
*Perspectives from FSF Scholars*
*July 30, 2012*
*Vol. 7, No. 19*

# The FCC's Mobile Data Inquiry: No New Privacy Regulation Needed

**by**

**Seth L. Cooper ***

Through July 30 the FCC is accepting public comments on its *Public Notice* inquiring into mobile data privacy and security. In the *Notice*, the FCC raises a number of questions about mobile data collection and use as well as how current practices might be brought under new regulatory controls.

The FCC's mobile data privacy inquiry may yield some interesting information. But new FCC regulations would be the wrong approach to address whatever mobile privacy concerns might exist in today's data and information-rich wireless market. The White House's comprehensive digital privacy initiative provides the better pathway for addressing data privacy policy across all broadband platforms.

**The complex and dynamic nature of the wireless marketplace makes it unwise for the FCC to impose a set of prescriptive rules regarding the transmission, storage, and use of data to or from wireless devices.**

In the span of just a few years tidal waves of continuous technological innovation have transformed wireless services. The days when wireless was a voice-centric service have given way to a new era. Wireless now serves a data-centric platform offering an expanding array of complex functionalities. Consumers are increasingly adopting smartphones which include features like specialized operating systems and web

browsers, streaming video viewing capabilities, downloaded apps, microSD chips for extra data storage, Wi-Fi connectivity and tethering, and built-in digital cameras. This transformation cautions against any attempt to force-fit onto today's wireless data and information services market a set of requirements geared to traditional telephone services. In the face of such rapid change and growing complexity, rigid rules covering the myriad of mobile functions involving consumers' data use and storage are impractical and a potential obstacle to continuing innovation. And a thicket of new rules would run counter to the light-touch regulatory environment in which the dynamic wireless market emerged.

If wireless carriers once held exclusive or gatekeeper control over consumers' mobile data, they no longer do so now. In any number of circumstances, personally identifiable information as well as text or e-mail communications may be transmitted or stored with device manufacturers, cloud-based service operators, or mobile app providers. Wireless carriers do not typically have access to much of this information, or to other information or content generated by consumers and stored on their devices or transmitted via Wi-Fi connections instead of the carriers' mobile networks. (And in many cases consumers have a variety of tools at their disposal to determine access to and use of their personal data.)

This means that any attempt by the FCC to impose more stringent mobile data privacy rules on wireless carriers would at best amount to a piecemeal approach. That would leave unaddressed any mobile data privacy issues raised by all the remaining dimensions of the so-called wireless eco-system. Not to mention mobile data and information services are typically integrated with non-mobile or fixed components, offering consumers non-mobile applications and relying on fixed networks for backhaul and storage.

**Congress never gave the FCC authority to comprehensively regulate mobile data privacy.**

The FCC's authority over "customer proprietary network information" (CPNI) under Section 222 of the Communications Act is too limited to address the present and future scope of mobile data use and storage practices. That section is part of the FCC's common carrier or Title II authority regarding traditional voice services. It specifically is directed to "[e]very telecommunications carrier," and to information "made available to the carrier by the customer solely by virtue of the carrier-customer relationship," along with billing information relating to carriers' voice services.

In particular, CPNI specifically addresses telecommunications providers' collection and use of individualized consumer data regarding the time and length of calls, phone numbers called, and consumer voice billing information. Therefore much of the mobile data and information created and stored on wireless devices by today's consumers are not CPNI. Also, device manufacturers, operating system and app software developers, and other competitors providing mobile data and other information services throughout the various segments and layers of the wireless market are beyond Section 222's reach.

**Mobile data privacy policy should be addressed through the Administration's multi-stakeholder digital privacy initiative, and FCC jurisdiction over privacy should be removed.**

In February, the White House released "Consumer Data Privacy in a Networked World: A Framework for Promoting Privacy and Promoting Innovation in the Global Digital Economy." This white paper lays the foundation for a comprehensive approach to consumer data privacy protection. It sets out a set of basic principles regarding consumer digital privacy expectations and calls for a multi-stakeholder process for voluntary implementation of those principles through development of codes of conduct. The Administration's framework calls for legislation to give the FTC enforcement power under Section 5 of the FTC Act with respect to all service providers that agree to adhere to the codes. And those who follow those codes in practice gain safe harbor from direct FTC enforcement.

Importantly, the white paper explains that "the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers." In an April *Perspectives* essay, FSF President Randolph May and I explain why "Any New Privacy Regime Should Mean An End To FCC Privacy Powers." FTC enforcement should coincide with the removal of FCC jurisdiction over consumer privacy for voice services (Section 222), cable services (Section 551) and direct broadcast satellite (Section 338 of the Satellite Home Viewing Improvement Act).

Establishing a common set of standards through a common enforcer makes sense for both providers of mobile data and information services and for wireless consumers. Providers of data and information services require clarity and predictability in the law. That allows them to follow the rules and avoid unnecessary compliance costs. And from a consumer's perspective, simple and consistent rules offer the most user-friendly approach. It's unreasonable to presume consumers prefer privacy controls and protections that differ based on whether the data is handled by a mobile broadband service provider or a mobile app provider.

Ultimately, the Administration's ongoing digital privacy initiative should be given a chance to carry out its mission. A hoped-for set of common data privacy standards should coincide with a coordinated federal agency response. To the extent that the FCC's mobile data privacy inquiry provides useful information to facilitate the Administration's process, the FCC's inquiry is fine. But new FCC regulatory mandates on mobile data information use and collection must be avoided, particularly when the Administration's digital privacy initiative calls for the FCC's limited jurisdiction to finally be transferred to the FTC.

* Seth L. Cooper is a Research Fellow of the Free State Foundation, a non-partisan Section 501(c)(3) free market-oriented think tank located in Rockville, Maryland.