HJC'S USA F-REDUX REPORT NARROWS LANGUAGE ON CALL DETAIL RECORDS

As I've written extensively, for the last 15 months, the government, FISC, and Congress have been playing around with the definition of Call Detail Records under the USA F-ReDux and its predecessors. As written, I believe the CDR language in USA F-ReDux would permit the government to ask providers for analysis (of the sort provided by AT&T under Hemisphere) using things like location data, without turning over location data.

The House Judiciary Committee report includes language that would go a long way to prohibiting the kind of analysis I worry about, however.

> The government may require the production of up to two "hops"—i.e., the call detail records associated with the initial seed telephone number and call detail records (CDRs) associated with the CDRs identified in an initial "hop." Subparagraph (F)(iii) provides that the government can obtain the first set of CDRs using the specific selection term approved by the FISC. In addition, the government can use the FISC-approved specific selection term to identify CDRs from metadata it already lawfully possesses. Together, the CDRs produced by the phone companies and those identified independently by the government constitute the first "hop." Under subparagraph (F)(iv), the government can then present session identifying information or calling card numbers (which are components of a CDR, as defined in section 107) identified in the first "hop" CDRs to phone companies to serve as the basis for companies to

> return the second “hop” of CDRs. As with the first “hop,” a second “hop” cannot be based on, nor return, cell site or GPS location information. It also does not include an individual listed in a telephone contact list, or on a personal device that uses the same wireless router as the seed, or that has similar calling patterns as the seed. Nor does it exist merely because a personal device has been in the proximity of another personal device. These types of information are not maintained by telecommunications carriers in the normal course of business and, regardless, are prohibited under the definition of “call detail records.”
>
> “Call detail records” include “session identifying information (including originating or terminating telephone number, International Mobile Subscriber Identity number, or International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call.” The Act explicitly excludes from that term the contents of any communication; the name, address, or financial information of a subscriber or customer; and cell site location or GPS information, and the Act should not be construed to permit the government to obtain any of this type of information through either of the two “hops.”

Some comments on this.

First, nothing in this passage suggests these “phone companies” are exclusively telephony companies (that is, old style phone companies). Indeed, it even mentions wireless routers, suggesting they’re accounting for IP addresses. That’s to be expected; much less of our call traffic is carried by such providers. But people should be aware this likely includes Google and Microsoft and Apple “calls.”

The passage explicitly permits the government to also chain on "metadata it already lawfully possesses." Which means it will do the EO 12333 hops, while the providers do the 215 hop. Remember this will produce a largely duplicative production for international calls, with more metadata involved on the EO 12333. But there's no way to deal with that. (Note, assuming the CDRs will come back in through FBI, this means they'll probably get access to EO 12333 data out of this.)

The passage lists a lot of things I was worried about (in part, because we know the government has obtained similar information using both Hemisphere and its own EO 12333 analysis) that cannot be used for these hops, including:

- Cell site or GPS location information
- An individual listed in a telephone contact list
- An individual on a personal device that uses the same wireless router as the seed
- An individual that has similar calling patterns as the seed
- A personal device has been in the proximity of another personal device

This would seem to rule out most of my concerns (especially if "calling patterns" included the kind of counter-surveillance tactics that last week's Intercept story made clear NSA tracks). It would seem to permit chaining on "friends and family" members (but the FBI is getting those, from AT&T at least, using NSLs). And it doesn't address owners of the same account (suggesting the government could use one device to obtain other related devices tied to the same account — but that's the same person, which therefore seems totally justifiable).

Finally, note this language seems to confirm what I have understood: that the definition of CDR includes 5 components, only one of which must be met to be a CDR, meaning that the government can obtain nothing more than device identifying information. Again, I don't find that problematic. It's just something to pay attention to.

All of which to say that, if HPSCI and the House overall don't come out with any language that changes this (Mike Rogers introduced some funky language last year, which is when I first started get worried about this), then I would be fairly comfortable that any non-call chaining under this CDR function would be perfectly reasonable. Indeed, these definitions exclude ones — like matching similar calling patters — that I wouldn't be surprised if they retained. Moreover, last week's Second Circuit ruling would seem to require any other interpretations of this language to be public to count as binding.

So for now, at least, one of my significant concerns about USA F-ReDux is alleviated.

Update: Adding, this language seems to envision the possibility of using 215 to get location data later, which is something James Cole explicitly admitted was possible last year.

> This new authority—designed to allow the government to search telephone metadata for possible connections to international terrorism— does not preclude the government's use of standard business records orders under Section 501 to compel the production of business records, including call detail records.

Again, that's not surprising. But this report explicitly limits prospective call record chaining to the CDR function, so they could not get location under this authority prospectively (they'd probably use PRTT for that in any case).

Update: Now that I read the definitions section, I do have a few more reservations about how they can chain — and am all but certain this is intended to include Internet "calls." Here's that section.

> For purposes of the call detail record authority, the term ''specific selection term'' is defined as a term specifically identifying an individual, account, or personal device.
>
> The term ''address'' means a physical address or electronic address, such as an electronic mail address, temporarily assigned network address, or Internet protocol address. This definition may overlap with the term ''account,'' which also can be considered a ''specific selection term'' under the bill. These terms are not mutually exclusive, and an electronic mail address or account also qualifies as an ''account'' for purposes of the bill.
>
> The term ''personal device'' refers to a device that can reasonably be expected to be used by an individual or a group of individuals affiliated with one another. For example, ''personal device'' would include a telephone used by an individual, family, or housemates, a telephone or computer provided by an employer to an employee or employees, a home computer or tablet shared by a family or housemates, and a Wi-Fi access point that is exclusively available to the inhabitants of a home, the employees of a business, or members of an organization. It would also include a local area network server that is used by a business to provide e-mail to its employees. The term ''personal device'' does not include devices that are made available for use by the general public or by multiple people not affiliated with one other, such as a pay phone

> available to the public, a computer available to library patrons to access the Internet, or a Wi-Fi access point made available to all customers at an Internet cafe. Depending on the circumstances, however, such devices could qualify as ‘‘any other specific identifier’’ that is used to limit the scope of the tangible things sought consistent with the purpose for seeking the tangible things. The term ‘‘personal device’’ also does not include devices that are used by companies to direct public communications, such as a router used by an Internet service provider to route e-mails sent by its customers, or a switch used by a telecommunications carrier to route calls made by its customers.

First, this section goes out of its way to say CDR SST includes “account” which includes “email address or account.” This strongly suggests they intend to go to Google and get everything associated with, for example, the “account” emptywheel. Again, I’m not at all surprised about that. But it is worth noting.

The “personal device” description distinguishes the “individual on a personal device that uses the same wireless router as the seed,” which is prohibited for chaining under the bill, from an individual “on the same personal device” which may include a home (or even business’, which is something FBI has obtained using NSLs) WiFi access point. That is, it does seem like your roommates could be chained, but not those using the same Internet cafe as you.

But again, these are legitimate chains, in my opinion.