Burr-Feinstein bill still looks to force companies to break encryption

Michael Heller

September 13, 2016

Potential revisions to the Burr-Feinstein encryption bill -- which would force companies to comply with court orders even if that means breaking strong encryption with a backdoor -- have reportedly been circulating, but no one is quite sure how close to final these revisions are.

Julian Sanchez, founding editor of Just Security and senior fellow at the Cato Institute, claims to have received proposed revisions to the Burr-Feinstein Compliance with Court Orders Act. However, a Feinstein spokesperson insisted there is no new official draft of the bill and Senator Feinstein is still gathering feedback, but Sanchez was in possession of "nothing more than a brainstorming document."

There is no guarantee that any of the changes found in this version of the bill would make it to the next official draft, but it does demonstrate work is being done to ready the bill for another attempt on Capitol Hill.

The Burr-Feinstein Compliance with Court Orders Act has had a tumultuous history to say the least and many call it the "**anti-encryption bill**." It was **first presented** in April in order to "solicit input from the public and key stakeholders before formally introducing the bill," but the bill was never formally introduced because of the storm of criticism it received.

The changes Sanchez **noted** followed a pattern of limiting various aspects of the original proposal. Sanchez said the overall scope was reduced so instead of the law applying to data rendered unintelligible "by a feature, product, or service owned, controlled, created, or provided, by the covered entity or by a third party on behalf of the covered entity," it would only apply to the person or company that "controls" the encryption process. This limitation would remove the ability for law enforcement to compel browser makers to build backdoors to encrypted traffic, or hold app store providers liable for software using encrypted communication.

The law could only be applied to investigations of serious crimes and not to "foreign intelligence, espionage, and terrorism" as originally written. Critical infrastructure would be excluded from the bill and there would be more limitations on the "technical assistance" obligations so those asked would only have to make "reasonable efforts" to comply with law enforcement.

"Incorporating these changes -- above all the first one -- would yield something a good deal narrower than the original version of the bill, and therefore not subject to all the same objections that one met with," Sanchez wrote. "It would still be a pretty bad idea. This debate clearly isn't going anywhere, however, and we're likely to see a good deal more evolution before anything is formally introduced."

Sanchez said the change to the overall scope to only apply to the entity that "controls" the encryption process would be a significant change but also one that doesn't make a lot of sense, unless it is meant to "specifically target companies like Apple that are seeking to combine the strong security of end-to-end encryption with the convenience of cloud services."

"If we interpret 'control' of an encryption process in the ordinary-language sense then the law becomes radically narrower in scope, but also fails to cover most of the types of cases that are cited in discussions of the 'going dark' problem. When a user employs a device or application to encrypt data with a user-generated key, that process is not normally under the 'control' of the entity that 'created' the hardware or software in any intuitive sense," Sanchez wrote. "On the other hand, when a company is in direct control of an encryption process -- as when a cloud provider applies its own encryption to data uploaded by a user -- then it would typically (though by no means necessarily) retain both the ability to decrypt and an obligation to do so under existing law."

As Sanchez noted, none of these changes alter the basic aim of the bill which many security professionals have criticized. Burr and Feinstein contended the aim was to compel companies to cooperate with a lawfully served court order, echoing the long-held **stance of the FBI** in the so-called "**going dark**" debate. But, critics said the only way companies would be able to comply with court orders under the bill would be to build **backdoors** in software and weaken encryption.

When the original draft of the Burr-Feinstein bill was released, Riana Pfefferkorn said it was an attack on strong encryption.

"As cryptography experts have repeatedly and consistently explained for over two decades, we cannot make a 'golden key' that only 'good guys' with a court order can use to 'unlock' encrypted information. Any built-in means for accessing encrypted data can, and will, be used by the bad guys too," Pfefferkorn **wrote**. "Yet the Burr-Feinstein bill perpetuates the golden key fantasy. In the pursuit of that impossible goal, the bill would effectively ban cornerstone security concepts such as **end-to-end encryption** … and perfect forward secrecy, which protects previous encrypted communications even if an encryption key or password is compromised in the future."