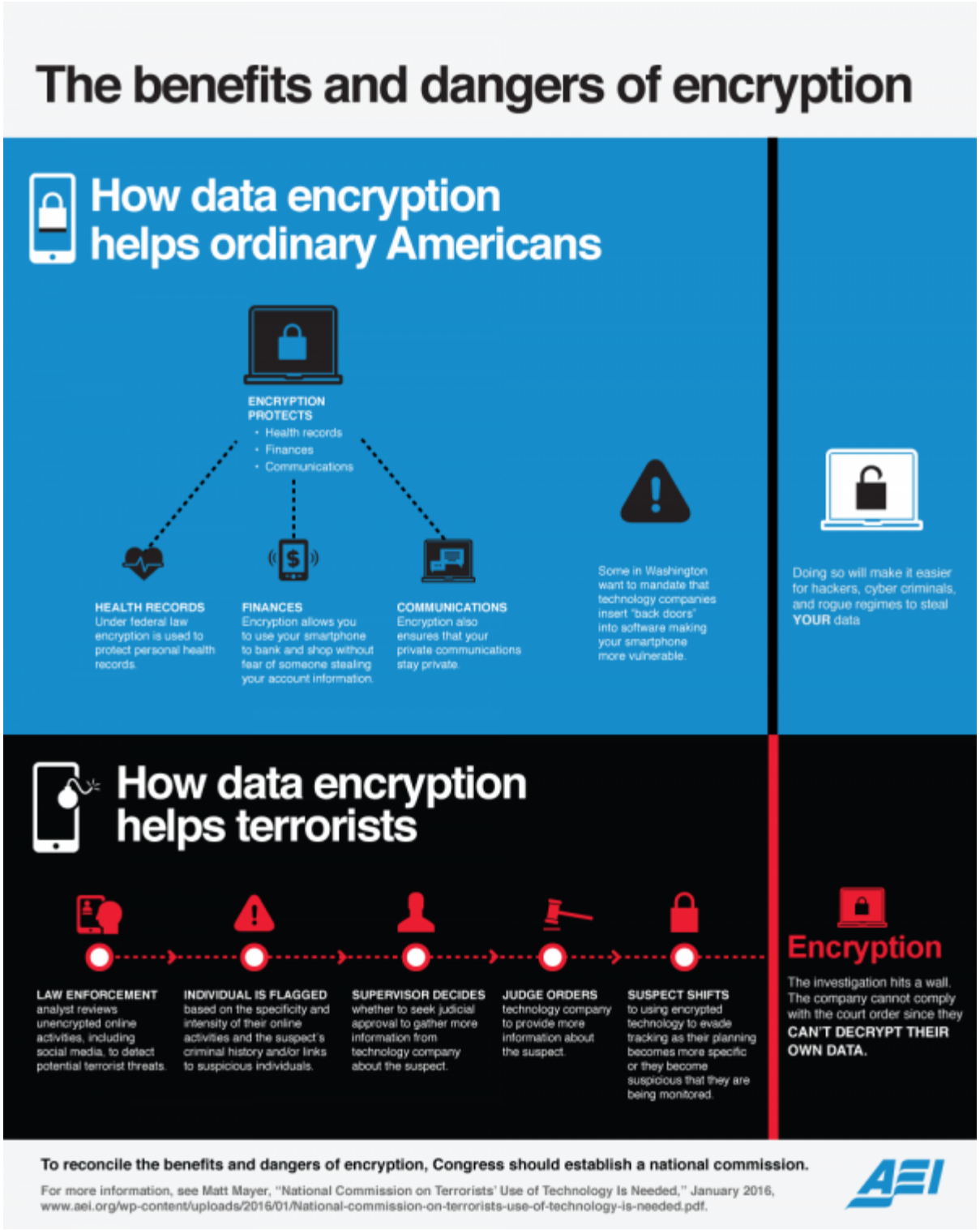
Feinstein-Burr encryption bill is too clever by half

Matt A. Mayer
April 29, 2016 10:50 am | *AEIdeas*

A couple of weeks ago, in response to the FBI versus Apply fight over an encrypted iPhone, US Senators Diane Feinstein and Richard Burr released a draft of their legislation titled, "Compliance with Court Orders Act of 2016 (https://josephhall.org/f0eabaa89b8ee38577bf7d0fd50ddf0d58ecd27a/307378123-Burr-Encryption-Bill-Discussion-Draft.pdf)." The reaction to the proposed legislation has been all over the map, with some lambasting the legislation as "ludicrous, dangerous, technically illiterate (https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/)." I actually think the Burr-Feinstein bill is as clever as it is underhanded. Nevertheless, this legislation *is* dangerous.

Encryption, while used by terrorists, also protects everyday Americans. Mandated backdoors will make your private information more vulnerable to hacking, will drive tech companies (and jobs) overseas, and won't stop terrorists who will just as easily procure off-the-shelf encryption technology overseas.



(http://www.aei.org/wp-content/uploads/2016/04/How-Data-Encryption-Benefits-and-Dangers-e1461940931198.png)

See in greater detail here. (http://www.aei.org/multimedia/how-data-encryption-helps-terrorists/).

In terms of the proposed legislation, section (3)(b) specifically allows Congress to claim it is not mandating backdoors so encryption is preserved as the status quo.

The section states: “Nothing in this Act may be construed to authorize any government officer to require or prohibit any specific design or operating system to be adopted by any covered entity.” In plain English, this means that there is no backdoor mandate allowed.

This provision is an exception that renders the rule in section (3)(b) meaningless.

However, section (3)(a)(1)(B) requires any covered entity to “provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order.” This section means that any company that encrypts its technology or software will be required to break its own encryption “as is necessary” to satisfy a court order. In effect, this legislation *does* mandate backdoors. This provision is an exception that renders the rule in section (3)(b) meaningless. It also covers issues on a case-by-case basis so Congress can claim it isn’t making everyone vulnerable, as the technology companies have claimed would be the case with a mandated backdoor.

Finally, section (3)(a)(3) supplements the previous provision by requiring cost recovery for the technology company, thereby eliminating claims that being forced to crack its encryption is a taking of some sort or that the private sector is being forced to do something without compensation. Congress will at least pay the private sector to do something it doesn’t want to do.

I think the proposed legislation would be terrible for our technology community because it will quell encryption, create more uncertainty, and incentivize US companies to move to foreign domiciles to avoid the law, among other items.

Learn more: Easy on encryption (http://www.aei.org/publication/easy-on-encryption/)

This type of legislation is precisely why a national commission is the best option (https://www.aei.org/wp-content/uploads/2016/01/National-commission-on-terrorists-use-of-technology-is-needed.pdf) to ensure thoughtful consideration of all equities and potential unintended outcomes. This issue is a critical one that requires the “worst-best” solution we can settle on without trying to be too clever by half, as Senators Feinstein and Burr are being.