

New Jersey Law Journal

VOL. 208 - NO 4

APRIL 23, 2012

ESTABLISHED 1878

COMMENTARY

Ban the 'Tiny Constable' From Our Cell Phones

BY GRAYSON BARBER

Most Americans expect their telephone conversations to be confidential, and they know the police need a warrant for wiretapping. Most Americans expect similar privacy for their cell phones, not knowing that law enforcement officials have started to use cell phones as convenient tracking devices.

Little would they imagine how much cell phone data is being harvested for countless purposes unrelated to their phone calls.

In *U.S. v. Jones*, where the U.S. Supreme Court held use of a GPS tracking device to be a Fourth Amendment search, Justice Samuel Alito offered the colorful metaphor of a tracking device as a "tiny constable" in a gigantic carriage.

The tiny constable can slip into the cell phone in your pocket now, and sidle up to the data aggregators who are tracking cell phones too, madly surveilling smart phone address books and photos, as well as geographic location, without the owners' knowledge or consent.

Most people have no idea how much information gets extracted from

Barber, a solo in Princeton, concentrates on privacy issues. She filed an amicus brief with the New Jersey Supreme Court in Earls on behalf of the Electronic Privacy Information Center, urging the justices to uphold Fourth Amendment protections for cell phone users.

their phones. On April 2, *The New York Times* reported that an unencrypted file on Apple's iPhone stored a 10-month record of a user's location data. In response, members of Congress and the media criticized Apple.

The Wall Street Journal has documented disclosures of detailed information from smart phones, including age, gender and geolocation, for purposes of tracking and predicting behavior. During the 2011 holiday season, a number of shopping malls decided to track shoppers from store to store. Some cell phones can locate a person to within 50 feet.

The data aggregators will say that if you want privacy, you shouldn't use a cell phone. Some in law enforcement might agree, but to do so raises a constitutional problem, because we are supposed to enjoy a government of limited power. Cell phone users do not want to disclose their location to app developers, much less to the police.

A study released this month by Consumers Union found widespread concern about online privacy. The survey found that 71 percent of consumers are "very concerned" about companies selling or sharing information about them. They don't want advertisers targeting kids with personalized ads, and they don't want online data to be used to prevent someone from getting a job or a loan.

The New Jersey Supreme Court is currently considering *State v. Earls*, 420 N.J. Super. 583 (App. Div. 2011), cert.

granted, 209 N.J. 97 (2011). At issue are the validity of the defendant's arrest, based on law enforcement's use of information from his cell phone provider about the phone's general location, and application of the plain view exception to the warrant requirement. The Appellate Division had held that an individual has no legitimate expectation of privacy in the location of his cell phone.

In 2001, the U.S. Supreme Court asked "what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy." In that case, *Kyllo v. United States*, the Court ruled that the use of a thermal imaging device was presumptively unreasonable without a warrant, noting that the device was "not in general public use." Cell phones, by contrast, are in general public use — and vigorously exploited by commercial entities as well as law enforcement.

Better guidance comes from *Katz v. United States*, the 1967 case that established the warrant requirement for telephones. Prior to *Katz*, the Supreme Court had ruled that a telephone user voluntarily projected his voice outside the room in which he was making the phone call. It took years before phones became an ordinary part of daily life, changing from a technological marvel to part of normal existence into which the government could not intrude without a very good reason.

The same thing has happened with cell phones. They have made the transition from novelty to commonplace, and are now used to call the doctor, the bank, the kids, etc. These are communications essential to the intimate and quotidian lives of ordinary people, into which a government of limited power should not be permitted to intrude

absent justification.

To most people, their cell phone is an intimate accessory, carried on their person at all times, and considered vital for work, school, and everyday social life. The device

is always on and always connected. They have become a primary means of communication, often replacing land lines.

It is not reasonable to impute knowledge to cell phone owners. They think the

device in their pocket is a phone, and reasonably expect to use it without intrusive governmental or commercial surveillance. People should be able to use cell phones without giving up their privacy. ■