

OPINION

Absurdity in Outdated Technology Legislation

Courts hearing the Google Maps case face a 'square peg' situation all too common today.

Steve Thomas, The National Law Journal

May 26, 2014

Despite more than a century of history, "radio communication" now has a new definition in the U.S. Court of Appeals for the Ninth Circuit, and Google Inc. is asking the U.S. Supreme Court to strike it down. Google says the new definition criminalizes watching television, while the Ninth Circuit concluded that Google's read of the law would convert the federal Wiretap Act into a license to steal people's private communications.

The case illustrates the analytical contortions involved in applying old laws to new technologies. Here, the "old" law is a 1986 amendment to the Wiretap Act enacted specifically to address the new technologies of the day, which now already are antiquated. Left standing, the Ninth Circuit's ruling would wreak havoc in the information technology and communications industries, with devastating ripple effects throughout our economy.

The Supreme Court should — must — grant certiorari, reverse the Ninth Circuit, affirm the district court, and send the parties back to bicker over discovery. Meanwhile, Congress should hire some tech-savvy aides and rewrite the Wiretap Act immediately.

Google v. Joffe revolves around Google's "Street View" service, which allows users to look up an address on Google Maps and see a "street-view" picture of that location. Camera-equipped Google vehicles captured the images while driving on public roads.

But from 2007 to 2010, the Google vehicles also were equipped with Wi-Fi antennas and software that collected data transmitted by Wi-Fi networks in nearby homes and businesses, including network name and the router's unique address number. Google needed that basic information — which can be captured from any nearby wireless network, encrypted or not — to pinpoint the network on the map so it could tell online users about nearby pizza parlors and nail salons.

But if the network was not encrypted, Google went further, gathering "payload data," which could include virtually anything transmitted over the network as the vehicle passed by — personal emails, videos, documents and even user names and passwords. During the four years, Google collected more than 600 gigabytes of information in more than 30 countries.

In 2010, Google acknowledged gathering such data, publicly apologized and rendered inaccessible the personal data it had captured. Class actions sprang up across the country and were consolidated into multidistrict litigation styled *In re Google Inc. Street View Electronic Communications Litigation*, in the U.S. District Court for the Northern District of California. The plaintiffs said Google had intercepted electronic communications in violation of the federal Wiretap Act, as amended by the Electronic Communication Privacy Act of 1986. It's a criminal statute, but it also provides for a private action for damages such as the Google class action.

Google acknowledged intercepting electronic communications, but not every interception is unlawful. A car radio "intercepts" the broadcast of the local radio station, and the definition of "electronic communication" under the statute includes any transfer of sounds by "radio," so technically listening to a radio station is a violation of the statute. But the Wiretap Act has exemptions, including one for communications "readily accessible to the general public." The statutory definitions limit that phrase to "radio communications" that are not "scrambled or encrypted." That's why listening to radio is not a crime.

And that was Google's primary argument on appeal: The "radio" spectrum includes Wi-Fi, so any Wi-Fi network that is not encrypted is a "radio communication" that is "readily accessible to the general public" and therefore exempted under the statute.

The Ninth Circuit implicitly recognized that if Google succeeded on that argument, every unencrypted Wi-Fi network in the country would become fair game. Hacking tools available free online make it easy even for users with limited technical know-how to capture information from other users of unencrypted wireless networks — emails, documents, contacts, photos and even credit card information or log-in credentials. At the same time, savvy users who avoid unencrypted networks would not be immune because they might unwittingly send information to someone using an unencrypted network on the receiving end.

The Ninth Circuit appeared determined to avoid that result. In *Joffe v. Google Inc.*, it recognized last year that the case involved "a novel question of statutory interpretation" and went on to define "radio communication" as "a predominantly auditory broadcast."

Since Wi-Fi payload data are not "predominantly auditory," the court held that they are not "radio communication" for purposes of the statutory exemption. The court said its definition better reflected the intent of the enacting Congress in 1986. "It seems doubtful that Congress wanted to emphasize that Google or anyone else could park outside of a police station that carelessly failed to secure its Wi-Fi network and intercept confidential data with impunity."

But in its petition to the Supreme Court, Google argued that the Ninth Circuit's definition would cause "mischief" in the real world.

Google said that interception of satellite transmissions and television broadcasts are lawful only as a result of the "radio communication" exception, which the Ninth Circuit's new definition would exclude because they are not "primarily auditory." Google concluded: "Surely Congress did not intend to criminalize watching television."

If the Supreme Court does not take up the case, only time will show the net effects of the Ninth Circuit's new definition.

Steve Thomas is a shareholder at Dallas-based McGuire, Craddock & Strother.