DIFI'S FAKE FISA FIX: THE ROAMER PRE-EMERGENCY EXIGENT EXCUSE TO BE USED ON INTERNET CONTENT

There's one more aspect of Dianne Feinstein's Fake FISA Fix bill that doesn't make any sense: it's proposed solution to the "roamer problem."

Roamers are, at least as the NSA's internal review explains them, when a foreign target with a GSM device (I think Keith Alexander has used the word "phone" when he describes this) — who may be targeted under either FISA Amendments Act or EO 12333 — travels into the US and NSA keeps tracking him, resulting in a violation because it means the NSA is wiretapping someone in the US without a warrant.

My sense is the NSA had tracked but never really cared about this GSM problem before Barton Gellman released an internal compliance report dating to May 2012 that revealed them. The NSA claimed to itself the problem was "largely unpreventable" (though it did commit to more research to understand it).

But now that it has been revealed as part of an eye-popping number of violations in 2011-12, NSA has proposed to fix it this way.

> (f)(1) Notwithstanding any other provision of this Act, acquisition of foreign intelligence information by targeting a non-United States person reasonably believed to be located outside the United States that was lawfully initiated by an element of the intelligence community may continue for a transitional period not to exceed 72 hours from the time when it is recognized that the non-United States person is reasonably believed to be

> located inside the United States and that the acquisition is subject to this title or title III of this Act, provided that the head of the element determines that there exists an exigent circumstance and—
>
> (A) there is reason to believe that the target of the acquisition has communicated or received or will communicate or receive foreign intelligence information relevant to the exigent circumstance; and
>
> (B) it is determined that a request for emergency authorization from the Attorney General in accordance with the terms of this Act is impracticable in light of the exigent circumstance.
>
> (2) The Director of National Intelligence or the head of an element of the intelligence community shall promptly notify the Attorney General of the decision to exercise the authority under this section and shall request emergency authorization from the Attorney General pursuant to this Act as soon as practicable, to the extent such request is warranted by the facts and circumstances.
>
> (3) Subject to subparagraph (4), the authority under this section to continue acquisition of foreign intelligence information is limited to 72 hours. However, if the Attorney General authorizes an emergency acquisition pursuant to this Act, then acquisition of foreign intelligence information may continue for the period of time that the Attorney General’s emergency authorization or any subsequent court order authorizing the acquisition remains in effect.
>
> (4) The authority to acquire foreign intelligence information under this

> subsection shall terminate upon any of the following, whichever occurs first
>
> (A) 72 hours have elapsed since the commencement of the transitional period;
>
> (B) the Attorney General has directed that the acquisition be terminated; or
>
> (C) the exigent circumstance is no longer reasonably believed to exist.
>
> (5) If the Attorney General authorizes an emergency authorization during the transitional period, the acquisition of foreign intelligence shall continue during any transition to, and consistent with, the Attorney General emergency authorization or court order.
>
> (6) Any information of or concerning unconsenting United States persons acquired during the transitional period may only be disseminated during the transitional period if necessary to investigate, prevent, reduce, or eliminate the exigent circumstance or if it indicates a threat of death or serious bodily harm to any person. [my emphasis]

Basically, what this does is provide NSA (or whatever other intelligence agency was collecting on this target) 3 days to continue collecting on a target when he comes into the US, in the name of exigent circumstances, in addition to the provision in FISA that permits the Attorney General to authorize emergency collection until authorization can be approved by the FISA Court, with a week to submit an application. If that collection lasts only for that 72-hour period, no paperwork will get submitted except for whatever notice the IC gives to the AG. The IC may immediately circulate US person information collected incidentally with the target's information in the name of the exigent circumstances, which doesn't even require the threat of death of

seriously bodily harm (which is probably secretly interpreted to mean threat to property anyway).

Exigent, then emergency, is the new watchword of the IC.

Or maybe the old one, given FBI's notorious abuse of the word "exigent" to track US person call records with almost no or no paperwork until 2006.

There are two weird aspects of this provision, in addition to its invention of exigent circumstances that are more urgent than emergencies.

First, there is no mention of GSM technology here. So nothing would limit the IC to using this solely with the claimed technological problem that purportedly justifies it. They could use it when a target enters the US and continues emailing from his Gmail account using a the hotel WiFi.

Indeed, the decision not to limit this to GSM devices (including tablets), along with the apparent decrease in EO 12333 "roamer" problems and an increase in FAA "roamer" increases right in that period in 2012 when this got exposed, leads me to believe the rising number of FAA "roamers" do not in fact pertain to GSM devices, but rather Internet monitoring. After all, there's little reason to collect phone content on a valid foreign target under FAA rather than EO 12333. So I suspect that all the squawking about "roamers" has served as cover for the fact that the NSA has also not been detasking PRISM collection when targets enter the US (though obviously, some of that Internet activity might take place on a GSM phone or tablet).

There's one more thing that supports that case. Here's how — at least in 2012 — the NSA would discover the GSM phones that entered the US.

> The largest number of incidents in the System Limitations category account for roamers where there was no previous

> indications of the planned travel. These incidents are largely unpreventable. Consistent discovery through the Visitor Location Register (VLR) occurs every quarter and provides analysts with timely information to place selectors into candidate status or detask. Analysis identified that these incidents could be reduced if analysts removed/detasked selectors more quickly upon learning that the status of the selector had changed and more regularly monitored target activity. This analysis indicates that continued research on ways to exploit new technologies and researching the various aspects of personal communications systems to include GSM, are an important step for NSA analysts to track the travel of valid foreign targets. [my emphasis]

Basically, what seems to happen (or have happened 18 months ago) with GSM roamers is that analysts aren't tracking feeds closely enough to notice from content that someone has entered the US. Instead, they learn of roamers only after they get quarterly Visitor Location Register reports that reveal their target had been in the US once a quarter. If that's still true, then the vast majority of roamers will remain undiscovered until well after the 72-hour period has elapsed. The roamer problem will still exist, though unless someone else leaks another internal SID report, we won't know about it.

But for those targets NSA (and other IC agencies) are tracking closely enough to know when they enter the US, this will give them an addition 3-day grace period, on top of the 7 days already available under FISA) to conduct surveillance, and do so without any paperwork.