relationship with its customers.

Second, the types of information that might fall within the CPNI definition are far from uniquely available to carriers. In fact, they may be available to a broad range of application providers and other actors in the mobile eco-system who have no relationship with carriers. Thus, imposing privacy and security regulation by means of the CPNI statute, far from focusing on an issue unique to carriers, is addressing a broader issue, and doing so in an asymmetrical and under-inclusive way.

This would have several negative consequences. First, it would do little to protect the privacy or security of information stored on consumer devices. As a consequence, it would likely give consumers a false sense of security. A far more effective approach would be an approach to security that applies to the entire mobile eco-system. However, the CPNI statute, which applies on its face only to telecommunications carriers, is not a vehicle for the FCC to address the mobile eco-system, and the FCC would exceed its authority by attempting to regulate it.

Second, the Commission’s contemplated approach would be arbitrary and distort competition. In today’s mobile market, telecommunications services represent only a sliver of

activity in the mobile eco-system. It would create a confusing asymmetry of regulation between various types of communications and other mobile services that consumers are choosing between in the market.

Interpreting the statute in this way would create a huge asymmetry in regulation, with hardware manufacturers, software, and app providers and advertisers wholly exempt from regulation and telecomm carriers uniquely and heavily regulated. Already, the CPNI rules impose data security requirements, such as audit trail requirements, that are more extensive than those that apply to any other mobile communications or other service platforms, and are as or more stringent than those that apply to financial services companies. For all these reasons, the Commission should not expand this regime further by issuing CPNI rules relating to carrier storage of information on end user devices.

Respectfully submitted,

/s/

Jim Halpert  
Sydney White  
Counsel to the Internet Commerce Coalition  
DLA Piper LLP (US)  
500 8th Street, NW  
Washington, D.C. 20004  
(202) 799-4441