WHY IS THE GOVERNMENT POISON-PILLING ECPA REFORM?

Back in 2009, the Obama Administration had Jeff Sessions gut an effort by Dianne Feinstein to gut an effort by Patrick Leahy to gut an effort by Russ Feingold to halt the phone and Internet dragnet programs (as well as, probably, some Post Cut Through Dialed Digit collections we don't yet know about).

> See what Jeff Sesssions—I mean Barack Obama—did in complete secrecy and behind the cover of Jeff Sessions' skirts the other night?
>
> They absolutely gutted the minimization procedures tied to pen registers! Pen registers are almost certainly the means by which the government is conducting the data mining of American people (using the meta-data from their calls and emails to decide whether to tap them fully). And Jeff Sesssions—I mean Barack Obama—simply gutted any requirement that the government get rid of all this meta-data when they're done with it. They gutted any prohibitions against sharing this information widely. In fact, they've specified that judges should only require minimization procedures in extraordinary circumstances. Otherwise, there is very little limiting what they can do with your data and mine once they've collected it. [no idea why I was spelling Sessions with 3 ses]

At each stage of this gutting process, Feingold's effort to end bulk collection got watered down until, with Sessons' amendments, the Internet dragnet was permitted to operate as it had been. Almost the very same time this happened, NSA's General Counsel finally admitted

that *every single record* the agency had collected under the dragnet program had violated the category restrictions set back in 2004. Probably 20 days later, Reggie Walton would shut down the dragnet until at least July 2010.

But before that happened, the Administration made what appears to be — now knowing all that we know now — an effort to legalize the illegal Internet dragnet that had replaced the prior illegal Internet dragnet.

I think that past history provides an instructive lens with which to review what may happen to ECPA reform on Thursday. A version of the bill, which would require the government to obtain a warrant for any data held on the cloud, passed the House unanimously. But several amendments have been added to the bill in the Senate Judiciary Committee that I think are designed to serve as poison pills to kill the bill.

The first is language that would let the FBI resume obtaining Electronic Communication Transaction Records with just a National Security Letter (similar language got added to the Intelligence Authorization; I'll return to this issue, which I think has been curiously reported).

The second is language that would provide a vast emergency exception to the new warrant requirement, as described by Jennifer Daskal in this post.

> [T]here has been relatively little attention to an equally, if not more, troubling emergency authorization provision being offered by Sen. Jeff Sessions. (An excellent post by Al Gidari and op-ed by a retired DC homicide detective are two examples to the contrary.)
>
> The amendment would allow the government to bypass the warrant requirement in times of claimed emergency. Specifically, it would *mandate* that

> providers turn over sought-after data in response to a claimed emergency from federal, state, or local law enforcement officials. Under current law, companies are *permitted*, but not required, to comply with such emergency – and warrantless – requests for data.
>
> There are two huge problems with this proposal. First, it appears to be responding to a problem that doesn't exist. Companies already have discretion to make emergency disclosures to governmental officials, and proponents of the legislation have failed to identify a single instance in which providers failed to disclose sought-after information in response to an actual, life-threatening emergency. To the contrary, the data suggest that providers do in fact regularly cooperate in response to emergency requests. (See the discussion here.)
>
> Second, and of particular concern, the emergency disclosure mandate operates with no judicial backstop. None. Whatsoever. This is in direct contrast with the provisions in both the Wiretap Act and Foreign Intelligence Surveillance Act (FISA) that require companies to comply with emergency disclosure orders, but then *also* require subsequent post-hoc review by a court. Under the Wiretap Act, an emergency order has to be followed up with an application for a court authorization within 48 hours (see 18 U.S.C. § 2518(7)). And under FISA, an emergency order has to be followed with an application to the court within 7 days (see 50 U.S.C. § 1805(5)). If the order isn't filed or the court application denied, the collection has to cease.
>
> The proposed Sessions amendment, by contrast, allows the government to claim

> emergency and compel production of emails, without any back-end review.

Albert Gidari notes that providers are already getting a ton of emergency requests, and a good number of them turn out to be unfounded.

> For the last 15 years, providers have routinely assisted law enforcement in emergency cases by voluntarily disclosing stored content and transactional information as permitted by section 2702 (b)(8) and (c)(4) of Title 18. Providers recently began including data about emergency disclosures in their transparency reports and the data is illuminating. For example, for the period January to June 2015, Google reports that it received 236 requests affecting 351 user accounts and that it produced data in 69% of the cases. For July to December 2015, Microsoft reports that it received 146 requests affecting 226 users and that it produced content in 8% of the cases, transactional information in 54% of the cases and that it rejected about 20% of the requests. For the same period, Facebook reports that it received 855 requests affecting 1223 users and that it produced some data in response in 74% of the cases. Traditional residential and wireless phone companies receive orders of magnitude more emergency requests. AT&T, for example, reports receiving 56,359 requests affecting 62,829 users. Verizon reports getting approximately 50,000 requests from law enforcement each year.
>
> [snip]
>
> Remember, in an emergency, there is no court oversight or legal process in advance of the disclosure. For over 15 years, Congress correctly has relied on

> providers to make a good faith determination that there is an emergency that requires disclosure *before legal process can be obtained*. Providers have procedures and trained personnel to winnow out the non-emergency cases and to deal with some law enforcement agencies for whom the term “emergency” is an elastic concept and its definition expansive.
>
> Part of the problem, and the temptation, is that there is no *nunc pro tunc* court order or oversight for emergency requests or disclosures. Law enforcement does not have to show a court after the fact that the disclosure was warranted at the time; indeed, no one may ever know about the request or disclosure at all if it doesn’t result in a criminal proceeding where the evidence is introduced at trial. In wiretaps and pen register emergencies, the law requires providers to cut off continued disclosure if law enforcement hasn’t applied for an order within 48 hours. But if disclosure were mandatory for stored content, all of a user’s content would be out the door and no court would ever be the wiser. At least today, under the voluntary disclosure rules, providers stand in the way of excessive or non-emergency disclosures.
>
> [snip]
>
> A very common experience among providers when the factual basis of an emergency request is questioned is that the requesting agency simply withdraws the request, never to be heard from again. This suggests that to some, emergency requests are viewed as shortcuts or pretexts for expediting an investigation. In other cases when questioned, agents withdraw the emergency request and return with proper

> legal process in hand shortly thereafter, which suggests it was no emergency at all but rather an inconvenience to procure process. In still other cases, some agents refuse to reveal the circumstances giving rise to the putative emergency. This is why some providers require written certification of an emergency and a short statement of the facts so as to create a record of events — putting it in writing goes a long way to ensuring an emergency exists that requires disclosure. But when all is in place, providers respond promptly, often within an hour because most have a professional, well-trained team available 7×24.

In other words, what seems to happen now, is law enforcement use emergency requests to go on fishing expeditions, some of which are thwarted by provider gatekeeping. Jeff Sessions — the guy who 7 years ago helped the Obama Administration preserve the dragnets — now wants to make it so these fishing expeditions will have no oversight at all, a move that would make ECPA reform meaningless.

The effort to lard up ECPA reform with things that make surveillance worse (not to mention the government's disinterest in reforming ECPA since 2007, when it first started identifying language it wanted to reform) has my spidey sense tingling. The FBI has claimed, repeatedly, in sworn testimony, that since the 2010 Warshak decision in the Sixth Circuit, it has adopted that ruling everywhere (meaning that it has obtained a warrant for stored email). If that's true, it should have no objection to ECPA reform. And yet … it does.

I'm guessing these emergency requests are why. I suspect, too, that there are some providers that we haven't even thought of that are even more permissive when turning over "emergency" content than the telecoms.