Bill Introduced To Prevent Government Agencies From Demanding Encryption Backdoors

from the *pushing-back-from-the-top-down* dept

The FBI continues its push for a solution to its "**going dark**" problem. Joined by the DOJ, agency head Christopher Wray has suggested the **only way forward** is a legislative or judicial fix, gesturing vaguely to the **thousands of locked phones** the FBI has gathered. It's a disingenuous push, considering the **tools available to the agency** to crack locked devices and obtain the apparently juicy evidence hidden inside.

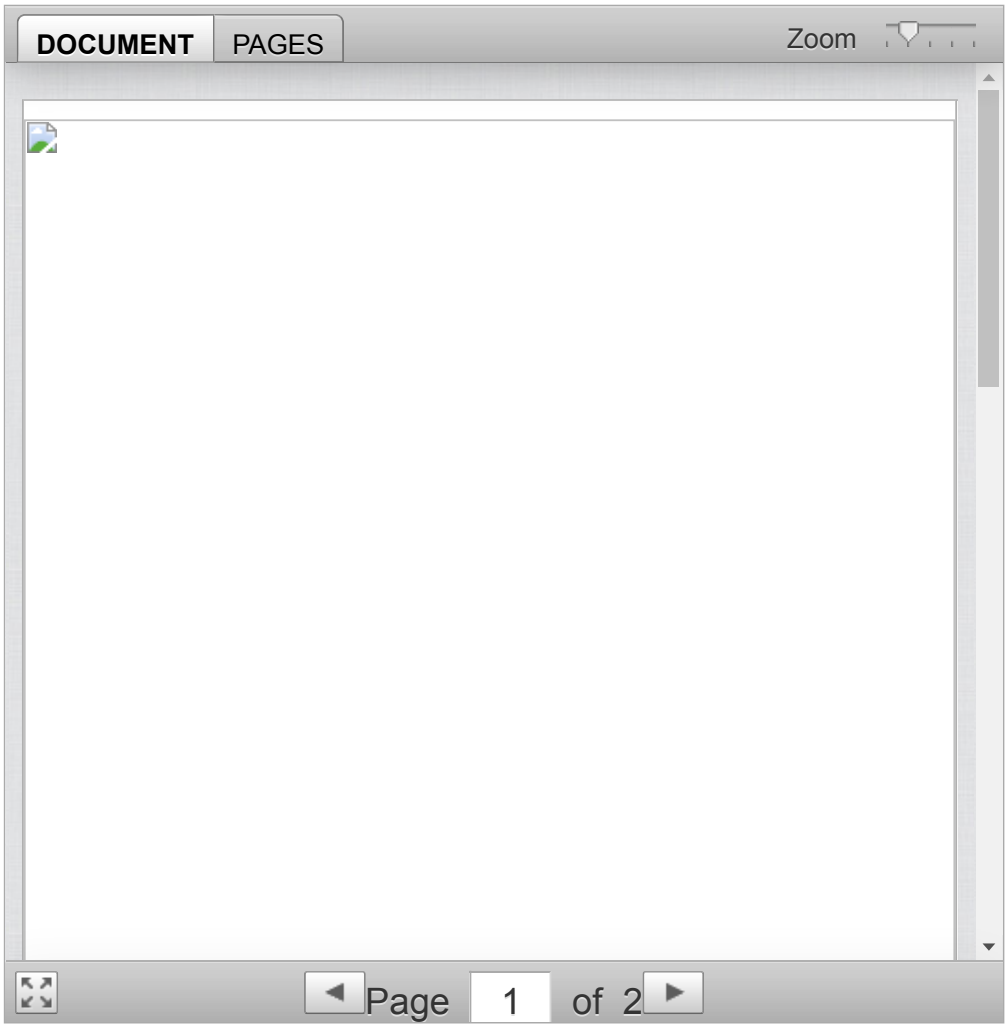
The FBI **hasn't been honest** in its efforts or its portrayal of the problem. **Questions put to the FBI**about its internal efforts to crack locked devices **are still unanswered**. The only "new" development isn't all that new: Ray Ozzie's **"key escrow" proposal** may tweak a few details but it's not that far removed in intent from the Clipper Chip that kicked off the first Crypto War. It's nothing more than another way to make device security worse, with the only beneficiary being the government.

The FBI's disingenuousness has not gone unnoticed. Efforts have been made over the last half-decade to push legislators towards mandating government access, but no one has been willing to give the FBI what it wants if it means making encryption less useful. A new **bill** [PDF], introduced by Zoe Lofgren, Thomas Massie, Ted Poe, Jerry Nadler, Ted Lieu, and Matt Gaetz **would codify this resistance to government-mandated backdoors**.

> *The two-page bill has sweeping safeguards that uphold security both for developers and users. As the bill says, "no agency may mandate or request that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency."*
>
> *This bill would protect companies that make encrypted mobile phones, tablets, desktop and laptop computers, as well as developers of popular software for sending end-to-end encrypted messages, including Signal and WhatsApp, from being forced to alter their products in a way that would weaken the encryption. The bill also forbids the government from seeking a court order that would mandate such alterations. The lone exception is for wiretapping standards required under the 1994 Communications for Law Enforcement Act (CALEA), which itself specifically permits providers to offer end-to-end encryption of their services.*

The Secure Data Act shouldn't be needed but the FBI and DOJ have forced the hand of legislators. Rather than take multiple hints dropped

by the previous administration, the agencies have only increased the volume of their anti-encryption rhetoric in recent months. Maybe the agencies felt they'd have the ear of the current administration and Congressional majority, but investigations involving the president and his staff have **pretty much killed** any "law and order" leanings the party normally retains. This bill may see widespread bipartisan support simply because it appears to be sticking it to the Deep State. Whatever. We'll take it. Hopefully, this makes a short and direct trip to the Oval Office for a signature.



14 Comments | **Leave a Comment**

If you liked this post, you may also be interested in...

- EFF Asks FBI, DOJ To Turn Over Details On Thousands Of Locked Phones The FBI Seems Uninterested In Cracking

- Congressional Members Decide It's Time To Make Assaulting A Police Officer A Federal Hate Crime
- FBI's Bust Of Black Open Carry Advocate Predicated On An InfoWars Video Ends In Dismissed Indictment
- Senate Will Vote Wednesday To Try And Save Net Neutrality
- DOJ, DHS Sued Over Inaccurate 'Terrorist Entry' Report

Reader Comments

View by: **Time** | **Thread** Subscribe: **RSS**

That One Guy (profile), *15 May 2018 @ 11:49am*

... and them too I suppose

It's nothing more than another way to make device security worse, with the only beneficiary being the government.

Oh not even close, the main beneficiaries would be the countless criminals who would be handed *millions* of peoples' data on a silver platter, for use and abuse. The various governments would be almost incidental beneficiaries, and *vastly*outnumbered by those without badges.