WIRED

Even Congress Is Slamming That Crummy Crypto Bill

Andy Greenberg

June 29, 2016

SINCE SENATORS RICHARD BURR and Diane Feinstein released their long-awaited legislation to address the conflict between encryption software makers and law enforcement last April, it's made about as much progress as a TI-82 calculator trying to crack a 2048-bit PGP key. The bill, which required all crypto tools to offer some way for a warrant-holding FBI agent to access encrypted information, was roundly reviled by the technology and privacy communities, and quickly lost momentum in DC, too. Now the Burr-Feinstein proposal has received its most definitive rejection yet, and this time the call is coming from inside the House.

On Wednesday the House Subcommittee on Homeland Security released a research paper with the findings of its own investigation into the ongoing crypto debate. The paper, which took into account more than a hundred meetings the researchers had with privacy advocates, cryptographers, technologists, and law enforcement officials, doesn't offer a definitive way forward on encryption legislation. But it does unequivocally state that no current bills—very clearly including the Burr-Feinstein effort—represent the right approach to solving the problem.

"Any legislative solutions yet proposed come with significant trade-offs, and provide little guarantee of successfully addressing the issue," the paper reads. "Lawmakers need to develop a far deeper understanding of this complex issue before they attempt a legislative fix."

The committee's researchers are far from the first to criticize the Senate encryption bill. Privacy advocates were immediately incensed at its heavy-handed approach, which was essentially to ban the encryption already present in everything from an iPhone to Whatsapp to a web browser. New America Foundation director Kevin Bankston told WIRED it was "easily the most ludicrous, dangerous, technically illiterate proposal I've ever seen." The White House also held off on any endorsement of the bill, giving it little chance of advancing this year.

But the House Homeland Security report may signal that Congress itself also harbors strong reservations about any law that would restrict widespread encryption technology. In fact, the committee's research report takes an approach to the encryption issue that at times sounds more like the arguments of the privacy community than those posed previously by the government.

It acknowledges, for instance, that the depiction of the crypto debate as one of "privacy versus security" mischaracterizes it; that encryption is itself a form of necessary security for everything from smartphones to online retail to medical records. "Thus, what we are really dealing with is

not so much a question of ‘privacy versus security,’ but a question of ‘security versus security,’" the paper states.

Rather than coming to any definitive conclusion on the crypto debate, the report instead calls for a so-called National Commission on Security and Technology Challenges to hammer out a more nuanced approach to the issue—the same proposal put forward in a bill late last year from Michael McCaul, who not so coincidentally chairs the House Homeland Security Committee. That commission would, in theory, allow “impacted parties themselves”—i.e. Silicon Valley, cryptographers, and the intelligence and law enforcement agents whose surveillance techniques are blocked their encryption—“to directly engage one another in an honest and in-depth conversation in order to develop the factual foundation needed to support sustainable solutions.”

After years of ongoing debate, however, that call for more discussion feels like a “stalling tactic,” says Susan Hennessey, a former NSA general counsel and current fellow at the Brookings Institution. “It’s a nice punt, by which no one has to take a controversial position,” she says. “The challenge is understanding what this commission is going to produce that isn’t in this report.”

Hennessey argues that Congress needs to instead acknowledge that there may be no solution that pleases both sides, and that legislators need to grapple with the substantive details of the debate: Questions like the interpretation of the All Writs’ Act that the FBI used to try to compel Apple to help bypass the iPhone’s encryption, or the “technical assistance” provision of the Wiretap Act that could force companies to rewrite their code on behalf of law enforcement. “These questions will be answered in modest, moderate ways,” she says. “What we really need is for Congress to start engaging on those issues.”

But merely the recognition from Congress that it needs to learn more before making any decision on the thorny topic of encryption represents progress, says privacy-focused Cato Institute fellow Julian Sanchez. “That may be the most hopeful sign. The dangerous thing is to be… too ignorant to recognize your own ignorance,” he says. Now, he says, “there seems to be willingness to learn, rather than an insistence on getting to what they ‘know’ is the right outcome.”