BUSINESS INSIDER

2011 CATO Article Nails The Stipulations For NSA Data Tracking

By Julian Sanchez – July 23rd, 2013

Barack Obama's AutoPen has signed another four-year extension of three Patriot Act powers, but one silver lining of this week's lopsided battle over the law is that mainstream papers like *The New York Times* have finally started to take note of the growing number of senators who have raised an alarm over a "secret interpretation" of Patriot's "business records" authority (aka Section 215).

It would appear to be linked to a "sensitive collection program" referenced by a Justice Department official at hearings during the previous reauthorization debate—one that would be disrupted if 215 orders were restricted to the records of suspected terrorists, their associates, or their "activities" (e.g., large purchases of chemicals used to make bombs). Naturally, lots of people are starting to wonder just what this program, and the secret interpretation of the law that may be associated with it, are all about.

All we can do is speculate, of course: only a handful of legislators and people with top-secret clearances know for sure.

But a few of us who closely monitor national security and surveillance issues have come to the same conclusion: it probably involves some form of cellular phone geolocation tracking, potentially on a large scale. The evidence for this is necessarily circumstantial, but I think it's fairly persuasive when you add it all up.

First, a bit of background. The recent fiery floor speeches from Sens. Wyden and Udall are the first time widespread attention has been drawn to this issue—but it was actually first broached over a year ago, by Sen. Richard Durbin and then-Sen. Russ Feingold, as I point out in my new paper on Patriot surveillance.

Back in 2005, language that would have required Section 215 business record orders to pertain to terror suspects, or their associates, or the "activities" of a terror group won the unanimous support of the Senate Judiciary Committee, though was not ultimately included in the final reauthorization bill.

Four years later, however, the Justice Department was warning that such a requirement would interfere with that "sensitive collection program." As Durbin complained at the time:

The real reason for resisting this obvious, common-sense modification of Section 215 is unfortunately cloaked in secrecy. Some day that cloak will be lifted, and future generations will

ask whether our actions today meet the test of a democratic society: transparency, accountability, and fidelity to the rule of law and our Constitution.

Those are three pretty broad categories of information—and it should raise a few eyebrows to learn that the Justice Department believes it routinely needs to get information outside its scope for counterterror investigations. Currently, any record asserted to be "relevant" to an investigation (a standard so low it's barely a standard) is subject to Section 215, and records falling within those three categories enjoy a "presumption of relevance."

That means the judges on the secret Foreign Intelligence Surveillance Court lack discretion to evaluate for themselves whether such records are really relevant to an investigation; they must *presume* their relevance. With that in mind, consider that the most recent report to Congress on the use of these powers shows a record 96 uses of Section 215 in 2010, up from 22 the previous year. Perhaps most surprisingly though, the FISC saw fit to "modify" (which almost certainly means "narrow the scope of") 42 of those orders.

Since the court's discretion is limited with respect to records of suspected terrorists and their associates, it seems probable that those "modifications" involved applications for orders that sweep more broadly. But why would such records be needed? Hold that thought.

Fast forward to this week. We hear Sen. Wyden warning that "When the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry," a warning echoed by Sen. Udall.

We know that this surprising and disturbing interpretation concerns one of the three provisions that had been slated for sunset. Lone Wolf remains unused, so that's out, leaving roving wiretaps and Section 215. In the context of remarks by Sens. Feingold and Durbin, and the emphasis recently placed on concerns about Section 215 by Sen. Udall, the business records provision seems like a safe bet.

By its explicit terms, that authority is already quite broad: What strained secret interpretation of it could be surprising to both legislators and the general public, but also meet with the approval of the FISC and the Office of Legal Counsel?

For one possible answer, look to the criminal context, where the Department of Justice has developed a novel legal theory, known as the "hybrid theory," according to which law enforcement may do some types of geolocation tracking of suspects' cellular phones without obtaining a full-blown probable cause warrant.

The "hybrid theory" involves fusing two very different types of surveillance authority. "Pen registers" allow the monitoring, in real time, of the communications "metadata" from phones or other communications devices (phone numbers dialed, IP addresses connected to).

For cellular phones, that "metadata" would often make it possible to pinpoint at least approximately—and, increasingly, with a good deal of precision, especially in urban areas—the location of the user. Federal law, however, prohibits carriers from disclosing location information "solely" pursuant to a pen register order. Another type of authority, known as a 2703(d) order, is a bit like Patriot's business records authority (though only for telecommunications providers), and is used to compel the production of historical (as opposed to real-time/prospective) records, without any exclusion on location information.

The Justice Department's novel theory—which I discussed at a recent Cato event with Sen. Wyden on geolocation tracking—is that by *bundling* these two authorities in a new kind of combination order, they can do real-time geolocation tracking without the need to obtain a full Fourth Amendment warrant based on probable cause.

Many courts have been skeptical of this theory and rejected it—but at least some have gone along with this clever bit of legal origami. Using the broad business records power of Patriot's Section 215 in a similar way, to enable physical tracking of anyone with a cellphone, would seem to fit the bill, then: certainly surprising and counterintuitive, not what most people think of when we talk about "obtaining business records," but nevertheless a maneuver with a legal track record of convincing some courts.

Now, consider that Sen. Wyden has also recently developed a concern with the practice of mobile location tracking, which has become so popular that the U.S. Marshall Service, now the federal government's most prolific (known) user of pen register orders, of which it issued over 6,000 last year, employs the "hybrid theory" to obtain location information *by default* with each such order.

Wyden has introduced legislation that would establish standards for mobile location tracking, which has two surprising and notable feature. First, while the location tracking known to the public all involves criminal investigations subject to the Electronic Communications Privacy Act (ECPA), that's not where Wyden's bill makes its primary modifications.

Instead, the key amendments are made directly to the Foreign Intelligence Surveillance Act—which language is then incorporated by reference into ECPA. Second, even though one section establishes the "exclusive means" for geolocation tracking, the proposal goes out of its way to *additionally* modify the FISA pen register provision and the Section 215 business records provision to explicitly prohibit their use to obtain geolocation information—as though there is some special reason to worry about those provisions being used that way, requiring any possible ambiguity to be removed.

Sen. Udall, meanwhile, always uses the same two examples when he talks about his concerns regarding Section 215: he warns about "unfettered" government access to "business records ranging from a cell phone company's phone records to an individual's library history," even when the records relate to people with no connection to terrorism. The reference to libraries is no surprise, because the specter of Section 215 being used to probe people's reading habits was raised so insistently by librarians that it became common to see it referenced as the "library provision."

The other example is awfully specific though: he singles out cell phone records, even though many types of sensitive phone records can already be obtained *without* judicial oversight using National Security Letters. But he doesn't just say "phone records"—it's *cell* phone records he's especially concerned about. And where he talks about "an individual's" library records, he *doesn't*warn about access to "an individual's" cell phone records, but rather the *company's* records. As in, the lot of them.

Tracking the location of suspected terrorists, and perhaps their known associates, might not seem so objectionable—though one could argue whether Section 215's "relevance" standard was sufficient, or whether a full FISA electronic surveillance warrant (requiring a showing of probable cause) would be a more appropriate tool.

But that kind of targeted tracking would not require broad access to records of people *unconnected* to terror suspects and their known associates, which is hinted at by both Sen. Udall's remarks and the high rate of modifications imposed on Section 215 orders by the FISA court. Why might that be needed in the course of a geolocation tracking program?

For a possible answer, turn to the "LocInt" or "Location Intelligence" services marketed to U.S. law enforcement and national security clients by the firm TruePosition. Among the capabilities the company boasts for its software (drawn from both its site and a 2008 white paper the company sponsored) are:

● the ability to analyze location intelligence to detect suspicious behavioral patterns,
● the ability to mine historical mobile phone data to detect relationships between people, locations, and events,
● TruePosition LOCINT can mine location data to find out if the geoprofile of a prepaid phone matches the geoprofile of a potential threat and identify it as such, and
● leveraging location intelligence, officials can identify mobile phones of interest that frequently communicate with each other, or are within close proximity, making it easier to identify criminals and their associates. [Emphasis added.]

Certainly one can see how these functions might be useful: terrorists trained in counterintelligence tactics might seek to avoid surveillance, or identification of co-conspirators, by communicating only in person. Calling records would be useless for revealing physical meetings—but location records are another story. What these functions have in common, however, is that like any kind of data mining, they require access to a*large pool of data*, not just the records of a known suspect.

You can find out who your suspect is phoning by looking at *his* phone records. But if you want to know who he's in close physical proximity to—with unusual frequency, and most likely alone—you need to sift through *everyone's* phone location records, or at any rate a whole lot of them. The interesting thing is, it's not obvious there's any legal way to actually do all that: full-fledged electronic surveillance warrants would be a non-starter, since they require probable cause for each target.

But clearly the company expects to be able to sell these capabilities to *some*government entity. The obvious candidate is the FBI, availing itself of the broad authority of Section 215—perhaps in combination with FISA pen registers when the tracking needs to happen in real time.

As a final note of interest, the Office of the Inspector Generals' reports on National Security Letter contain numerous oblique references to "community of interest [REDACTED]" requests. Traditional "community of interest" analysis means looking at the pattern of communications of not just the primary suspect of an investigation, but their whole social circle—the people the suspect communicates with, and perhaps the people *they* in turn communicate with, and so on.

Apparently the fact that the FBI does this sort of traditional CoI analysis is not considered secret, because that phrase remains unredacted. What, then, could that single omitted word be? One candidate that would fit in the available space is "location" or "geolocation"—meaning *either* location tracking of people called by the suspect *or* perhaps the use of location records to build a suspect's "community of interest" by "identify[ing] mobile phones…within close proximity" to the suspects.

The Inspector General reports cover the first few years following passage of the Patriot Act, before an opinion from the Office of Legal Counsel held that NSLs could not properly be used to obtain the full range of communications metadata the FBI had been getting under them. If NSLs *had* been used for location-tracking information prior to that 2008 opinion, it would likely have been necessary to rely on Section 215 past that point, which would fit the timeline.

Is all of that conclusive? Of course not; again, this is speculation. But a lot of data points fit, and it would be quite surprising if the geolocation capabilities increasingly being called upon for criminal investigations were *not* being used for intelligence purposes. If they are, Section 215 is the natural mechanism.

Even if I'm completely wrong, however, the larger point remains: while intelligence*operations* must remain secret, a free and democratic society is not supposed to be governed by secret laws—and substantive judicial interpretations are no less a part of "the law" than the text of statutes.

Whatever power the government has arrogated to itself by an "innovative" interpretation of the Patriot Act, it should be up to a free citizenry to consider the case for it, determine whether it is so vital to security to justify the intrusion on privacy, and hold their representatives accountable accordingly. Instead, Congress has essential voted blind—reauthorizing powers that even legislators, let alone the public, do not truly understand. Whether it's location tracking or something else, this is fundamentally incompatible with the preconditions of both democracy and a free society.