Can You Hear Me Now? Audio Snooping Triggers FTC Warning to Mobile App Developers

Alyssa Z. Hutnik

March 18, 2016

This week, a dozen mobile app developers received warning letters from the FTC concerning audio monitoring software used in their apps, but not clearly disclosed to consumers.

The app developers allegedly used software development kits created by a company called SilverPush. The warning letters explain that SilverPush makes a “Unique Audio Beacon” technology available for app developers, enabling the apps to “listen” for unique codes embedded into television or advertising content to determine what television shows or advertisements are playing nearby. The beacon is configured to access the device’s microphone to collect audio information, even while the app is not actively in use. Using this technology, SilverPush can generate a detailed log of the television or advertising content that the user views for targeted advertising and analytics.

The warning letters explain that, although there is no apparent functionality in the app that would require access to the mobile devices microphone, the app requires permission to access the microphone prior to install. Once the app is installed, no disclosures were provided about the audio beacon functionality – either contextually as part of the setup flow, in the privacy policy, or elsewhere.

The letters note that SilverPush has represented that its audio beacons are not currently embedded into any television programming aimed at U.S. households. Nonetheless, the FTC warning letters explain that, if the mobile app enables third parties to monitor television-viewing habits of U.S. consumers, and the app’s privacy policy or user interface states or implies otherwise, this could constitute a violation of Section 5 the FTC Act, which prohibits unfair and deceptive business practices.

Take Heed: after the FTC warns, enforcement for ignoring such warnings can come later for the same or similar practices. It is a good reminder to assess what consumers data is being collected by the business (and its mobile apps, websites, devices, etc.), and whether those practices are

sufficiently disclosed. The more surprising (or personal) the data collection, the more obligation that can mean for the company to effect clear disclosures in a timely manner.