Graham, Cotton introduce yet another attempt to torpedo encryption

Enlarge / This dog was part of widespread protests against the FBI’s attempts to penetrate iPhone encryption.

reader comments

132 with 96 posters participating, including story author

Share this story

On Tuesday, Sens. Lindsey Graham (R-S.C.), Tom Cotton (R-Ark.), and Marsha Blackburn (R-Tenn.) introduced yet another bill attempting to poke holes in data encryption, called the Lawful Access To Encrypted Data Act. This bill follows previous US efforts to weaken encryption, including March’s proposed EARN IT Act and demands made by US Attorney General William Barr in his 2019 keynote address at the International Conference on Cyber Security.

A press release from the Senate Judiciary Committee—which is chaired by Graham—describes the bill as “a balanced solution that keeps in mind the constitutional rights afforded to all Americans, while providing law enforcement the tools needed to protect the public from everyday violent crime and threats to our national security.” It goes on to emphasize—in both bold and italic text—that the bill would “only” require service providers to grant law enforcement a back door after a court issues a warrant.

Graham expresses his personal position in strong terms:

> *Terrorists and criminals routinely use technology, whether smartphones, apps, or other means, to coordinate and communicate […] tech companies have refused to honor [court orders] and assist law enforcement in their investigations. My position is clear: After law enforcement obtains the necessary court authorizations, they should be able to retrieve information to assist in their investigations. Our legislation respects and protects the privacy rights of law-abiding Americans.*

Unfortunately, as is typical for these resolutions, Graham's expressed ideas don't adhere to technological reality. In order for a service provider to "honor and assist" law enforcement investigations in the way Graham demands, it would necessarily—and fatally—have to compromise the very encryption it offered in the first place. This would apply to every consumer the provider services (American or otherwise), whether a warrant were issued or not.

Encryption doesn't work that way

Providing the sort of backdoor Graham and company keep asking for means, among other things, providing the service provider itself access to "encrypted" data. This, in turn, opens that provider's customers up to privacy violations from the service provider—or rogue employees of the service provider—themselves, which in turn would break much of the security model of modern cloud services. This would gravely impact not only end consumer privacy but enterprise business security as well.

In recent years, large cloud providers such as Amazon, Microsoft, and Google have made big and successful pushes to convince large businesses to host increasingly confidential business data in their data centers. This is only feasible because of secure encryption using keys inaccessible to the cloud provider itself. Without provider-opaque encryption,

those businesses would return to storing critically confidential data only in self-managed and controlled private data centers—increasing cost and decreasing scalability for those businesses.

This, of course, only scratches the surface of the true impact of such a misguided effort. Secure encryption is an already widely available technology, and it doesn't require massive infrastructure to implement. There is no reason to assume that the very terrorists Graham, Cotton, and Blackburn invoke wouldn't simply revert to privately managed software without holes poked in it were such a bill to pass.

There's also no reason to assume that the service providers themselves would be the only ones able to access the critical loopholes LAEDA would require. It's difficult to imagine that such vulnerabilities would not rapidly become widely known and be exploited by garden-variety criminals, foreign and domestic business espionage units, and foreign nations.

Follow-on economic impact

Finally, the passage of a US bill such as LAEDA would not constrain service providers in foreign countries. Another likely impact of such a bill would be to simply shift such services offshore to European and Asian providers—reducing American tax revenues and technical prominence, while pushing the very data Graham so badly wants access to even further out of his reach.

Deputy Director Evan Greer of advocacy group Fight for the Future gave Ars the following statement about LAEDA and a similar predecessor, the EARN IT Act:

> *Politicians who don't understand how technology works need to stop introducing legislation like this. It's embarrassing at this point. Encryption protects our hospitals, airports, and the water treatment facilities our children drink from.*

> *Security experts have warned over and over again that weakening encryption or installing back doors will make everyone less safe, not more safe. Full stop. Lawmakers need to reject the Lawful Access to Encrypted Data act along with the EARN IT act. These bills would enable mass government surveillance while doing nothing to make children, or anyone else, any safer.*

Although the actual text of the bill does not seem to be publicly available yet, the Judiciary Committee's press release outlines a few key points. The attorney general would be prohibited from issuing directives with specific technical steps for complying with the act—but would be allowed to issue directives requiring compliance. The AG would also be empowered to direct service providers or device manufacturers to report both their ability to comply and timeline for implementation of the loopholes necessary to comply.

The bill specifies that service providers and device manufacturers issued such directives would be compensated with government funding for reasonable costs incurred in compliance with that directive. It also establishes a prize competition to award participants who "create a lawful access solution in an encrypted environment, while maximizing privacy and security."

https://arstechnica.com/?p=1686929