Mobile privacy in the US

The US Federal Communications Commission's role in mobile privacy

Parties that submitted comments to a Federal Communications Commission Public Notice[1] on mobile privacy and security issues are deeply divided over whether the agency should pursue further action in the area.

As background, Section 222 of the Communications Act of 1934, as amended, imposes a duty on all 'telecommunications carriers' to protect customer proprietary network information (CPNI)[2]. CPNI is defined as '(A) 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; and (B) information contained in the bills pertaining to [a] telephone exchange service or telephone toll service received by a customer of a carrier.'[3] Among other restrictions, carriers may use, disclose, or permit access to CPNI only in limited circumstances[4].

The FCC Public Notice sought comment on 'the privacy and data security practices of mobile wireless service providers with respect to customer information stored on their users' mobile communications devices, and the application of existing privacy and security requirements to that information.'[5] It also sought comment on how the practices of mobile wireless service providers have evolved since 2007 with respect to information stored on their customers' mobile communications devices[6]. The proceeding follows up on a report from the agency on location-based services, issued earlier this year[7]. It also references Carrier IQ's mobile diagnostics and usage software, and notes that much has changed in the industry during the last five years (the last time the FCC sought comment on these issues)[8].

Although public interest groups and industry commentators noted that the mobile wireless marketplace has changed dramatically in recent years, they disagreed as to whether those changes necessitate further FCC action. Public interest groups and privacy advocates generally called for the FCC to ramp up efforts to protect consumer privacy and data security, with some seeking new mobile regulations focused on wireless carrier activity. The Electronic Privacy Information Center suggested that the FCC require carriers to implement 'comprehensive privacy and security protections based on Fair Information Practices' and 'give consumers a range of choices about the collection and retention of consumer data before or at the time of collection.' The New America Foundation's Open Technology Institute added that last year's Carrier IQ events 'make it clear that [industry] efforts, if they are occurring, are inadequate to give consumers knowledge and control to ensure that their data is being protected.'

Wireless carriers and other commentators, on the other hand, argued that no further FCC action is needed. According to them, changes in the wireless marketplace have produced intense competition for mobile data services (including mobile device applications, 'apps') and an extremely decentralised data collection and use environment. They also encouraged the FCC to defer to current self-regulatory efforts, as well as the ongoing NTIA privacy multistakeholder process[9]. NTIA is seeking to develop voluntary, enforceable codes of conduct related to the transparency of mobile app privacy practices[10].

Industry commentators also pointed out the FCC's limited jurisdiction in this area and its inability to comprehensively address problems involving a wide range of parties in the mobile wireless ecosystem. They noted that the FCC's CPNI regulatory framework was developed for legacy voice telephone services in a pre-broadband era, while many of today's new wireless apps, services, and platforms are not subject to the CPNI protections. However, public interest groups responded that the FCC is the agency best suited to regulate CPNI and that it has explicit statutory authority to address mobile privacy and data security issues. Those groups also noted that the NTIA effort was just beginning and could be a lengthy endeavor, while the FCC could act to address consumer concerns expeditiously.

The Future of Privacy Forum, which has actively worked to focus attention on data collection issues raised by mobile apps and other mobile services, encouraged the FCC to work with stakeholders and help educate consumers and app developers about the importance of protecting personal information. The Federal Trade Commission commented in the proceeding, detailing its privacy experience and that it 'look[ed] forward to working with the FCC to ensure that [they] avoid duplicative actions in areas where . . . jurisdictions may be overlapping.'

Most observers believe that the FCC is unlikely to move forward on these issues in the near future, although some think it could be heading towards a set of proposed rules to update the CPNI framework.

Mark W. Brennan Associate
Hogan Lovells LLP, Washington D.C.
mark.brennan@hoganlovells.com

1. Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices, CC Docket No. 96-115, Public Notice, DA 12-818 (WCB WTB OGC rel. 25 May 2012) ('Notice').
2. 47 U.S.C. § 222. The FCC has extended the CPNI requirements to providers of interconnected Voice over Internet Protocol services. 47 C.F.R. § 64.2003(o).
3. 47 U.S.C. § 222(h)(1).
4. See 47 U.S.C. § 222; see also 47 C.F.R. §§ 64.2001-2011.
5. Notice at 1.
6. Ibid. at 4.
7. See Location-Based Services: An Overview of Opportunities and Other Considerations, Federal Communications Commission Staff Report, (rel. 25 May 2012).
8. Notice at 2-3.
9. See National Telecommunications & Information Administration, Privacy Multistakeholder Process: Mobile Application Transparency, at http://www.ntia.doc.gov/other-publication/2012/privacy-multistakeholder-process-mobile-application-transparency.
10. Ibid.