

Your Phone is a Pocket Rat

A federal appeals court approves warrantless cellphone tracking, which the NSA may already be doing.

By: Jacob Sullum – August 7, 2013

Last month the New Jersey Supreme Court ruled that police generally need a warrant to obtain information about the locations of cellphone users. Last week the U.S. Court of Appeals for the 5th Circuit said just the opposite.

The first decision was based on Article I, Paragraph 7 of the New Jersey Constitution, while the second was based on the Fourth Amendment to the U.S. Constitution. But those provisions are virtually identical, banning "unreasonable searches and seizures" of "persons, houses, papers, and effects." The crucial difference between the two decisions is the "third party doctrine," an increasingly alarming menace to privacy.

Since the early 1970s, the U.S. Supreme Court has repeatedly declared that people have no constitutional right to privacy with respect to information they voluntarily share with others. New Jersey's courts have always rejected this principle, recognizing that people who disclose information for particular purposes do not thereby surrender all expectations of privacy.

A unanimous New Jersey Supreme Court therefore had no difficulty concluding that the government may not demand cellphone location data at will. "Disclosure of cell-phone location information, which cell-phone users must provide to receive service, can reveal a great deal of personal information about an individual," the court noted. "Yet people do not buy cell phones to serve as tracking devices or reasonably expect them to be used by the government in that way."

The 5th Circuit, by contrast, said people should know by now that connecting their wireless phone calls entails transmitting their locations to their service providers. Since no one is forced to use a cellphone, it reasoned, anyone who chooses to do so is voluntarily disclosing his whereabouts to a third party, thereby losing any reasonable expectation of privacy in that information.

"Cell site data are business records and should be analyzed under that line of Supreme Court precedent," the appeals court said, meaning they receive only as much protection as legislatures give them. While the case involved requests for two months of specific customers' location data, the court's logic would also apply to less discriminating investigations.

Suppose the National Security Agency (NSA), in addition to collecting information about the destinations, timing, and length of our calls, decided to amass a comprehensive database showing everywhere we go with our cellphones. It may be doing something like that already.

In a July 23 speech, Sen. Ron Wyden (D-Ore.), a member of the Senate Intelligence Committee who is constrained by secrecy rules from explicitly discussing classified surveillance programs,

repeatedly hinted that we have not yet learned the full extent of the NSA's domestic snooping. As Cato Institute privacy specialist Julian Sanchez noted, Wyden also mentioned the perils of cellphone tracking no fewer than five times, which would be puzzling unless it had something to do with the subject of his speech, NSA surveillance.

"Government officials are openly telling the press that they have the authority to effectively turn Americans' smart phones and cell phones into location-enabled homing beacons," Wyden said, adding that "the case law is unsettled." That warning takes on added gravity in light of the 5th Circuit's decision, the first by a federal appeals court to squarely address the issue.

The 5th Circuit's ruling sits uneasily with *U.S. v. Jones*, the 2012 decision in which the Supreme Court said police need a warrant to track a car by attaching a GPS device to it. Although the majority opinion hinged on the physical intrusion required to install the device, five justices expressed the view that the breadth of information generated by tracking someone's car for a month was enough to trigger Fourth Amendment protection. Two months of cellphone location data provide an even more intimate view of a person's private life.

Concurring in *Jones*, Justice Sonia Sotomayor argued that the Court should reconsider the third party doctrine in light of all the sensitive information that is nowadays stored outside of people's homes. Her suggestion is looking wiser by the day.