

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information)	CC Docket No. 96-115
)	
Privacy and Security Information Stored on Mobile Communications Devices)	DA 12-818
)	

REPLY COMMENTS OF T-MOBILE USA, INC.

T-Mobile USA, Inc. (“T-Mobile”) hereby replies to comments submitted in response to the Public Notice (“*Public Notice*”) issued on May 25, 2012 in the above-captioned proceeding regarding privacy and security of customer information stored on mobile communications devices.¹

INTRODUCTION AND SUMMARY

T-Mobile places a very high priority on safeguarding its customers’ personal information and works continually to ensure that its collection, use, storage, and sharing of customer data comply with the law, the Commission’s customer proprietary network information (“CPNI”) rules, and T-Mobile’s robust privacy policy.²

¹ *Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, Public Notice, CC Docket No. 96-115, DA 12-818 (WCB/WTB/OGC May 25, 2012) (“*Public Notice*”). The *Public Notice* seeks comment to “refresh the record” in a 2007 proceeding. *Public Notice* at 4; see also *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).

² For example, T-Mobile abides by the CTIA—The Wireless Association (“CTIA”) Code for Wireless Conduct, available at files.ctia.org/pdf/The_Code.pdf, which requires T-Mobile to “abide by a policy regarding the privacy of customer information in accordance with applicable

The record in this proceeding provides a number of compelling reasons for the Federal Communications Commission (“FCC” or “Commission”) to refrain from expanding its CPNI rules at this time. First, the mobile wireless ecosystem is dynamic and complex, and any privacy-related regulation limited to carriers would be unbalanced and ineffective. Any effort to address mobile device privacy must also consider the many layers of interaction between carriers, devices, operating systems, and applications (“apps”), thereby requiring a regulatory approach that is consistent and integrated. Given the limited nature of the Commission’s jurisdiction under Section 222 of the Communications Act³—which by definition applies only to carriers and telecommunications services—this FCC CPNI proceeding is not the proper forum for action.

Second, the record also demonstrates that many uses of data on mobile devices are beneficial to customers and allow carriers to diagnose and quickly address any problems with the network or with devices on the network. Such uses, which are currently permitted by law, do not threaten consumer privacy. Moreover, piecemeal or premature attempts to regulate in this area run the risk of constraining the benefits of such uses.

Third, given the recently-launched Obama Administration multi-stakeholder effort, facilitated by the Department of Commerce’s National Telecommunications and Information Administration (“NTIA”), the Commission should wait to address mobile device privacy. Through this process, the White House contemplates that voluntary industry codes of conduct

federal and state laws, and [to] make available to the public its privacy policy concerning information collected online.” T-Mobile also abides by the CTIA Best Practices and Guidelines for Location-Based Services, available at http://www.ctia.org/consumer_info/service/index.cfm/AID/11300.

³ 47 U.S.C. § 222.

will be developed and then backstopped by Federal Trade Commission (“FTC”) enforcement.⁴ Indeed, the first topic selected to be addressed by NTIA is ensuring that companies providing apps and interactive services are transparent with respect to how mobile devices handle personal data.⁵ T-Mobile urges the Commission to monitor—and perhaps assist with—the NTIA multi-stakeholder process, rather than taking premature, piecemeal action that could be inconsistent with, and potentially disrupt, the broader Administration-endorsed NTIA process. Once that process is completed and the relevant voluntary code(s) of conduct established, the Commission can consider whether any carrier-specific privacy concerns exist in the mobile ecosystem that require Commission attention.

DISCUSSION

I. THE MOBILE WIRELESS ECOSYSTEM IS DYNAMIC AND COMPLEX

As numerous commenters have demonstrated in response to the *Public Notice*, today’s wireless device marketplace is vibrant and layered, and mobile device privacy-related regulation limited to carriers therefore would be unbalanced and ultimately ineffective.⁶ This market has been, and continues to be, noted for its rapid rate of change, as consumers today are choosing to

⁴ See 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 Privacy Blueprint”). See also FTC, *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> (“FTC Privacy Report”).

⁵ 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>.

⁶ See generally AT&T Inc. (“AT&T”) Comments, Consumer Electronics Association (“CEA”) Comments, CTIA Comments, Sprint Nextel Corporation (“Sprint”) Comments, and Verizon Wireless Comments. (All comments referenced herein were filed in the instant docket on or around July 13, 2012, unless otherwise noted.)

store and share their own data—including location information—without carrier involvement.⁷ Recognizing the continual need to safeguard customer information, mobile wireless service providers have established privacy practices that can evolve in response to the ever-developing technologies at issue, the changing demands and expectations of consumers, and the explosion of data use.⁸ As many commenters have pointed out, however, the market is too complex for carriers alone to protect consumer privacy.⁹ Although carriers play a part in the data collection process, such data also is collected and stored by device manufacturers, apps developers, operating systems, and consumers themselves. For example, a handset purchased at a T-Mobile store may be manufactured by one of several companies, could run on one of multiple operating systems, and could host applications from myriad developers. Any of these manufacturers or developers may collect, use, store, and/or share customer data. Responsibility for safeguarding customer information becomes even more complex once a handset leaves the store, because users may later download apps from a wide range of storefronts without T-Mobile’s knowledge. Such apps—which often utilize customer information and provide substantial value from the consumer perspective—typically are wholly independent of any carrier and may store data either on the device or in the cloud.

⁷ See, e.g., Jason Kincaid, *Zuckerberg: Online Sharing Is Growing At An Exponential Rate (And Users Are Sharing 4 Billion Things a Day)*, TechCrunch (July 6, 2011), available at <http://techcrunch.com/2011/07/06/zuckerberg-online-sharing-is-growing-at-an-exponential-rate-and-users-are-sharing-4-billion-things-a-day/> (“Facebook has observed [that] the rate that its users are sharing is increasing in an exponential rate”); Ernan Roman, *Megatrend #3: Consumers Shared Detailed Information in Exchange for Value*, HUFFINGTON POST (Nov. 30, 2010), available at http://www.huffingtonpost.com/ernan-roman/megatrend-3-consumers-sha_b_789808.html (“[T]here is a growing recognition among consumers that, in order to receive or access increasingly relevant information, they must share increasing amounts of information about their preferences.”).

⁸ See, e.g., AT&T Comments at 5-7.

⁹ See, e.g., *id.* at 5-8; Sprint Comments at 3-5; Verizon Wireless Comments at 2-4.

As AT&T explains, rules that single out telecommunications services, while ignoring the large majority of other services and providers that obtain and use substantially the same (or more) consumer information, are “anachronistic in the new mobile landscape” and cannot even protect privacy and security, because they fail to reach the entities that most implicate consumer privacy.¹⁰ In 2012, carriers are neither the gatekeepers nor sole enablers of the mobile experience, and accordingly, the Commission should not try to use its CPNI rules to impose new mobile device-related privacy obligations on carriers alone.¹¹

II. MANY ESSENTIAL AND BENEFICIAL DATA USES COULD BE CONSTRAINED BY PIECEMEAL REGULATORY EFFORTS

There are many essential and beneficial uses of data stored on mobile devices.¹² Most notably, wireless carriers use network diagnostic information to improve the customer experience and assist in rendering service.¹³ As wireless devices have become more complex and consumer use of those devices has diversified, customers seek assistance from T-Mobile in resolving issues on a broad range of device, service, and performance issues. To respond to these inquiries in a timely manner and achieve results that help maintain high levels of customer satisfaction, T-Mobile needs data about how, when, and where customers are using their devices. As discussed above, T-Mobile is vigilant in safeguarding this data.

¹⁰ AT&T Comments at 8. *See also*, Sprint Comments at 10; Verizon Wireless Comments at 8; CTIA Comments at 4.

¹¹ Further, as numerous commenters explain, there are serious questions regarding the extent to which the data on a mobile device constitutes CPNI. *See* CTIA Comments at 6-10; Verizon Wireless Comments at 8; Sprint Comments at 11-14.

¹² *Public Notice* at 1 (“Service providers’ collection and use of this information may be a legitimate and effective way to improve the quality of wireless services.”).

¹³ *See, e.g.*, CTIA Comments at 5.

For example, when customers call T-Mobile’s care representatives with complaints about their devices or with the network, its care representatives can access system diagnostic data to troubleshoot issues and, ideally, resolve them expeditiously. T-Mobile also obtains information that helps the company determine how its network is working and how it may be improved (*e.g.*, if a significant number of customers are dropping calls in one particular area, then T-Mobile’s engineering team may prioritize that area in building out service). Likewise, if a particular model of phone is experiencing more dropped calls than others, T-Mobile can work with the manufacturer to address any issues. Carriers need to make assessments about their network performance by monitoring their networks and the performance of devices on those networks; diagnostic tools assist a provider in better understanding performance issues by aggregating data and incorporating handset information. These uses of customer data are beneficial to *all* of a carrier’s customers. Any regulation relating to carriers’ involvement with, or use of, such software here would be piecemeal and premature, and it would constrain carriers’ ability to better serve customers through the use of diagnostic tools.

In addition to protections employed directly by carriers such as T-Mobile, many carriers and manufacturers also offer numerous tools that enable customers to protect the security and privacy of their information.¹⁴ Carriers have committed to educate consumers about smartphone theft, protections, and preventative measures by launching a new campaign this month that highlights the range of resources available.¹⁵ T-Mobile’s website has tools to help better inform

¹⁴ See, *e.g.*, CEA Comments at 13-14; Sprint Comments at 11.

¹⁵ 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> (committing the wireless industry by July 1, 2012, to “launch an education campaign for consumers on the safe use of smartphones and highlight [new] solutions by using a range of resources, including a public service announcement and online tools such as websites and social media”).

customers about safeguarding their information and devices, including instruction on what to do if a phone is lost or stolen, measures taken by the company to protect CPNI, tips about password security, and practices to help mitigate identity theft.¹⁶

III. ONGOING INDUSTRY SELF-REGULATORY INITIATIVES AND THE RECENTLY-LAUNCHED MULTI-STAKEHOLDER PROCESS WILL BE MORE APPROPRIATE AND EFFECTIVE THAN FCC REGULATION

The Commission should allow ongoing industry self-regulatory initiatives to proceed without regulatory interference.¹⁷ The weight of the record evidence indicates that such industry efforts are the most effective means to address complex issues—such as consumer privacy—that arise from the continued evolution of communications networks and equipment.¹⁸

In this case, industry self-regulation is further bolstered by the pending voluntary, multi-stakeholder process at NTIA. Outlined in the White House Privacy Blueprint, the process is intended to facilitate the development of voluntary codes of conduct on particular privacy sub-topics, such as transparency regarding privacy practices for mobile apps and interactive services. Once developed through the NTIA process and adopted by industry entities, the codes of conduct will be backstopped by FTC enforcement. This process, announced less than six months ago by the Obama Administration, already is underway. Although numerous areas of consumer privacy will be addressed through the process, NTIA determined that the first topic would be the mobile environment; it convened an initial multi-stakeholder meeting on this topic earlier this month. Any FCC carrier-focused effort regarding mobile device privacy could be inconsistent with, and

¹⁶ See www.t-mobile.com/Company/PrivacyResources.aspx?tp=Abt_Tab_IdentityTheft; www.t-mobile.com/devicesecurity.

¹⁷ See, e.g., TechAmerica Comments at 4 (ongoing initiatives by the Digital Advertising Alliance, the Mobile Marketing Association and CTIA should be allowed to proceed without regulatory interference).

¹⁸ See, e.g., Alliance for Telecommunications Industry Solutions Comments at 1.

potentially disrupt, the broader Administration-endorsed NTIA process. The FCC can best foster a consumer-friendly environment for mobile privacy by using its expertise on telecommunications services to support, and perhaps assist, NTIA as that agency works with industry and other stakeholders to develop a broader privacy and security framework.¹⁹

The NTIA multi-stakeholder process also is preferable to Commission action because it has the potential to set technology-neutral standards of conduct for all participants in the mobile wireless ecosystem, a result that cannot be achieved under the Commission's CPNI rules. As discussed above, any privacy concerns should be addressed comprehensively, not through piecemeal regulation of the telecommunications service-related privacy and security practices of carriers alone.²⁰ The NTIA process also is better suited to maintain the flexibility that wireless carriers need in implementing privacy protections.²¹ CEA correctly states that where the industry is working on its own—and, particularly as in this case, *with* government—to develop and ensure consistent and appropriate practices, regulation is unwarranted.²²

The Commission should allow the NTIA multi-stakeholder process to advance, and should wait for the participants in that process to establish the voluntary industry codes of conduct contemplated in the White House Privacy Blueprint.

¹⁹ See AT&T Comments at 10-11; see also Comments of Internet Commerce Coalition at 2 (the NTIA multi-stakeholder process is a more appropriate framework [than FCC regulation] and will avoid making the thicket of medium-specific communications sector privacy regulation even more complex than it already is).

²⁰ Verizon Wireless Comments at 5-6; see also TechAmerica Comments at 5-6.

²¹ See, e.g., CTIA Comments at 5.

²² CEA Comments at iii.

CONCLUSION

The record is clear that the concerns raised in the *Public Notice* do not warrant action by the Commission at this time. If there is a need to consider mobile device privacy, such a review must also include examination of the many layers of interaction between carriers, devices, operating systems, and apps to ensure a regulatory approach that is balanced and effective in scope. As noted above, the CPNI rules are not the appropriate vehicle for such regulatory action. Instead, T-Mobile urges the Commission to monitor—and perhaps assist with—the NTIA multi-stakeholder process, which is specifically intended to take such a consistent, broad approach.

Respectfully submitted,

T-MOBILE USA, INC.

/s/ Kathleen O'Brien Ham

Kathleen O'Brien Ham
Luisa L. Lancetti
Shellie Blakeney
601 Pennsylvania Avenue, NW
North Building - Suite 800
Washington, DC 20004
(202) 654-5900

July 30, 2012