Before the

WIRELINE COMPETITION BUREAU, WIRELESS TELECOMMUNICATIONS BUREAU

AND OFFICE OF GENERAL COUNSEL

FEDERAL COMMUNICATIONS COMMISSION

Washington, DC

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

COMMENTS OF

THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

July 13, 2012

Daniel Castro

Information Technology and Innovation Foundation[1]
1101 K Street NW, Suite 610
Washington, DC 20005

[1] ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

Introduction

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Federal Communication Commission's (FCC's) request for comment on the privacy and security of information stored on mobile devices. Primarily these comments will address FCC's inquiry into whether it should take steps to encourage privacy and security in the design of mobile devices by exercising its authority under Section 222 of the Communications Act.

The FCC's Authority Does Not Extend to Regulating the Applications and Operating Systems on Mobile Devices

The FCC is seeking comments on its analysis that Section 222(h)(1) of the Communications Act of 1934, as amended, gives it authority to regulate "information collected at a carrier's direction even before it has been transmitted to the carrier."[1] Section 222 defines customer proprietary network information (CPNI) 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." The FCC's suggested interpretation would seem to suggest that it could regulate all of the software, including mobile apps and operating systems, that is initially distributed on mobile phones by a carrier.

The FCC's proposed interpretation is not valid based on a close reading of Section 222(h)(1). The text is clear that the CPNI clause only covers specific types of information collected by carriers, not all possible customer information. Moreover, it certainly does not extend to the mechanisms that may be used to collect information. If it did, then this would suggest the FCC could, under this authority, regulate every aspect of the device that collects input including microphones, keyboards, touch screens, and any other sensor. On the contrary, the intent of the language in this section seems to clearly identify information that a telecommunications service provider might have access to as a result of its unique relationship with its customers. Historically the nature of telecommunications has meant that carriers providing services to customers have access to certain information about their customers. Examples of this customer information include the amount and type of services used, the destination of communication, the location of the customers, and technical information about the devices used. The FCC should continue to limit its authority to this scope.

Carriers Should Be Allowed to Use Third-Party Products

While service providers need CPNI for billing and operational purposes, they also have a responsibility to maintain the privacy of this information. Identifiable information can only be used for specific purposes, such as for billing or public safety. In addition, the collection and use of CPNI may be necessary at times to detect and diagnose problems with the network or devices

on the network. This restriction should not prohibit carriers from using third-party services to assist with these functions.

Particular concern has been raised by the FCC about the use of third-parties, such as Carrier IQ, by carriers. Carrier IQ is a software-based solution that is embedded in mobile devices. Many carriers use products like Carrier IQ as a diagnostics and analytics tool to better understand their customers, the devices used on their networks, and the performance of their networks. Types of data collected by Carrier IQ include data on when and where calls fail; where customers have problems accessing the network; and the reliability and battery performance of the make and model of devices.[2] This type of information is then used to improve service quality and answer the questions of consumers. For example, this information can be used so that a service provider's technical support staff can help their customers better understand and resolve issues, such as a mobile device losing connectivity in a certain location or a tablet PC's battery draining too quickly. Consumers would be worse off if the FCC disallowed these types of product or service or made it more difficult for carriers to use them.

Allow Carriers to Innovate with Aggregated and De-Identified Data

Under Section 222, carriers are permitted to use, disclose and permit access to CPNI that has been aggregated and de-identified. The FCC should ensure that if it does pursue rulemaking under Section 222, it does not impair the ability of carriers to use aggregated and de-identified data. The FCC should not make any decisions without considering the impact that changes might have on the availability of certain data. Data such as these may have important uses for consumers, especially as new opportunities are identified for using geo-location data. For example, this data may be used to identify and improve real-time information about traffic patterns, thereby reducing congestion and enabling transportation planners to improve roadways or better deploy transit options.

Keep a Narrow Focus and Do Not Duplicate Existing Efforts Already Underway

Finally, if the FCC moves forward with its interpretation of Section 222, it is unclear the scope of devices that the FCC might consider under this authority. There are an increasing number of devices that communicate using mobile wireless networks. For example, modems for mobile networks are also used to connect devices in many settings, such as health care, and in-vehicle systems are increasingly using mobile networks for access to information and entertainment. In addition a variety of other devices including smart phones, tablet PCs, netbooks, notebooks, GPS devices, e-book readers, and wireless sensors use mobile networks as well.

Many mobile phones today contain more computing power than the average desktop computer did a decade ago. Just as the FCC did not attempt to extend its authority to regulate the software on PCs, neither should the FCC attempt to extend its authority to regulate these mobile devices

or the software that runs on these devices. There is in fact, no rational distinction between information collected on a non-mobile device (e.g., a desktop computer) and a mobile one, and therefore no rationale for regulating the latter. However, if the FCC moves forward with its interpretation, it should keep its focus as narrow as possible.

All players in the Internet ecosystem, including the mobile Internet ecosystem, should work together and share responsibility for solving unique challenges online. This requires balancing the different needs of stakeholders and the different opportunities that each stakeholder has to implement a solution. Wireless carriers are just one of many stakeholders on the mobile Internet, and the FCC should be careful not to impose unfair burdens on them. The mobile Internet ecosystem is complex and has many stakeholders. It includes mobile device manufacturers, mobile operating system developers, mobile application developers, mobile app stores, and users, to name just a few. Each of these may all be better positioned to enact certain policies, such as enabling better transparency of data handling practices or restricting certain behaviors on mobile devices. And of course at times users may be in the best position to influence how their data is handled through their decisions about what information to share, what devices to purchase, and what applications to use.

Finally, the FCC should only consider pursuing consumer privacy rulemaking if it finds that consumers face specific privacy harms. If the FCC does identify harms, then before taking action, the FCC should consider the extent to which other regulatory efforts are already underway. First, there are a number of industry-led self-regulatory efforts that address some of the issues raised by the FCC.[3] Second, National Telecommunications and Information Administration (NTIA) has already launched a multi-stakeholder process to develop consumer data privacy codes of conduct in partnership with consumer interest groups and the private sector.[4] And of course the Federal Trade Commission (FTC) has jurisdiction over some privacy issues and has proposed legislation to give it more. For example, the FCC has asked in this notice whether consumers are given sufficient notice with regards to the information practices of service providers. Both industry-led and government-led processes are already pursuing this line of questions. Rather than duplicate existing efforts, the FCC should allow existing avenues of self-regulation and co-regulation to be pursued. Given the rapid rate of change in this industry, where possible, the FCC should apply a light touch and rely on flexible industry codes of conduct, rather than more restrictive government regulations, to govern how information is used.

Conclusion

In short, the FCC should not extend its authority to regulate the software that is installed on mobile devices. The current uses of CPNI by carriers are appropriate and neither the FCC nor consumers advocacy group have identified any specific harms to consumers. While privacy is an important issue to consider, the potential negative impact of additional regulation on the mobile Internet, mobile devices, and mobile applications should be considered as well. The FCC should

instead use its expertise to help identify issues that need attention and actively participate in existing multistakeholder efforts to improve consumer privacy.

Endnotes

[1] "Comments Sought on Privacy and Security of Information Stored on Mobile Communication Devices," Federal Communications Commission, May 25, 2012, http://www.fcc.gov/document/privacy-and-security-information-mobile-devices.

[2] "Understanding Carrier IQ: What Carrier IQ Does and Does Not Do," Carrier IQ, December 12, 2011, http://www.carrieriq.com/documents/12-december-2011-understanding-carrier-iq-technology/6596/.

[3] For a detailed look at self-regulation and online privacy, see Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising," Information Technology and Innovation Foundation, December 2011, http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.

[4] See for example, "July 12, 2012 Privacy Multistakeholder Meeting," National Telecommunications & Information Administration, July 11, 2012, http://www.ntia.doc.gov/other-publication/2012/july-12-2012-privacy-multistakeholder-meeting-details.