FCC Seeks Comment on Privacy and Security of Information Stored on Mobile Phones and Other Devices

May 29, 2012

Days before tomorrow's Federal Trade Commission (FTC) Workshop on Mobile Disclosures, the FCC weighed in with a pair of releases on privacy and security issues raised by mobile devices. In the first item released on Friday, the FCC is seeking to refresh its record regarding the privacy and data security practices of mobile wireless service providers in light of recent disclosures concerning software developed by CarrierIQ. The FCC's Public Notice seeks to update the record in a five-year-old rulemaking proceeding addressing carrier obligations in connection with devices that function on their networks. In the second item released, the FCC released its staff report on location-based services (LBS). Consistent with the approach of the Administration and the FTC (as was discussed at our 4th Annual Privacy Seminar), the FCC focused on ways carriers can protect information from misuse or mishandling, transparency in carrier disclosures and maximizing consumer choice in the use of LBS.

Collectively, the releases demonstrate that the FCC will continue to work cooperatively with the FTC and the Administration (including the NTIA) to address privacy issues in the mobile market. The FCC appears to believe it has sufficient statutory authority to act on mobile and device privacy, with its emphasis being on its jurisdiction over carrier practices in connection with both services and devices.

Public Notice Seeking Comments. While the FCC has been active in protecting CPNI both from a rulemaking and enforcement perspective, it has not taken significant action on the policy/rulemaking front since its 2007 rule changes to address pretexting (pretending to be a customer or other authorized person to obtain access to that customer's private communication records). At that time, the FCC adopted a Further Notice of Proposed Rulemaking to address the obligations of mobile carriers to secure the privacy of customer information stored on mobile devices. At the time, most carriers indicated that consumers control the information residing on their devices. However, late last year several large wireless carriers responded to inquiries from Senator Al Franken and acknowledged using software embedded or pre-installed on wireless devices to collect information about the performance of the devices and the provider's network.

Although several large wireless carriers have stated that the information gathering is used to collect information about their networks from the perspective of users' devices, the FCC is concerned about whether consumers are given meaningful notice and choice with respect to the collection of this data. In the Public Notice, the FCC is seeking input from industry and consumers on a series of questions designed to refresh the record for the purpose of potentially issuing a declaratory ruling clarifying carriers' obligations with respect to information collected from and stored on mobile devices. The specific questions the FCC on which the FCC seeks comment include a set of broad questions that carry themes reflective of recent Administration and FTC activity with respect to

mobile applications privacy. These themes, include transparency, notice and consent, data security, as well as "privacy by design". The FCC also asks for comment on how the following factors, if at all, impact a mobile carrier's obligations under the CPNI rules to protect the privacy of customer information:

- Whether the device is sold by the service provider;
- Whether the device is locked to the service provider's network;
- The degree of control that the service provider exercises over the software that collects or stores information from the device;
- The service provider's role in connection with the device's operating system, pre-installed software or security capabilities;
- The manner in which the information is used;
- Whether the information pertains to voice service, data service, or both; and
- The role of third parties in collecting and storing data.

Comments will be due 30 days after publication in the Federal Register and replies will be due 15 days later.

FCC Staff Report on Location-Based Services. On Friday, the FCC also released its long-anticipated report on LBS. The Staff Report notes that the FCC has decades of experience in protecting consumer privacy, and that, as the expert agency on communications and broadband networks, the agency in conjunction with its federal partners in the Executive Branch and at other independent agencies, has an important role in protecting consumer privacy in the future. LBS offer many conveniences to consumers and are gaining in popularity. However, it cautions that LBS "have the inherent ability to create accurate snapshots of their users' activities that can contain very personal information." As such, the Staff Report expresses caution in the use and monitoring of LBS. It identifies the FCC's goals in monitoring LBS to be three-fold: ensuring that personal information is protected from misuse and mishandling, requiring providers to be transparent about their practices, and enabling consumer control and choice.

The Staff Report does not make any specific recommendations or propose best practices for carriers. Instead, it offers a useful overview of the FCC's role in privacy regulation and enforcement, the LBS market, the FCC's June 2011 Forum on LBS, and privacy issues for LBS, and provides commentary on issues it will be monitoring:

- **Consideration of Privacy Issues at Earliest Stages of Product Development**. What are the most effective means to ensure privacy considerations become an integral part of the product design and development process for all players in the LBS industry? What should consumers be told?
- **Security of data**. What are the rights, duties, and obligations of the parties that generate, aggregate, or hold LBS-related data to secure such data from unauthorized disclosure or access? Do they vary as a result of a party's relationship with the customer?
- **Timing and sufficiency of notice.** How much information should be pushed to consumers at different points in their interaction with an LBS, mobile, application or other provider and how should it be presented? Must the information be provided each time an application or service is

used? Should there always be an opt out?

- **Data Minimization.** Should parties be encouraged to collect the minimal amount of data technically required to provide a location-based service and retain that data for the minimum amount of time necessary?

The Staff Report concludes with the admonishment that the FCC may take action, “if privacy issues are not met as effectively and comprehensively as possible or within reasonable time frames.”