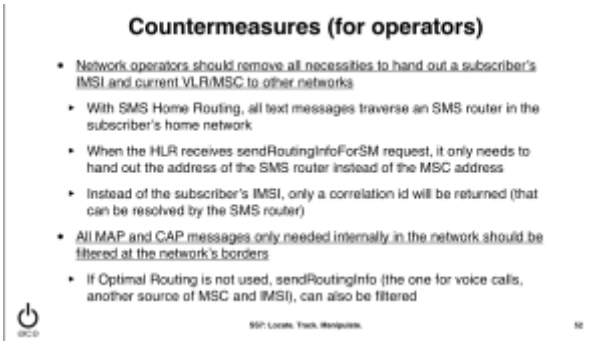
SS7 AND NSA'S REDUNDANT SPYING



On Sunday, 60 Minutes brought attention to an issue first exposed by researchers some years back: the ease with which people can use the SS7 system that facilitates global mobile phone interoperability to spy on you.

> Sharyn Alfonsi: If you just have somebody's phone number, what could you do?
>
> Karsten Nohl: Track their whereabouts, know where they go for work, which other people they meet when— You can spy on whom they call and what they say over the phone. And you can read their texts.

60 Minutes was smart in that they got Congressman Ted Lieu to agree to be targeted.

> Congressman Lieu didn't have to do anything to get attacked.
>
> All Karsten Nohl's team in Berlin needed to get into the congressman's phone was the number. Remember SS7 —that little-known global phone network we told you about earlier?
>
> Karsten Nohl: I've been tracking the congressman.
>
> [snip]Sharyn Alfonsi: Are you able to track his movements even if he moves the location services and turns that off?
>
> Karsten Nohl: Yes. The mobile network

> independent from the little GPS chip in your phone, knows where you are. So any choices that a congressman could've made, choosing a phone, choosing a pin number, installing or not installing certain apps, have no influence over what we are showing because this is targeting the mobile network. That of course, is not controlled by any one customer.
>
> [snip]
>
> Sharyn Alfonsi: What is your reaction to knowing that they were listening to all of your calls?
>
> Rep. Ted Lieu: I have two. First, it's really creepy. And second, it makes me angry.
>
> Sharyn Alfonsi: Makes you angry, why?
>
> Rep. Ted Lieu: They could hear any call of pretty much anyone who has a smartphone. It could be stock trades you want someone to execute. It could be calls with a bank.
>
> Karsten Nohl's team automatically logged the number of every phone that called Congressman Lieu — which means there's a lot more damage that could be done than just intercepting that one phone call.

So now Lieu is furious — and pushing House Oversight Committee to conduct an investigation into SS7's vulnerabilities.

Of course, it's probably best to think of SS7's vulnerabilities not as a "flaw," as 60 Minutes describes it, but a feature. The countries that collectively aren't demanding change are also using this vulnerability to spy on their subjects and adversaries.

But the fact that Lieu — who really is one of the smartest Members of Congress on surveillance issues — is only now copping onto

the vulnerabilities with SS7 suggests how stunted our debate over dragnet surveillance was and is. For two years, we debated how to shut down the Section 215 dragnet, which collected a set of phone records that was significantly redundant with what we collected "overseas" — though in fact the telecoms' production of such records was mixed together until 2009, suggesting for years Section 215 probably served primarily as legal cover, not the actual authorization for the collection method used. We had very credulous journalists talking about what a big gap in cell phone records NSA faced, in part because FISC frowned on letting NSA collect location data domestically. Yet all the while (as some smarter commenters here have said), NSA was surely exploiting SS7 to collect all the cell phone records it needed, including the location data. Members of Congress like Lieu — on neither the House Intelligence (which presumably has been briefed) or the House Judiciary Committees — would probably not get briefed on the degree to which our intelligence community thrives on using SS7's vulnerabilities.

What I find perhaps most interesting about this new flurry of attention on SS7 is that the researchers behind it were hired by some "international telecoms" to find ways to improve security sometime in advance of December 2014 (when they first presented their work). The original CCC presentation on this vulnerability (see after 40:00) included a general discussion of what cell phone providers could do to increase the security of their users (see above). 60 Minutes noted that some US providers were doing more than others.

The NSA presumably could and did use entirely SS7 collection for cell phones — especially US based ones — until such time as domestic providers started making them less accessible (and once they were unaccessible overseas, then subject to legal process, though even some of the countermeasures would still leave a US user exposed to other US providers). That needs to be

understood (should have been, before the passage of USA Freedom) to really understand the degree to which Congress has any influence over the NSA.