

FCC Requests Comments on the Privacy and Security of Information Stored on Mobile Communications Devices

June 2012

With features that can turn a simple electronic device the size of a deck of playing cards into a personal assistant, personal shopper, navigation system and lifeline, consumers are turning to mobile devices for more and more of their daily activities. To take full advantage of these emerging mobile opportunities, consumers are trusting mobile devices with increasing amounts of personal information.

At the same time, providers of mobile services may use these same expanded capabilities to collect information about customers' use of the device, the mobile network or customers' locations. While such practices are usually tied to important network management and efficiency goals, they also carry with them a potential threat to consumers' personal information. The juxtaposition between this benefit and potential threats has led the Federal Communications Commission (FCC) to solicit comments regarding these practices and the security of consumers' personal information.

30-Day Comment Period

Five years after launching an initial inquiry on the matter, the FCC has issued a Public Notice requesting comments on wireless service providers' privacy and data security practices with respect to information stored on their customers' mobile communications devices. Based on the hypothetical questions posed, the FCC is interested in comments regarding current data collection practices, policy implications related to such practices and the potential relationship between such practices, and Communications Act

Authors

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

Section 222—specifically, whether customer information stored or collected via mobile device constitutes Customer Proprietary Network Information (CPNI). The notice was published in the *Federal Register* on June 13, 2012. Comments are due by July 13, 2012, and reply comments are due by July 30, 2012.

Areas of Interest

First, the FCC is interested in comments relating to current data collection practices. For example, the FCC asks how mobile service providers' collection practices have changed since its 2007 inquiry. It also asks if consumers are currently given meaningful “notice and choice” with respect to data collection. Additionally, the FCC asks if the current collection practices serve the needs of providers and customers.

Second, the FCC is soliciting comments regarding potential policy concerns associated with wireless service providers' current wireless device privacy and data security practices. For instance, the FCC asks potential commenters if providers' current practices raise privacy concerns and if risks associated with the practices are similar or different from the risks that the Commission has historically addressed under its CPNI rules. The FCC also asks if privacy and data security should be larger considerations in the design of mobile devices, and, if so, what steps the Commission should take to encourage such “privacy by design.” Additionally, the FCC asks to what extent consumers should be charged with ensuring the privacy and security of data on mobile devices under their own control.

Third, the FCC asks for comments concerning the applicability of Section 222 of the Communications Act of 1934 to the privacy and security of consumer data on mobile devices. In asking for comment on whether the Section 222(a) duty to protect customer information applies to wireless providers in this context, the FCC asks if the definition of CPNI provided in Section 222(h)(1) could apply to “information collected at a carrier's direction even before it has been transmitted to the carrier.”

Finally, the FCC asks for comments regarding what factors it might consider when assessing a wireless provider's obligations under Section 222 or the Commission's implementing rules. If carriers have such obligations in this context, the FCC asks how Section 222's requirement that carriers “take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI” would apply, and what obligations should apply, in situations where carriers use third parties to collect, store, host or analyze data collected via mobile devices.

This request for comments provides an opportunity for service providers and mobile device manufacturers to weigh in on data collection generally, and on the importance of monitoring activities in an age of growing network congestion. Additionally, given the regulatory compliance burden potentially associated with expanded CPNI requirements, it is important that mobile service providers take this opportunity to inform the FCC of their existing privacy and information security procedures.