IMPORTANT VICTORIES FOR THE FOURTH AMENDMENT MAY POSE BIG THREAT TO DRAGNET

Sorry for the absence of late. I've been traveling and working on outside deadlines. But I should be back in the saddle for the next little while.

During the period I've been traveling, there have been two significant victories for the Fourth Amendment at the Circuit level. On June 11, the 11th Circuit (covering Florida, Georgia, and Alabama) ruled you need a warrant for stored cell location data. Relying on a close analysis of the various opinions in US v. Jones (the SCOTUS GPS tracking case), it ruled cell transmissions should be even more private than GPS device collection of your car's movement, as your cell phone accompanies you to private places, which makes it more like communications content than observable location.

> One's car, when it is not garaged in a private place, is visible to the public, and it is only the aggregation of many instances of the public seeing it that make it particularly invasive of privacy to secure GPS evidence of its location. As the circuit and some justices reasoned, the car owner can reasonably expect that although his individual movements may be observed, there will not be a "tiny constable" hiding in his vehicle to maintain a log of his movements. 132 S. Ct. at 958 n.3 (Alito, J., concurring). In contrast, even on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted

> in a public way. One's cell phone, unlike an automobile, can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one. When one's whereabouts are not public, then one may have a reasonable expectation of privacy in those whereabouts. Therefore, while it may
> be the case that even in light of the Jones opinion, GPS location information on an automobile would be protected only in the case of aggregated data, even one point of cell site location data can be within a reasonable expectation of privacy. In that sense, cell site data is more like communications data than it is like GPS information.

It then relied on a Third Circuit decision finding cell phone users did not voluntarily provide their location to their cell providers, and therefore cell location cannot be governed by the Third Party doctrine, in which the government may obtain anything you've given willingly to a third party without a warrant.

The ruling, then, is the broadest possible support for requiring a warrant for cell location data.

The second ruling, issued yesterday by the 2nd Circuit (covering New York, Connecticut, and Vermont), found that the government cannot just retain all the data seized from your computer indefinitely, only to use it years later under a new warrant. Of particular interest are two counterarguments the court made to the government's claim that such a practice was reasonable.

First, it rejected the government's claim that obtaining a warrant for information obtained years earlier would be legal.

> Second, the Government asserts that by

> obtaining the 2006 search warrant, it cured any defect in its search of the wrongfully retained files. But this argument "reduces the Fourth Amendment to a form of words."
>
> [snip]
>
> If the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed probable cause, every warrant to search for particular electronic data would become, in essence, a general warrant.

And it rejected the government's complaints that destroying the information it seized would be impractical, therefore making the later use of that data permissible.

> Fourth, the Government contends that returning or destroying the non-responsive files is "entirely impractical" because doing so would compromise the remaining data that was responsive to the warrant, making it impossible to authenticate or use it in a criminal prosecution.
>
> [snip]
>
> But even if we assumed it were necessary to maintain a complete copy of the hard drive solely to authenticate evidence responsive to the original warrant, that does not provide a basis for using the mirror image for any other purpose.

These opinions are both momentous ones on their own, within the criminal context. But they also seriously threaten the NSA's dragnets – and perhaps even the proposed dragnet under USA Freedumber Act. Jennifer Granick explains why the 11th Circuit decision threatens the program.

> The appellate judges in Davis, by refusing to apply Smith and Miller to a

> case involving stored records, have taken a giant step toward undermining the legal justification propping up many of the government's targeted and bulk metadata collection practices. The call detail records that the NSA gets under its Section 215 collection program — which provide information about phone numbers called and received and the duration of calls — include far more detailed data than the simple information at issue in Smith and are far more revealing of private conduct, social networks, and thought processes. This is especially true because the records are collected in bulk.

Under the new program, the NSA will almost certain rely on stored cell location data in its chaining process. Unless the government can claim the analysis the telecoms do for the government somehow doesn't amount to a search, this location-chaining would seem to be illegal under this decision, for the states covered by the circuit.

And the 2nd Circuit decision undermines the argument the government uses to distinguish "collection" (as we would understand it) from the "collection" they claim to undertake when they later access information. More importantly, the government maintains (relying on a pre-computer Ted Olson opinion) that once it obtains information, it can do anything with it, up to conducting searches without even establishing Reasonable Suspicion. This opinion holds that such an argument amounts to a general warrant.

This ruling is particularly important for the government's back door searches, which it justifies based on that logic.

It's too early yet to see how this will affect the dragnet. The government could appeal both of these. The government could try to find a way around these jurisdictions — though New York and Florida are both so central to their claimed

primary counterterrorism purpose, I don’t see how they could do it. They could try to argue a national security exception to this rule, based on special needs.

But for the moment, the principles laid out in these decisions cut to the core of the NSA’s dragnet.