Apple v. FBI encryption case shows that lawsuits are inherently polarizing

Matt A. Mayer
March 8, 2016 11:43 am | *AEIdeas*

Over the last week, technology companies have filed two "friend of court" briefs in the case involving Apple and the Federal Bureau of Investigation (FBI) over the iPhone of San Bernardino terrorist Syed Rizwan Farook.

The technology companies represented in the first brief (http://www.scribd.com/doc/302020545/Apple-Amicus-Brief-Final) included, among others, Airbnb, eBay, Kickstarter, LinkedIn, Reddit, Square, Twitter, and Wickr. The technology companies represented in the second brief (https://cloud.app.box.com/AmicusBrief) included, among others, Amazon, Cisco, Dropbox, Facebook, Google, Microsoft, Mozilla, Pinterest, Snapchat, WhatsApp, and Yahoo. The collection of companies included in the two briefs shows near unanimity among technology companies in opposition to two major points: (1) the use of the All Writs Act of 1789 to force Apple to create code to enable the FBI to brute force hack Farook's iPhone and (2) the need for Congress to act. These filings demonstrate the inherent polarization of legal actions, as lawsuits create the ultimate "us versus them" dynamic.

(http://www.aei.org/wp-content/uploads/2016/03/RTS8TCG_comey_apple_fbi-e1457455134798.jpg)

Bruce Sewell, general counsel for Apple Inc., watches as FBI Director James Comey testifies during a House Judiciary hearing on Capitol Hill in Washington March 1, 2016. REUTERS/Joshua Roberts.

The second amicus brief contains a few key sections worth reading. First, on the two opposition points, the brief notes that "[f]or technology companies like amici, the difference between judicial action and legislative action is not merely philosophical and constitutional. It is critical from a practical standpoint that regulatory changes come, if at all, through the legislative process—and not through decisions from individual judges across the country applying the All Writs Act." This opposition goes beyond the interests of the technology companies. It undermines every American's role as a voter and as a consumer, as well. As the brief notes, "The American people as voters are cut out of this important debate, because their elected representatives have no opportunity to weigh complex policy choices. And the American people as consumers are cut out of the debate, because they cannot select products based on company policies or security features if the government may override those policies and features without notice." These are important considerations to keep in mind.

When it comes to the specific application of the powers of the All Writs Act of 1789 to this case, the brief observes the fundamental difference between giving technical assistance and being forced to write new software code:

> That is an altogether different power from the one the government seeks here, a power to commandeer private engineers working for private companies to write computer code that would disable the security protections their employers have designed into their products. …
>
> How apps and programs store data is not just — as the government claims — a "public brand marketing strategy." It is at the core of the products' identities… Indeed, how companies store and manage customers' data is one way companies tailor their chat, e-mail, social-media, and data-storage solutions to customers' needs. Change those features and the government has changed the product in a fundamental way. The government therefore does not seek unobjectionable technical assistance; it seeks the ability to compel technology companies to modify their products, on spec, for the FBI in ways that are contrary to their core values.

No matter which side you think is right in this specific case, that last sentence speaks volumes about how the technology industry sees this case. The federal government wants them to do something that is against their "core values."

Learn more: National commission on terrorists' use of technology is needed (http://www.aei.org/publication/national-commission-on-terrorists-use-of-technology-is-needed/) | Conflicting district court decisions show why Congress should act on encryption (http://www.aei.org/publication/conflicting-district-court-decisions-show-why-congress-should-act-on-encryption/) | Support for national commission on terrorists' use of encryption grows (http://www.aei.org/publication/support-for-national-commission-on-terrorists-use-of-encryption-grows/)

I don't know about you, but, when someone attacks my core values, I will do everything I can to defend myself and prevail. America cannot afford a fight between the federal government and the technology industry. Silicon Valley is one of America's greatest success stories, as it shows the reality of the American Dream, the power of entrepreneurship, and what can happen when government largely stays out of the way. Any government action that undermines our overwhelming technological superiority and attacks the core values of Silicon Valley runs the risk of incentivizing our greatest companies to do what they are already doing with their cash due to high tax rates and move operations elsewhere.

As I advocated over two months ago, Congress should launch a national commission (https://www.aei.org/wp-content/uploads/2016/01/National-commission-on-terrorists-use-of-technology-is-needed.pdf) on terrorists' use of technology that brings the parties together to hash out their equities and come up with the "worst-best" recommendations for Congress to use in legislation. This is an incredibly complex issue. The best way to solve it is by way of a commission that unites us, rather than a lawsuit that divides us.

Full Disclosure: My wife and I own 251 shares of Apple stock, as well as 113 shares of Cisco and 116 shares of Microsoft. Of course, like many Americans, my family also owns two Apple computers, three iPhones, an iTouch, two Apple TVs, and two iPads.