Street View Privacy Wiretap Case Against Google May Proceed

In a win for privacy rights and a setback for Google, the Ninth Circuit agreed that unencrypted Wi-Fi is protected from outside snooping under the federal Wiretap Act.

When Google sent vehicles out to take pictures for its Street View search feature, the vehicles not only captured the street images but also captured data from unencrypted Wi-Fi networks in nearby homes and businesses. This information included network names, SSID, MAC addresses, and payload data, such as personal emails, passwords, videos, and documents. Google later apologized for the data collection.

Several individuals sued Google and are seeking class certification. Google sought to dismiss the Wiretap Act claim arguing that Wi-Fi for a computer network is not subject to the Wiretap Act because the Wi-Fi transmission falls under an exception allowing access to radio or electronic communications that are readily accessible to the general public. The trial court denied Google's motion to dismiss but agreed to certify the question to the appellate court.

The appellate court disagreed with Google's argument that the Wi-Fi data it captured was except from the Act as an electronic communication readily accessible to the general public. The court found that "payload transmitted over an unencrypted Wi-Fi network is not 'readily accessible to the general public' under the ordinary meaning of the phrase."

The court reasoned that Wi-Fi transmissions are not readily available because "they are geographically limited and fail to travel far beyond the walls of the home or office where the access point is located. Google was able to intercept the plaintiffs' communications because its Street View vehicles passed by on the street outside of each plaintiff's house. In addition, the data is accessible only "with some difficulty. Unlike traditional radio broadcasts, a Wi-Fi access point cannot associate or communicate with a wireless device until it has been authenticated." To capture the information requires expertise to intercept and decode the payload data transmitted, a skill "the general public lacks."

Google additionally argued that the Wi-Fi transmissions met the definition of being a "radio communication" open to the general public because the term "radio communication" encompasses all radio wave technologies, including Wi-Fi. Again the appellate court disagreed, finding "Google's proposed definition is in tension with how congress—and virtually everyone else—uses the phrase. In common parlance, watching a television show does not entail 'radio communication.' Nor does sending an email or viewing a bank statement while connected to a Wi-Fi network."

If Google's definition that unencrypted Wi-Fi is readily accessible to the general public, then the law would condone intrusive and unwarranted invasions of privacy.

"Consider an email attachment containing sensitive personal information sent from a secure Wi-Fi network to a doctor, lawyer, accountant, priest, or spouse. A company like Google that intercepts the contents from the encrypted home network has, quite understandably, violated the Wiretap Act. But the sender of the email is in no position to ensure that the recipient—be it a doctor, lawyer, accountant, priest, or spouse—has taken care to encrypt her own Wi-Fi network. Google, or anyone else, could park outside of the recipient's home or office with a packet sniffer while she downloaded the attachment and intercept its contents because the sender's 'radio communication' is 'readily accessible to the general public' solely by virtue of the fact that the recipient's Wi-Fi network is not encrypted. Surely, Congress did not intend to condone such an intrusive and unwarranted invasion of privacy when it enacted the Wiretap Act 'to protect against the unauthorized interception of electronic communications,'" the appellate court wrote.

Joffe v. Google, Inc., Ninth Cir. No. 11-17483, issued September 10, 2013.