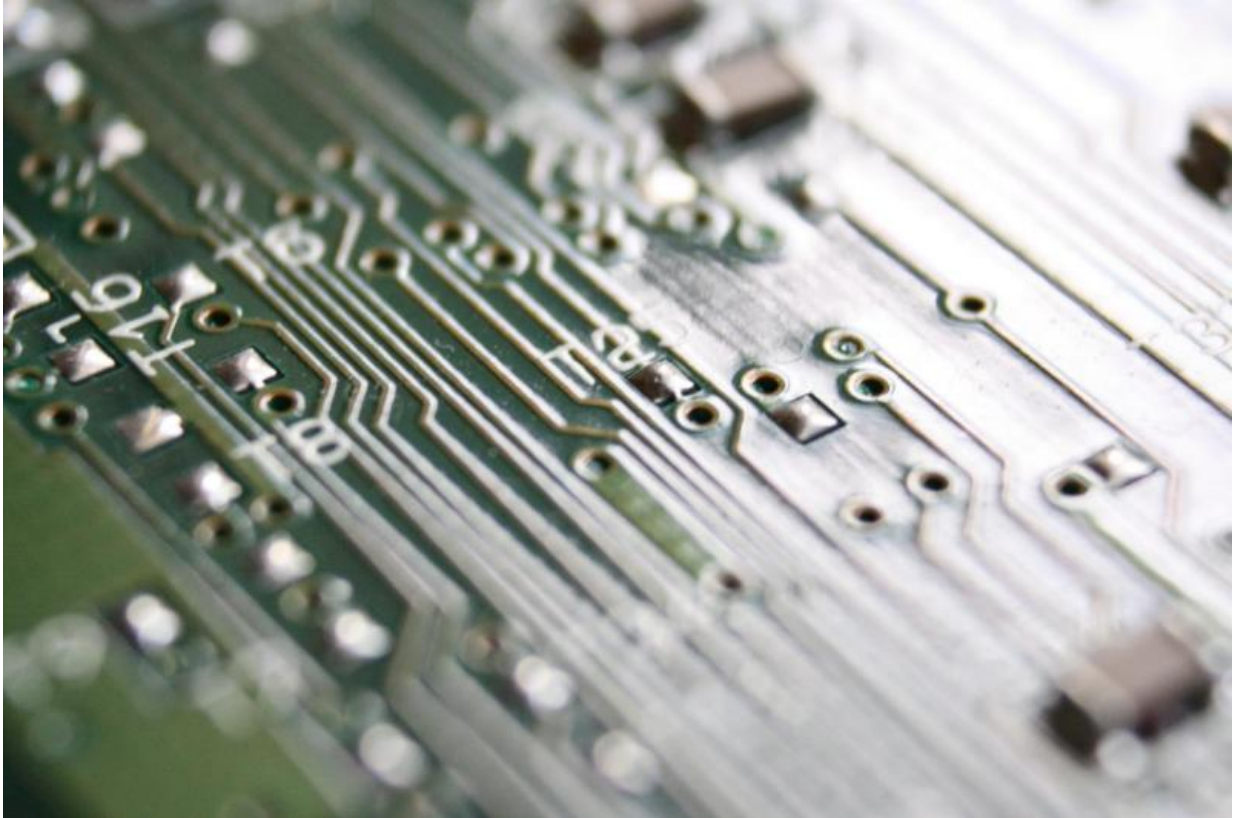


Encryption debate isn't going away

March 31 2016, by Troy Wolverton, San Jose Mercury News



Credit: Public Domain

The fight over encryption isn't going away just because the FBI has figured out a way to glean the data off the iPhone used by a San Bernardino attacker.

Indeed, it's only likely to get more heated in the future.

Underneath Apple's battle with the FBI are deep-rooted differences between the tech industry and the government authorities. And neither side is backing down.

The Justice Department said Monday that ensuring that they have access to digitized data remains a "priority," adding pointedly it will "continue to pursue all available options" to get at it.

Meanwhile, Apple reiterated that its stance that the government's efforts were "wrong" and "dangerous" and that the company would only increase the security of its products.

Despite the momentary truce, should another mass terror attack happen in the U.S., and should it be found that the attackers used [encryption](#) to cloak their plans, you better believe the calls to break the security or leave open holes for [law enforcement](#) will come back with a vengeance.

But apart from the debates about national security and the ability of law enforcement to get information that they believe will protect us, we actually need encryption and security to get stronger. Encryption isn't just a thorn in the side of law enforcement; it's a crucial tool that protects personal data from thieves, hackers and others with malicious intentions.

Millions of people have had their [personal data](#) - health records, Social Security numbers, [credit card accounts](#) - compromised, in large part due to lax security. Better protection can save millions of dollars - and it also can save lives because encryption doesn't just cloak the communications of terrorists, it also protects government dissidents and whistle-blowers.

Tech security is something of a binary thing. Either it works or it doesn't. Either something is secure or it isn't. You can't open a hole for only the "good guys." The bad guys can use the same hole if they find it - and

sooner or later they will.

Neither Apple in particular nor U.S. companies in general own a monopoly on [encryption software](#). Indeed, some of the foundational encryption technologies are open source, freely available to anyone to use.

The divide between the security and law enforcement community in Washington and the [tech companies](#) and Silicon Valley dates back long before the San Bernardino attacks. As the Edward Snowden revelations and other reports have made clear, efforts since 9/11 to prevent further terrorist attacks often went beyond what was clearly legal, constitutional or even wise.

Those revelations shattered the trust customers had in the tech companies and the trust between those companies and the government, setting the stage for the current escalation of words and threats in the courts - and perhaps soon in Congress with efforts to clarify the law. It's been clear from the beginning - despite the denials on the government's part - that this case has been about more than just this one iPhone. The government wanted to set a precedent that it could force a technology company to undermine its own security.

At the same time, moves by government groups to thwart security protections have encouraged companies, particularly Apple, to ramp up, not weaken, their [security](#) efforts.

And part of the difference between the two sides stems from a clash of cultures. Painting admittedly with a broad brush, Washington is about laws and the establishment and deferring to traditions and authority. Silicon Valley, by contrast, has a libertarian streak that infuses its technology and startups and its belief in challenging received wisdom and the status quo.

None of those differences are going to just disappear. So prepare for the encryption wars to continue.

©2016 San Jose Mercury News
Distributed by Tribune Content Agency, LLC.

Citation: Encryption debate isn't going away (2016, March 31) retrieved 26 April 2024 from <https://phys.org/news/2016-03-encryption-debate-isnt.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.