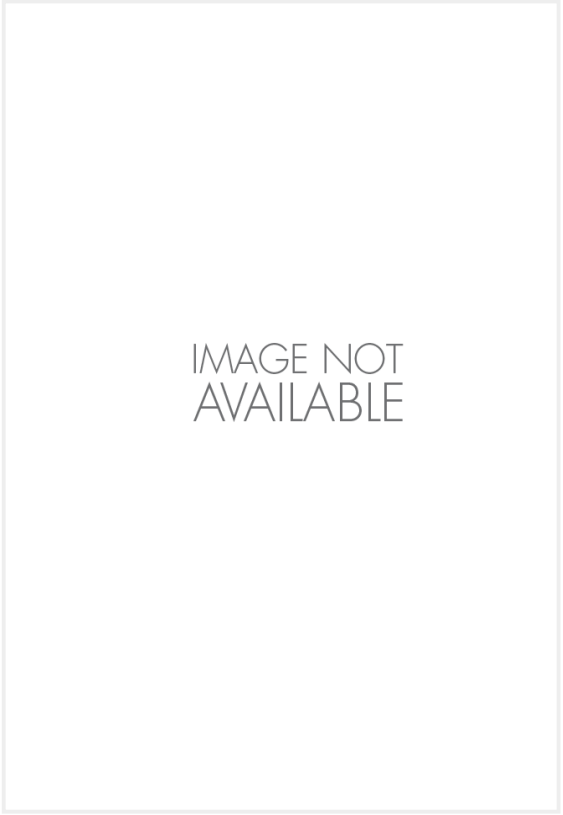
iWitness

THERMOSTATS THAT TESTIFY—WHO KNEW?



FRANK SOMMERS

The author is with Sommers & Schwartz, San Francisco.

Instead of the usual carping about how we've lost all our privacy, let's talk about all of the new data available to the knowledgeable litigator in discovery as a result of this very same loss. I'm going to limit it to data that allow you to physically track someone's whereabouts—an electronic private investigator, as it were.

First, let me paraphrase a newspaper item that caught my eye several years ago: A Contra Costa police detective moonlighting as a private investigator was found to have been offering his clients (women seeking a divorce) a service whereby he would tag the client's husband's car with a GPS locator system. As you might expect, the primary attraction of this service for the women was to enable them to catch their husbands at home with a mistress.

Is this fair game in private litigation? When the issue was presented to the U.S. Supreme Court in *United States v. Jones*, the Court held that police use of such a tracking device without a valid warrant violates the Fourth Amendment. *See* 132 S. Ct. 945, 949 (2012). For private litigants, however, such tactics are mostly unregulated, though several states, including New York and California, are moving to make it illegal. The general rule is, once your opponent is in public, he or she loses any reasonable expectation of privacy that might otherwise shield him or her from being observed in public. If you can physically follow someone, you can track that person electronically.

Sticking a GPS unit to someone's car, however, is by no means the only way to track its whereabouts and route. Many cities and police departments now use automatic license plate readers (ALPRs), which pick up every license plate on every car driving through designated areas, or even entire cities, and then run computer matches of those plates against, for example, lists of stolen cars. Police are also starting to install single units in police cars, and they merrily scan vehicles passed, then alert the officer when a match to a "vehicle of interest" comes up.

Private Litigants

The question is: Can you, as counsel for a private litigant, subpoena the police department for ALPR data associated with an opposing party's license plate number to determine that party's whereabouts during a given period?

So far, the answer seems to be no. In a recent case in Los Angeles, the Electronic Frontier Foundation (EFF) requested a week's worth of the Los Angeles Police Department's ALPR data, only to be met by the department's objection that such a release would "compromise ongoing investigations." *See* Jason Henry, *Public Cannot See Extensive License Plate Database Kept by LAPD, LASD, Judge Rules*, San Gabriel Valley Trib., Aug. 28, 2014, www.sgvtribune.com/

Illustration by Lisa Haney

Published in *Litigation*, Volume 41, Number 3, Spring 2015.

government-and-politics/20140828/public-cannot-see-extensive-license-plate-database-kept-by-lapd-lasd-judge-rules. Despite the department's admission that it was collecting three million plates a week from everybody who drove along certain streets in the city—meaning there was no possibility they were investigating them all—the trial judge upheld the objection. EFF is appealing. A New York reporter's request for his own license plate "hits" was met with the same objection, though police admitted there was no pending investigation of the reporter. Both decisions have been criticized as illogical, given the scope of the data capture, and courts may ultimately find that these records are subject to state open-records law requests.

Don't give up—there's more. Every car sold in this country after 2000 contains an event data recorder (EDR) that monitors several vehicle parameters, not unlike an airplane's black box. Unlike ALPR records, EDR data are protected by statute in a rising number of states.

A motion to compel production of someone's thermostat might be fun.

Almost every one of those laws, however, has an exception for court orders, making it possible for the tenacious litigant to secure the information by subpoena. To date, however, there's an additional hurdle: Many car companies contend that the software and coding system used to record the data on the EDR (and hence decode it) are proprietary. They refuse to translate the data on the ground that it would constitute a violation of their trade secrets. In addition, like aircraft black boxes, EDRs overwrite the data after a certain period, limiting the recoverable information.

There are also radiofrequency identification (RFID) transponders, most commonly encountered in your FastPass or E-ZPass toll payment device. While you might assume these contain little in the line of data because, after all, there only so many bridges to cross, that's not the case. Most states now use RFID scanners in roadside units to monitor traffic flow. Depending on your state, the data may be stored and retrievable by subpoena from your local department of transportation.

Telephone Data

No discussion of public space monitoring is complete without reference to your telephone. All semi-new phones are equipped with GPS locator chips. Until 2013, they were turned on automatically and kept broadcasting your location unless and until you turned them off. New phones should default to the "GPS off" setting. While the GPS data stored in your individual phone can provide an extraordinarily precise description of your whereabouts, there is only a limited amount of GPS data stored in the phone, as is true of EDR data.

Much more wide-ranging are the telephone company's location data, derived from your phone's constant "pinging" of nearby cell towers as you move around. Short of taking the battery out of your phone (which Osama bin Laden insisted his couriers do), this activity cannot be turned off because it is needed for the phone to function. While Edward Snowden's revelations have made us all much more familiar with the fact that these data are being collected (and provided in bulk to the government), little law exists on the question of whether a private litigant could subpoena the location data associated with a telephone in much the same manner as the numbers called are readily available in litigation. Provided you have the ability to show that such information meets the relatively low threshold for discovery, courts could presumably order its production.

Unlike telephone numbers called, however, cell tower location data are highly technical and would require access to the telephone company's analysis software before locations could be derived from the raw data. Who knows whether a court would be able or willing to order a service provider to translate its cell tower data into locations on a map. I'm sure you'll have fun trying, though.

Then there are the ubiquitous security cameras. We don't live in London, where they cover every square foot, but you would still be surprised how much public space here is also captured by private businesses' wall-mounted cams. This information is available through subpoena and open to discovery based on the "no reasonable expectation of privacy" argument. The problem is the "overwrite" issue mentioned above. By the time you figure out that a given location is of interest, the cameras have likely overwritten the good stuff because they can't store data beyond what they record over the course of three to seven days or so. Relevant witnesses should be interviewed as soon as possible to mine this source of data before it's too late.

Finally, just for grins, there's the new and ever-proliferating field of home sensors. These are exemplified by the Nest thermostat, made by a company recently bought by Google. That device captures, among other things, the presence of someone in the house or even a specific room, creating a record of the times of occupancy. Similarly, home monitoring apps on someone's iPhone can also provide records of a person's location. A motion to compel production of someone's thermostat might be fun, right? Good luck in this brave new world of discovery options. ■