YUP: THE GOVERNMENT IS SECRETLY HIDING ITS CRYPTO BATTLES IN THE SECRET FISA COURT

When I analyzed the Wyden-Paul Section 702 reform bill, I noted language that suggested Wyden was concerned about the government using the secrecy of FISA Court proceedings to demand technical assistance from providers they otherwise couldn't get. Wyden's bill makes it clear he's concerned that the government would (or is) making technical demands without even telling the FISC it is doing so. His bill would explicitly require review of any technical demands by the court.

> (B) LIMITATIONS.—The Attorney General or the Director of National Intelligence may not request assistance from an electronic communication service provider under subparagraph (A) without demonstrating, to the satisfaction of the Court, that the assistance sought—
>
> (i) is necessary;
>
> (ii) is narrowly tailored to the surveillance at issue; and
>
> (iii) would not pose an undue burden on the electronic communication service provider or its customers who are not an intended target of the surveillance.
>
> (C) COMPLIANCE.—An electronic communication service provider is not obligated to comply with a directive to provide assistance under this paragraph unless
>
> (i) such assistance is a manner or method that has been explicitly approved by the Court; and
>
> (ii) the Court issues an order, which

> has been delivered to the provider, explicitly describing the assistance to be furnished by the provider that has been approved by the Court.

I suggested the most likely use of such a "technical assistance" demand would be requiring a company (cough, Apple) to back door its encryption.

> The most obvious such application would involve asking Apple to back door its iPhone encryption.
>
> As a reminder, national security requests to Apple doubled in the second half of last year.
>
> > The number of national security orders issued to Apple by US law enforcement doubled to about 6,000 in the second half of 2016, compared with the first half of the year, Apple disclosed in its biannual transparency report. Those requests included orders received under the Foreign Intelligence Surveillance Act, as well as national security letters, the latter of which are issued by the FBI and don't require a judge's sign-off.
>
> We would expect such a jump if the government were making a slew of new requests of Apple related to breaking encryption on their phones.

In his statement on the bill, Wyden made it clear that that's precisely what he is concerned about.

> It leaves in place current statutory authority to compel companies to provide assistance, potentially opening the door

> to government mandated de-encryption without FISA Court oversight. [my emphasis]

And note: he is saying that the government will (that is, has already, most likely) done this without asking the FISC to review whether its technical demands are narrowly tailored and necessary.

Update: This post has been updated in response to comments to clarify that Wyden is not concerned about technical demands per se, but about technical demands with no FISC review.

Update: One more point to make clear: for "individual" orders, the court will review every facility, which will involve some review of what kinds of access the government will get (such as when, in 2015, the government ordered Yahoo to scan all its users for some kind of signature).

But under 702, the "assistance" language that the government could use to obligate back doors (or whatever else) is not tied to anything the court reviews. Annual certifications have to affirm *that* the collection requires domestic provider assistance (but does not require a description of what that assistance entails).

> vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

But then once that certificate is signed, the government can work at the level of directives, demanding, compensating, and indemnifying the provider for that assistance *all without any court review*.

> (h) Directives and judicial review of directives
>
> (1) Authority: With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may

> direct, in writing, an electronic communication service provider to—
>
> (A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and
>
> (B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.
>
> (2) Compensation
>
> The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).
>
> (3) Release from liability
> No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

That's why the risk is that much greater for 702: because the court is never going to review the individual directives which is where the specific technical assistance gets laid out (unless a provider is permitted to challenge those directives).