



Ninth Circuit: Government Can Access Third Party Records

By Jim Harper on 08/10/2012

Twice in the last month, the Ninth Circuit Court of Appeals has affirmed that the government can access records about you held by third parties without getting a warrant. It's a nice illustration of the broad and deep reach of the "third party doctrine."

U.S. v. Golden Valley Electric Association is the more recent of the two. In that case, the government delivered an administrative subpoena to a member-owned electricity cooperative asking for quite a bit of information about three residences it served:

"customer information including full name, address, telephone number, and any account information for customer; method of payment (credit card, debit card, cash, check) with card number and account information; to include power consumption records and date(s) service was initiated and terminated for the period 10-01-2009 through 12-14-2010..."

Golden Valley resisted the subpoena on a number of bases, including by arguing that criminal investigations require a warrant.

The court rejected the Fourth Amendment argument because the customer of a business like Golden Valley "lacks 'a reasonable expectation of privacy in an item,' like a business record, 'in which he has no possessory or ownership interest.'" That's the third-party doctrine: The government can access your electricity usage records and billing information without implicating the Fourth Amendment.

In mid-July, a different panel of the Ninth Circuit concluded the same thing about hotel records.

Los Angeles Municipal Code section 41.49 requires hotel operators to maintain information about their guests,

“including name and address; total number of guests; make, type and license number of the guest’s vehicle if parked on hotel premises; date and time of arrival; scheduled date of departure; room number; rate charged and collected; method of payment; and the name of the hotel employee who checked the guest in.”

These records must be held for 90 days and made available for inspection by any officers of the Los Angeles Police Department.

The owners of motels in Los Angeles challenged the law as a facial violation of the Fourth Amendment. The court rejected that argument, finding that the information the ordinance makes available to law enforcement “does not, on its face, appear confidential or ‘private’ from the perspective of the hotel operator.” For their part, hotel guests do not have a “reasonable expectation of privacy in guest registry information once they have provided it to the hotel operator.”

This is another unremarkable application of the third party doctrine, which says that people do not have Fourth Amendment rights against unreasonable search and seizure with respect to information they have shared with others.

Last January, in her concurrence to the Supreme Court’s ruling in *U.S. v. Jones*, Justice Sotomayor questioned the “third party doctrine” (as Justice Alito had done during oral argument).

“[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.”

It is not a slam dunk that utility and hotel records should be Fourth-Amendment protected, requiring probable cause and a warrant before law enforcement can access them. But if electric providers and hoteliers maintain information in confidence due to contractual or regulatory obligations, that should extend the protection of the Fourth Amendment to what I think of as the digital effects

created by modern living. This is not so much because of the sensitivities around electricity use or lodging, but because this is the rule we need to secure the much more sensitive data we routinely share and store with third parties online.

—

This article, originally published at Cato at Liberty by Jim Harper, is reprinted with permission from the Cato Institute.