

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

In the Matter of )  
 )  
Implementation of the Telecommunications Act of ) CC Docket No. 96-115  
1996: Telecommunications Carriers' Use of )  
Customer Proprietary Network Information and )  
Other Customer Information )  
 )  
Privacy and Security Information Stored on Mobile )  
Communications Devices )  
 )

To: The Commission

**COMMENTS OF THE  
CONSUMER ELECTRONICS ASSOCIATION**

Julie M. Kearney  
Vice President, Regulatory Affairs

Laura Knapp Chadwick  
Manager, Government Affairs

Consumer Electronics Association  
1919 S. Eads Street  
Arlington, VA 22202  
(703) 907-7644

July 13, 2012

**TABLE OF CONTENTS**

EXECUTIVE SUMMARY ..... i

I. Introduction and Background ..... 1

II. The Commission’s Authority to Regulate Privacy Is Severely Constrained..... 4

III. The Limited Scope of Section 222 Prohibits Any Regulation of Mobile Apps,  
Operating Systems, or Manufacturers ..... 6

IV. The Commission Should Not Broaden or Alter the CPNI Rules ..... 9

    A. Existing Commission Rules, Consumer Protection Laws, and Industry Self-  
    Regulation Sufficiently Protect Consumers ..... 9

    B. Consumers Have Numerous Built-In Tools to Protect Information Stored on Their  
    Devices ..... 13

V. Conclusion ..... 15

## EXECUTIVE SUMMARY

Consumer electronics manufacturers, including manufacturers of mobile devices, deeply respect consumer privacy and employ numerous measures to protect such privacy. Irrespective of any regulatory requirement, manufacturers recognize that protection of consumer privacy is an important and necessary business practice. They consistently develop, implement, and enforce robust industry self-regulation and apply best business practices in a variety of areas related to consumer privacy. In addition, CEA and its members are actively working in industry groups and in government-facilitated self-regulatory processes, such as the NTIA multistakeholder process, to ensure that privacy protections are consistent with consumer expectations. With such industry-wide initiatives underway to ensure continued protection of consumer privacy in the mobile space, the Commission need not revive the instant proceeding, which has been dormant for five years.

As a preliminary matter, the Commission's jurisdiction to act in the privacy space is severely constrained. The *Notice* released by the Wireline Competition Bureau, Wireless Telecommunications Bureau, and Office of General Counsel implicitly acknowledges these constraints, focusing on Section 222 of the Communications Act as one of the sole grants of authority to the Commission to enact rules regarding privacy. Section 222 is itself limited, extending only to customer proprietary network information ("CPNI") from mobile phone users and the protection of such information by telecommunications carriers. As such, the Commission does not have authority regarding information collected or transmitted by mobile apps or operating systems that do not qualify as CPNI, nor does it have any authority to impose privacy mandates on manufacturers or operating system providers.

In addition, there is no need to broaden or alter the Commission's existing CPNI rules. Existing law and evolving self-regulatory schemes sufficiently protect the privacy of customer information stored on mobile devices. In contrast to self-regulatory models, government regulation frequently struggles to keep pace with technological innovation. Where the industry is working on its own and with government to develop and ensure consistent and appropriate practices, regulation would be unwarranted. At the very least, the Commission should allow the NTIA multistakeholder process to work and allow industry to develop appropriate and well-balanced self-regulatory models that would be enforceable by the FTC, the primary federal agency responsible for consumer privacy. If the Commission nevertheless chooses to take action on consumer privacy, rather than adopting any regulatory approach, it could be instrumental in supporting and participating in consumer education efforts.

While CEA underscores that the Commission need not and should not take regulatory action in this proceeding, in order to assist the Commission in evaluating the CPNI framework questions raised in the *Notice*, these comments provide information regarding manufacturers' role in decisions about the collection of CPNI. The design, development, and deployment of mobile devices involve a complicated ecosystem with numerous players providing input into – and ultimately making – design decisions. In this ecosystem, manufacturers have limited access to devices that are deployed in the market. Further, manufacturers collaborate with carrier-customers and operating system licensors to design and build the functionality of mobile devices, including software and applications.

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

In the Matter of )  
 )  
Implementation of the Telecommunications Act of ) CC Docket No. 96-115  
1996: Telecommunications Carriers' Use of )  
Customer Proprietary Network Information and )  
Other Customer Information )  
 )  
Privacy and Security Information Stored on Mobile )  
Communications Devices )  
 )

To: The Commission

**COMMENTS OF THE  
CONSUMER ELECTRONICS ASSOCIATION**

**I. INTRODUCTION AND BACKGROUND**

The Consumer Electronics Association (“CEA”)<sup>1</sup> hereby responds to the Public Notice issued by the Wireline Competition Bureau (“WCB”), Wireless Telecommunications Bureau (“WCB”), and Office of General Counsel (“OGC”) (together “Bureaus”) regarding the privacy and data-security practices of mobile wireless service providers with respect to customer information stored on their users’ mobile communications devices.<sup>2</sup>

---

<sup>1</sup> CEA is the principal U.S. trade association of the consumer electronics and information technologies industries. CEA’s more than 2,000 member companies lead the consumer electronics industry in the development, manufacturing and distribution of audio, video, mobile electronics, communications, information technology, multimedia and accessory products, as well as related services, that are sold through consumer channels. Ranging from giant multi-national corporations to specialty niche companies, CEA members cumulatively generate more than \$195 billion in annual factory sales and employ tens of thousands of people.

<sup>2</sup> *Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, Public Notice, CC Docket No. 96-115, DA 12-818 (May 25, 2012) (“*Notice*”). The *Notice* is intended to “refresh the record in this docket concerning the practices of mobile wireless service providers with respect to information stored on their customers’ mobile communications devices.” *Notice* at 4. The Commission last sought comment on these issues in

Consumer electronics manufacturers, including manufacturers of mobile devices, deeply respect consumer privacy and employ numerous measures to protect such privacy. Irrespective of any regulatory requirement, manufacturers recognize that protection of consumer privacy is an important and necessary business practice. They consistently develop, implement, and enforce robust industry self-regulation and apply best business practices in a variety of areas related to consumer privacy. CEA recently launched a privacy working group that enables its members to convene regularly to address privacy issues. One core function of the new working group has been the development and adoption of the CEA Privacy Principles, which represent CEA members' commitment to enhancing consumers' continued use of and trust in technology and technology products, as well as their consensus view on the appropriate scope and direction of any public policy proposals concerning privacy and electronic data collection.<sup>3</sup>

In addition, CEA and its members are actively working in industry groups and in government processes, such as the Department of Commerce's National Telecommunications & Information Administration ("NTIA") multistakeholder process, to ensure that privacy protections are consistent with consumer expectations. With numerous self-regulatory and government-facilitated initiatives underway to ensure continued protection of consumer privacy, the Federal Communications Commission ("FCC" or "Commission") need not revive the instant proceeding, which has been dormant for five years.

---

2007. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115, WC Docket No. 04-36, 22 FCC Rcd 6927 (2007).

<sup>3</sup> The CEA Privacy Principles include, among other things, the principle that innovations in technology and resulting consumer benefits made possible through electronic data collection should be protected and promoted, and that efforts should be made to increase consumer knowledge about existing privacy protections, as well as the benefits to consumers made possible through electronic data collection.

As a preliminary matter, given the Commission’s limited authority with respect to privacy matters, the Commission is not the appropriate government entity to consider broad questions of privacy on mobile devices. This limitation is seen in the scope of the *Notice*, which focuses only on Section 222 of the Communications Act. Under this provision, the Commission may only adopt and enforce regulations intended to ensure protection of customer proprietary network information (“CPNI” or “customer information”) on mobile devices, and may do so only with respect to telecommunications carriers in their provision of telecommunications services. However, information collected or transmitted by, or related to, mobile applications (“apps”), operating systems, or data services that is stored on mobile devices generally is not CPNI.<sup>4</sup> In addition, manufacturers have limited access to devices that are deployed in the market, and, to the extent data collection may occur, the focus typically is on diagnostic information and improving device performance.<sup>5</sup> Further, manufacturers collaborate with carrier-customers and operating system licensors to design and build the functionality of mobile devices, including software and applications. Carriers necessarily are intimately involved in the design process to ensure that devices operate efficiently on their networks. Device manufacturers may not have complete control over all functionalities in the application layer of mobile device operating systems, which typically are developed according to specifications

---

<sup>4</sup> In addition, CEA notes that consumers have ownership of their personal data, and therefore maintain the right to share such personal information with application developers in exchange for services. *See, e.g.*, Comments of the Consumer Electronics Association, State of New York Public Service Commission, CASE 10-E-0285, at 6 (filed Sept. 17, 2010) (“[t]he critical first step in making smart grid technologies a successful consumer experience is by making clear that consumers own their energy consumption data”).

<sup>5</sup> Alternatively, manufacturers may provide software on the device, such as the operating system itself or applications, which may collect data. Manufacturers in this context are no different from other application developers and, where concerns may arise, may be subject to enforcement by the Federal Trade Commission (“FTC”).

supplied by the operating system licensors. Once a device is deployed in the marketplace, any information collected, used, or transmitted by the operating system is generally not within the review or control of the manufacturer. Further complicating the ecosystem, applications – whether embedded by the operating system provider, required by a carrier-customer, or downloaded by the user – may use, collect, and transmit personal information. Manufacturers usually cannot control the information that may be transmitted by such applications. Thus, the Commission’s CPNI authority does not allow the Commission to take any industry-wide action on mobile device privacy and any FCC action would not have the desired effect in any event. More specifically, the Commission lacks authority to impose privacy and data security mandates on device manufacturers or application developers, and any action it takes here cannot include such entities. Moreover, there is no need for the Commission to broaden or alter its CPNI rules given the protections offered by currently-available tools.

## **II. THE COMMISSION’S AUTHORITY TO REGULATE PRIVACY IS SEVERELY CONSTRAINED**

Congress has granted the Commission only limited authority with respect to the protection of consumer privacy. The federal government’s foremost consumer protection agency, the FTC, should continue to exercise its plenary jurisdiction for protecting consumer privacy.<sup>6</sup> As the White House has recognized, the FTC has used its authority under Section 5 of the Federal Trade Commission Act<sup>7</sup> to take numerous enforcement actions that “effectively

---

<sup>6</sup> See, e.g., The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting and Promoting Innovation in the Global Digital Economy*, at 29 (Feb. 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> (“White House Report”) (“The FTC is the Federal Government’s leading consumer privacy enforcement authority.”).

<sup>7</sup> See 15 U.S.C. § 45. The FTC does not have authority to prosecute common carriers, but does have authority over the other entities involved in the mobile device ecosystem, including manufacturers, operating system providers, and app developers.

protect consumer data privacy within a flexible and evolving approach to changing technologies and markets.”<sup>8</sup> In addition, as discussed further below, the FTC carefully considered consumer privacy issues in the context of a major report earlier this year and separately has addressed the issue of mobile apps for children. Further, some states also have been active in this arena. In contrast, the FCC only has jurisdiction over specific aspects of information privacy and lacks the broad cross-industry data privacy enforcement experience of the FTC. The FCC’s main jurisdiction over privacy matters is found in Section 222 of the Communications Act, which provides that “[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of and relating to... customers....”<sup>9</sup> Under Section 222, “customer proprietary network information” means information “made available to the carrier by the customer solely by virtue of the carrier-customer relationship,” in addition to information contained in bills pertaining to certain telephone services received by a customer of a carrier.<sup>10</sup> Section 222 also limits disclosure and access to individually identifiable CPNI that is acquired “by virtue of [the carrier’s] provision of a telecommunications service....”<sup>11</sup> Section 222, however, does not provide the FCC with general authority to regulate privacy practices – it only governs defined information that is acquired in a specific manner by telecommunications carriers. Likewise, as discussed below, Section 222 applies only to telecommunications services, not data and other information services. The FCC thus does not have general authority to

---

<sup>8</sup> White House Report at 29.

<sup>9</sup> 47 U.S.C. § 222(a); *see also* 47 C.F.R. §§ 64.2001-.2011.

<sup>10</sup> 47 U.S.C. § 222(h)(1).

<sup>11</sup> *Id.* § 222(c)(1).

regulate privacy practices beyond the protections found in Section 222, which covers a shrinking part of the services and providers in the mobile marketplace.<sup>12</sup>

However, as WTB staff recognized in that bureau's May 2012 report on location-based services ("LBS"), the Commission can have a role in educating consumers about privacy and data security.<sup>13</sup> Pursuant to this role, the Commission could remind consumers of the importance of taking the initiative in safeguarding personal data on mobile devices by, among other things, setting passwords and reading privacy policies. The Commission could play a role in helping consumers learn about the numerous software and hardware tools that are readily available to consumers to help them protect their privacy and data.

### **III. THE LIMITED SCOPE OF SECTION 222 PROHIBITS ANY REGULATION OF MOBILE APPS, OPERATING SYSTEMS, OR MANUFACTURERS**

As the *Notice* implicitly recognizes, only the protection of CPNI by telecommunications carriers (in this case, wireless providers) is covered by Section 222. The Commission's CPNI authority does not extend to information collected or transmitted by mobile apps or operating systems. Further, the Commission has no authority to impose privacy mandates on manufacturers and operating system providers, and cannot mandate that products be designed in a particular fashion.

---

<sup>12</sup> Other sections of the Act also require communications providers to protect the personal information of subscribers of satellite and cable television providers. However, these sections, like Section 222, do not provide broad authority to regulate privacy practices. Instead, like Section 222, they only address specific circumstances.

<sup>13</sup> Federal Communications Commission Wireless Telecommunications Bureau, *Location-Based Services: An Overview of Opportunities and Other Considerations* (May 2012), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-314283A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-314283A1.pdf) ("LBS Report").

First, as discussed above, the Commission’s authority to regulate consumer privacy in the mobile wireless space is limited to the protection of CPNI.<sup>14</sup> Section 222 does not provide broad rulemaking authority to regulate privacy practices in the telecommunications industry – it merely provides that CPNI must be protected. CPNI is defined by statute as “information that relates 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 that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.*”<sup>15</sup> Information stored on the device that is collected or transmitted by applications or the mobile operating system is not *made available to the carrier by the customer solely by virtue of the carrier-customer relationship*, but rather is made available to third parties or the operating system provider irrelevant of the carrier-customer relationship. Such information is not and cannot be considered CPNI, and it thus does not and cannot fall under the Commission’s rules.<sup>16</sup>

Next, Section 222 clearly applies to “telecommunications carrier[s],”<sup>17</sup> and the Commission thus has no authority to impose privacy and data security mandates directly on manufacturers and operating system providers, which are not telecommunications carriers. The

---

<sup>14</sup> See 47 U.S.C. § 222(c)(1). In addition to customer information, Section 222 also provides for protection of proprietary information of, and relating to, carriers and equipment manufacturers. See *id.* §§ 222(a), (b).

<sup>15</sup> *Id.* § 222(h)(1) (emphasis added).

<sup>16</sup> Moreover, even if such information arguably could be considered CPNI, the collection, storage, and transfer of such information is still not within the Commission’s authority.

<sup>17</sup> 47 U.S.C. § 222(a).

*Notice* appropriately recognizes this distinction.<sup>18</sup> Moreover, Congress has not authorized the Commission to implement far-reaching privacy regulations that effectively would regulate manufacturers or application developers. Thus, the Commission lacks authority to adopt any “privacy by design” requirements.<sup>19</sup> While privacy by design is a laudable practice that already is employed by many manufacturers, the Commission cannot place privacy by design mandates on carriers because any such mandates would constitute indirect regulation of device manufacturers and information service providers (*e.g.*, application providers or software and operating system developers). Moreover, in contrast to the principle of privacy by design, Section 222 focuses on a certain type of information and that information’s use and access in the provision of telecommunications service or services used in the provision of such service.<sup>20</sup> The statute never speaks to the design of devices, but rather to the handling of a certain category of information that is obtained by a telecommunications carrier.

In this regard, the Commission should recognize that overbroad FCC regulations regarding the design of devices could have unintended consequences, and specific technological mandates for carriers and device manufacturers are not required to protect CPNI. Instead of

---

<sup>18</sup> *Notice* at 1 (soliciting 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....”) (emphasis added).

<sup>19</sup> *See, e.g., Notice* at 4 (“Should privacy and data security be greater considerations in the design of software for mobile devices, and, if so, should the Commission take any steps to encourage such privacy by design?”). The FTC, which released its privacy report in March 2012, recommended a general privacy by design regime through industry self-regulation. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 22 (Mar. 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>. As defined by the FTC, privacy by design means that “[c]ompanies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.” *Id.*

<sup>20</sup> *See* 47 U.S.C. § 222(a), (c).

mandating specific security standards which may not always be appropriate, the Commission should allow carriers and manufacturers through private negotiation and contract to decide the proper design and methods for protecting CPNI.<sup>21</sup> Carriers are already required under FCC rules to protect CPNI, and manufacturers collaborate with them to protect CPNI, in many cases engaging in privacy by design. Manufacturers, operating system providers, and carriers can and should engage in a meaningful dialogue regarding privacy by design, but should not be subject to a mandate that may have the effect of inhibiting innovation.

#### **IV. THE COMMISSION SHOULD NOT BROADEN OR ALTER THE CPNI RULES**

##### *A. EXISTING COMMISSION RULES, CONSUMER PROTECTION LAWS, AND INDUSTRY SELF-REGULATION SUFFICIENTLY PROTECT CONSUMERS*

As WTB staff noted in its recent LBS Report, “the Section 222 protections are sound, well understood by industry and consumers, and judicially approved,” and “the Commission has seen the number of consumer complaints related to CPNI decline steadily.”<sup>22</sup> While the *Notice* notes that technologies and business practices have evolved dramatically in the last five years,<sup>23</sup>

---

<sup>21</sup> Generally, in this complicated mobile ecosystem, the responsibility of different players for privacy and data security – including providing consumer notice and obtaining consumer consent – should track control. This is particularly true with respect to mobile devices, where components are supplied and controlled by a variety of ecosystem players other than device manufacturer. It is not possible for a device manufacturer to ensure that device components outside of its control contain appropriate privacy controls. Therefore, the device manufacturer should not be held responsible for ensuring the privacy controls of components that were outside its control. Given the number of entities and complexities involved, these matters are best left to private contract.

<sup>22</sup> LBS Report at 5; *see also Privacy and Data Security: Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science, & Transportation*, 112th Cong. (June 29, 2011) (statement of Austin C. Schlick, General Counsel, Federal Communications Commission).

<sup>23</sup> *Notice* at 1.

there is no evidence that the current CPNI regime is insufficient to protect consumers from improper handling of CPNI. Accordingly, there is no need for a change to the CPNI rules.<sup>24</sup>

More broadly, the FTC has been active in investigating and enforcing violations of consumer privacy. The FTC has authority to prosecute manufacturers that do not live up to claims and commitments that they made. Manufacturers should (and do) have privacy policies and procedures by virtue of existing laws and regulations. Should a manufacturer not follow the practices and promises it has identified in its privacy policy, it would be susceptible to an FTC enforcement action. The FTC's case-by-case enforcement has already induced companies to adopt additional safeguards to protect consumer privacy. Indeed, its February 2011 report, the White House noted the FTC's success and efficacy in protecting consumers' privacy.<sup>25</sup> The FTC has been tremendously effective in ensuring that consumer privacy is protected, whether the consumer is accessing content and services from a computer or a mobile device.

Evolving self-regulatory schemes also play an important role in protecting the privacy of the information stored on devices. Self-regulation has been effective in protecting consumers, and industry continues to evaluate and update self-regulatory models to ensure that consumers are adequately protected. In contrast to government mandates, which frequently struggle to keep pace with technological innovation, self-regulation provides needed flexibility for the

---

<sup>24</sup> The *Notice* notes the recent concerns raised regarding Carrier IQ. *See Notice* at 3. If the information transmitted by Carrier IQ was CPNI, then the current rules would be adequate for the Commission to find a violation if there had been a violation. In the alternative, if such information is not CPNI, then the FCC still would lack the authority to address any concerns regarding the collection of such information under new CPNI rules. Accordingly, the Carrier IQ controversy does not support a revision of the CPNI rules.

<sup>25</sup> *See* White House Report at 5.

development of new technology and services.<sup>26</sup> One example of self-regulation of privacy practices in the mobile wireless space is CTIA’s Consumer Code for Wireless Service.<sup>27</sup> Under the code, wireless carriers make their privacy policy concerning information collected available online and have agreed to abide by the Best Practices and Guidelines for Location-Based Services.<sup>28</sup> The Guidelines rely on two fundamental principles for LBS: user notice and consent.<sup>29</sup> These self-regulatory efforts in addition to others – including the efforts of CEA’s privacy working group – have provided for the protection of consumer privacy without sacrificing industry flexibility to develop new products and services.

Even more importantly, the NTIA multistakeholder processes to develop enforceable privacy codes of conduct, which was endorsed by the Administration, is just beginning.<sup>30</sup>

---

<sup>26</sup> See, e.g., *Statement of Commissioner Jessica Rosenworcel, Nominations Hearing: Hearing Before the S. Comm. On Commerce, Science, & Transportation*, 111th Cong. 1-2 (2011) (“[C]ommunications technology is changing at a brisk pace. Laws and regulations struggle to keep up. . . . In approaching this challenge, I believe that a little humility helps.”); *Statement of Commissioner Meredith Baker. Preserving the Open Internet; Broadband Industry Practices*, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17905, 18090 (2010) (also calling for regulatory humility).

<sup>27</sup> CTIA, *Consumer Code for Wireless Service* (2011), available at [http://files.ctia.org/pdf/The\\_Code.pdf](http://files.ctia.org/pdf/The_Code.pdf).

<sup>28</sup> CTIA, *Best Practices and Guidelines for Location-Based Services*, v. 2.0 (Mar. 23, 2010), available at [http://files.ctia.org/pdf/CTIA\\_LBS\\_Best\\_Practices\\_Adopted\\_03\\_10.pdf](http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf).

<sup>29</sup> *Id.* at 1. More specifically the Guidelines provide: “First, LBS Providers must ensure that users receive meaningful notice about how location information will be used, disclosed and protected so that users can make informed decisions whether or not to use the LBS and thus will have control over their location information. Second, LBS Providers must ensure that users consent to the use or disclosure of location information, and LBS Providers bear the burden of demonstrating such consent. Users must have the right to revoke consent or terminate the LBS at any time.” *Id.*

<sup>30</sup> Press Release, National Telecommunications & Information Administration, *First Privacy Multistakeholder Meeting: July 12, 2012* (rel. June 15, 2012), available at <http://www.ntia.doc.gov/other-publication/2012/first-privacy-multistakeholder-meeting-july-12-2012> (“First Multistakeholder Process Meeting Announcement.”)

Industry, advocates, academics, law enforcement, state attorneys general, and others have been invited to participate in these processes.<sup>31</sup> As noted by the White House Report, the multistakeholder processes “can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges” and “can produce solutions in a more timely fashion than regulatory processes and treaty-based organizations.”<sup>32</sup> This is the appropriate forum for government, together with industry and consumer groups, to consider privacy issues in the mobile ecosystem. Indeed, the goal of the very first process, beginning this week, “is to develop a code of conduct to provide transparency in *how companies providing applications and interactive services for mobile devices handle personal data.*”<sup>33</sup> The codes of conduct established through the processes will supplement the ample privacy protections already in place for consumers.

It would be an inopportune time to revise the CPNI rules, given the numerous industry and government efforts already underway to address consumer privacy on mobile devices. At the very least, the Commission should allow the multistakeholder process to work and allow industry to develop, through the processes, appropriate and well-balanced self-regulatory models that would be enforceable by the FTC.<sup>34</sup> Should the Commission believe that any eventually developed self-regulatory model still leaves gaps with respect to the protection of CPNI – and only CPNI due to the Commission’s limited authority – it can then initiate a proceeding to fill

---

<sup>31</sup> See White House Report at 23.

<sup>32</sup> *Id.*

<sup>33</sup> First Multistakeholder Process Meeting Announcement (emphasis added).

<sup>34</sup> See White House Report at 27 (“The Administration expects that a company’s public commitment to adhere to a code of conduct will become enforceable under Section 5 of the FTC Act (15 U.S.C. § 45), just as a company is bound today to follow its privacy statements.”).

those gaps. Any action prior to that point, including the adoption of privacy by design principles, would be vastly premature.

*B. CONSUMERS HAVE NUMEROUS BUILT-IN TOOLS TO PROTECT INFORMATION STORED ON THEIR DEVICES*

Consumers can further protect the information stored on their devices by using the numerous built-in tools that manufacturers and operating system providers offer to enable consumers to protect their privacy and better manage the information stored. Indeed, device users are often encouraged to opt to use these built-in protections. For instance, devices generally have built-in tools to enable owners to “lock” their handsets, and many manufacturers provide detailed instructions on how to do so.<sup>35</sup> Such tools prevent unauthorized access to the information on the device should it be lost or stolen and users are typically encouraged upon booting the device for the first time to implement the “lock” feature. Consumers are thus empowered and encouraged by manufacturers and operating system providers to take proactive steps that will ensure that the information stored on their devices is protected.<sup>36</sup>

---

<sup>35</sup> By December 31, 2012, all manufacturers will include information on how to secure and/or lock new smartphones in-box and/or through online “Quick Start” or user guides. *See* Press Release, CTIA, *U.S. Wireless Industry Announces Steps to Help Deter Smartphone Thefts and Protect Consumer Data* (Apr. 10, 2012) (“*CTIA Press Release*”), available at <http://www.ctia.org/media/press/body.cfm/prid/2170>.

<sup>36</sup> There is also a robust, yet still growing, ecosystem of solutions that have been developed to address privacy issues, many of which are commercially available for individual consumers. For example, available third-party applications allow users to add additional layers of protection on their devices through additional passwords to access certain stored data. Other applications enable users to remotely wipe or lock a device and/or store encrypted information on the device, providing yet an additional layer of protection should the device be lost or stolen. In addition, there are numerous antivirus and antimalware applications available for consumers to download, which can help protect consumers from malicious applications that collect and send personal data without authorization. These applications, many of which are available for free, can easily be downloaded through the various app stores.

Device manufacturers and operating system providers also take affirmative steps to protect consumers' geolocation information. For example, Apple's iPhone notifies a user when a pre-loaded application or a third-party application is using the handset's geolocation information and requires the user to "opt-in" through a set of prompts. Additionally, at any time, an iPhone user can turn off the handset's ability to communicate geolocation information through the "Location Services" tab in the phone's Settings Menu. Similarly, applications for Google's Android operating system display permissions requested by an application to users before the application is installed. These protections ensure that consumers are aware that geolocation information may be used or collected and authorize such collection and use.

Particularly with the prevalence of these tools, consumers can take responsibility for the data and applications they download and store on connected devices that can impact their personal and financial security. To this end, manufacturers, software developers, and carriers intend to continue their efforts to work together to educate consumers on the tools available to protect their privacy and secure their data.<sup>37</sup> The FCC can be instrumental in supporting and participating in these educational efforts.

---

<sup>37</sup> See generally *CTIA Press Release*.

## V. CONCLUSION

Consumer electronics manufacturers understand the critical importance of protecting consumer privacy. CEA members have taken numerous steps in this regard and continue to participate in industry self-regulatory efforts, including through CEA's own privacy working group, as well as government-facilitated processes. The Commission is not the appropriate forum to consider mobile privacy issues as a general matter, and in any event, CPNI is adequately protected under existing laws and through the use of existing consumer tools. At the very least, the Commission should postpone any action in the instant proceeding until conclusion of the NTIA multistakeholder process and the related development of industry codes of conduct.

Respectfully submitted,

CONSUMER ELECTRONICS  
ASSOCIATION

By: /s/ Julie M. Kearney

Julie M. Kearney  
Vice President, Regulatory Affairs

Laura Knapp Chadwick  
Manager, Government Affairs

Consumer Electronics Association  
1919 S. Eads Street  
Arlington, VA 22202  
(703) 907-7644

July 13, 2012