"CIRCUMVENTING" ENCRYPTION IS DIFFERENT THAN "WEAKENING" OR "ALTERING" IT

I'm still catching up to the Questions for the Record that ODNI submitted to the Senate Intelligence Committee after its June hearing on 702. So I'd like to look more closely at something from the QFRs first reported by Zack Whittaker on encryption.

It has to do with a response to a Ron Wyden question about whether 702 provides authority to "circumvent or weaken" encryption.

Question 16: Does Section 702 provide authority to direct a provider to circumvent or weaken the encryption in a service or app that it offers and, if so, has that occurred?

Answer:

(U) Section 702(h) provides that, with respect to an authorization pursuant to section 702(a), the Attorney General and Director of National Intelligence may direct, in the form of a written directive, an electronic communication service provider to "provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition." 50 U.S.C. § 1881a(h)(1)(A). To the extent that a provider does not fully provide such information, facilities, or assistance, FISA provides a means for the government to require the provider's compliance. Specifically, "the Attorney General may file a petition for an order to compel the electronic communications service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition." 50 U.S.C. § 1881a(h)(5). The nature of the "information, facilities, or assistance necessary to accomplish the acquisition" may vary among providers, services, and technologies. The government has not to date sought an order pursuant to Section 702(h)(5) seeking to compel an electronic communication service provider to alter the encryption afforded by a service or product it offers.

Whittaker notes what I pointed out here — because of the way 702 works, "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)." That's the headline point of his piece, one I agree with.

> The US government does not need the approval of its secret surveillance court to ask a tech company to build an encryption backdoor.

Whittaker also notes that this language falls far short of denying (or confirming) whether it has asked for a back door. Meaning, it's

possible they asked a provider for a back door, and the provider complied without being forced to.

That said, I wanted to point out the limits to this claim from Whittaker.

> In its answers, the government said it has "not to date" needed to ask the FISC to issue an order to compel a company to backdoor or weaken its encryption.

It is true that the government says it has not asked an ECSP to "alter the encryption provided by a service or product it offers."

But that answer is non-responsive to the totality of Wyden's question, which asks if the government ordered a provider to "*circumvent* or weaken" encryption. The government only addresses the latter question, whether the government has altered (presumably by weakening) encryption. It hasn't answered, at all, whether it has ordered a provider to "circumvent" encryption.

That's an important point regardless. These QFRs are always carefully crafted, particularly in responses to Wyden (or the few other people who actually exercise oversight).

I think it's particularly important given something that happened with iOS in the last year: rather than just answering, yes or no, before a phone trusts a computer (meaning it will share its contents with iTunes and therefore potentially with Apple), iOS 11 now requires you to enter your password before a phone will trust a computer.

> A different and more significant change is requiring the passcode to "trust" a new computer. Currently, when the police wish to search a phone, they unlock it either with the fingerprint reader, by convincing the suspect to unlock the phone (e.g. to look up a phone number), or they simply seize the phone while it

> is unlocked. None of these avenues directly implicate suspects' constitutional rights. Once the unlocked phone is obtained, officials connect the device to a computer running forensics software, or even just iTunes, direct the device to "trust" the new computer when prompted, and download a backup that contains almost all of the relevant information stored on the phone. Requiring the passcode in order to sync the device with a new machine means that, even with an unlocked device, a party that wants access is now limited to searching the phone manually for visible items and can only perform that search while the phone remains unlocked.

I had already been thinking trusted backups provided a way the government could, through Apple, obtain contents from phones that would otherwise be hard to decrypt (I believe it would require altering iTunes, not the encryption itself). Such an approach would be particularly useful for NatSec investigations, where collecting contents wasn't so much about solving an already committed crime (which is what all the iPhones the government hasn't been able to break into were collected for), but to prevent one or otherwise collect prospective data.

I don't even know if this is technically feasible. Nor do I know whether someone would be better sticking with iOS 10 and just rigorously refusing to trust a given computer or upgrading to iOS 11 and never entering that password.

But I do know this passage on encryption is — with respect to whether the government has ever ordered a company to circumvent encryption — a non-denial.

And I have learned that non-denials, especially in response to Wyden, generally should be closely scrutinized.