FCC clarifies CPNI obligations on mobile for wireless carriers

Declaratory Ruling confirms CPNI obligations

On 27 June 2013, the US Federal Communications Commission (FCC) adopted a Declaratory Ruling confirming that wireless carriers have an obligation to secure and protect customer proprietary network information (CPNI) collected and stored on mobile devices, if the CPNI is collected at the carrier's direction and the carrier has access to or control over the information[1]. The FCC's decision could have ripple effects throughout the mobile ecosystem.

What is CPNI?

The Communications Act of 1934, as amended, requires telecommunications service providers and interconnected voice-over-internet protocol (VoIP) providers to protect sensitive consumer information[2]. The most specific carrier obligations concern CPNI, which Section 222 of the Communications Act defines to include information about a customer's use of the service 'that is made available to the carrier by virtue of the carrier-customer relationship.' CPNI encompasses information such as calls placed, the frequency and duration of calls, services purchased, as well as any information that appears on a consumer's telephone bill.

What prompted the Declaratory Ruling?

Last year, the FCC discovered that certain network diagnostics software that carriers install on mobile devices could store and transmit CPNI. The FCC recognised that there was confusion regarding whether CPNI stored on mobile devices was subject to the CPNI protections under the Communications Act and the FCC's rules. The FCC also learned that some carrier-installed software may have contained security vulnerabilities that could result in the unauthorised access and disclosure of CPNI and other personal data stored on a mobile device. Acknowledging the confusion, the FCC clarified that wireless carriers are obligated to protect the privacy and security of CPNI that they can access or collect from mobile devices.

First, the FCC confirmed that information collected and stored on a customer's mobile device at the behest of the carrier can be CPNI. The FCC explained that carriers in some instances can and do exercise control over the wireless devices connected to their networks and determine: the type of CPNI the device will collect; how it will be stored; and when the information will be transmitted back to the carrier, all without the customer's knowledge or ability to change those parameters. Thus, this information is 'made available to the carrier by virtue of the customer-carrier relationship' and is therefore required to be protected under the Communications Act and the CPNI rules.

Second, the FCC affirmed that CPNI on a customer's device remains CPNI regardless of whether it has been transmitted to the carrier. Because the stored CPNI is still available to the carrier, the FCC found that carriers must protect such data.

Third, the Commission made clear that when information collected and stored on a customer's mobile device is not under the carrier's control, not intended to be transmitted to the carrier, or otherwise accessible by the carrier, it is not CPNI. Additionally, the FCC noted that information collected by user-installed third-party applications is not CPNI.

In clarifying these obligations, the FCC did not adopt or propose new rules governing CPNI. By requiring wireless carriers to provide the same security and protection to CPNI collected and stored on a customer's mobile device that they provide to other CPNI, the Commission reasoned that it was 'avoid[ing] a potential gap in consumer's privacy protections.'

The effect on the wider ecosystem

Equipment manufacturers & operating system developers

The FCC's ruling may indirectly lead equipment manufacturers and operating system developers to upgrade the security of their handsets and systems. For example, carriers may require equipment manufacturers and operating system developers to ensure that the devices and systems are not vulnerable to cyberattacks that could lead to unauthorised access of the CPNI. Manufacturers and developers may need to inquire about the software that carriers plan to load onto mobile devices and better understand how carrier-installed software will gather CPNI and interact with the devices.

App developers

The FCC noted that mobile customers often install third-party applications on their devices and that these apps may collect sensitive information. The Declaratory Ruling confirmed that wireless carriers are not liable for protecting customer information on mobile devices that is collected by third-party apps and also confirmed that third-party apps are beyond the scope of Section 222 and the FCC's CPNI rules. However, carriers may nonetheless find it prudent to partner with app developers to make certain that sensitive customer information that carriers cause to be stored on mobile devices is not made vulnerable by the installation of third-party apps. App developers may find it wise to consider how apps, operating systems, and carrier-installed software will interact; if such interaction creates security vulnerabilities; and whether additional security measures are necessary to protect CPNI.

Mark W. Brennan Associate
Phillip Berenbroick Associate
Hogan Lovells US LLP
mark.brennan@hoganlovells.com
phillip.berenbroick@hoganlovells.com

1. Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609, 9611 ¶ 7 (2013) ('CPNI Declaratory Ruling').
2. See 47 U.S.C. § 222.