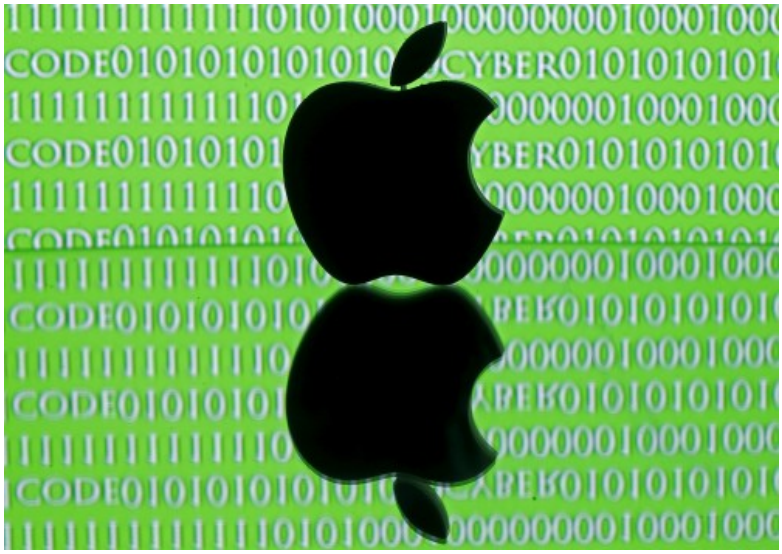
Conflicting district court decisions show why Congress should act on encryption

Matt A. Mayer
March 1, 2016 10:43 am | *AEIdeas*

Over the course of thirteen days, two magistrates issued two conflicting decisions on whether the All Writs Act of 1789 gave the courts the power to order Apple to create software to assist the government in breaking into an iPhone.

The first decision, delivered by the United States District Court for the Central District of California on February 16, 2016, over access to San Bernardino terrorist Syed Rizwan Farook's encrypted iPhone, concluded that the All Writs Act did permit (http://www.ndaa.org/pdf/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf) the court to order Apple to assist the government and received extensive media coverage for it. (We've covered that case here (https://www.aei.org/publication/apple-is-right-to-fight-encryption-court-order-as-congress-dithers/), here (https://www.aei.org/publication/order-for-apple-to-unlock-iphone-raises-myriad-of-technological-and-legal-questions/), and here (https://www.aei.org/publication/all-apples-writs-are-belong-to-us/) and you can read Apple's response here (http://www.scribd.com/doc/300522240/Motion-to-Vacate-Brief-and-Supporting-Declarations).)



(http://www.aei.org/wp-content/uploads/2016/03/RTX28R0L_apple-e1456846514603.jpg)

REUTERS/Dado Ruvic.

Just yesterday, a magistrate judge from the United States District Court in the Eastern District of New York issued a separate decision stating the All Writs Act did not give the court the power (http://www.politico.com/f/?id=00000153-2f2b-d640-a7fb-7fbb72380001) to order Apple to assist the government in breaking into an iPhone in a drug trafficking case — with far less media coverage. In that decision, Magistrate Judge James Orenstein concluded:

> In deciding this motion, I offer no opinion as to whether, in the circumstances of this case or others, the government's legitimate interest in ensuring that no door is too strong to resist lawful entry should prevail against the equally legitimate societal interests arrayed against it here. Those competing values extend beyond the individual's interest in vindicating reasonable expectations of privacy – which is not directly implicated where, as here, it must give way to the mandate of a lawful warrant. They include the commercial interest in conducting a lawful business as its owners deem most productive, free of potentially harmful government intrusion; and the far more fundamental and universal interest – important to individuals as a matter of safety, to businesses as a matter of competitive fairness, and to society as a whole as a matter of national security – in shielding sensitive electronically stored data from the myriad harms, great and small, that unauthorized access and misuse can cause.
>
> How best to balance those interests is a matter of critical importance to our society, and the need for an answer becomes more pressing daily, as the tide of technological advance flows ever farther past the boundaries of what seemed possible even a few decades ago. *But that debate must happen today, and it must take place among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive. It would betray our constitutional heritage and our people's claim to democratic governance for a judge to pretend that our Founders already had that debate, and ended it, in 1789*. (emphasis added).

Magistrate Judge Orenstein is exactly right. As I wrote back on January 7, 2016, before the first Apple iPhone case hit the airwaves (http://www.aei.org/wp-content/uploads/2016/01/National-commission-on-terrorists-use-of-technology-is-needed.pdf), given the complexity of the issues and the absence of an obvious right answer, Congress needs to launch a national commission to dig into the issue of terrorists' use of technology and make recommendations to Congress on the "worst-best" solutions.

We now have the benefit of two conflicting court decisions illustrating the challenges in balancing the needs of law enforcement to detect and prosecute criminal activity with the rights of the private sector to do business as it deems best, and with the rights of Americans to feel secure in their use of encryption. We know there are hundreds of other cases in which local law enforcement and the federal government want the private sector's help in breaking encrypted technology. Congress can do nothing and let the courts issue conflicting decisions on a case-by-case basis, or it can do its job by acting.

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/) | Apple is right to fight encryption court order as Congress dithers (http://www.aei.org/publication/apple-is-right-to-fight-encryption-court-order-as-congress-dithers/) | 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/)

The wisest course of action is for Congress to launch the national commission to ensure that all parties get the opportunity to fully articulate their equities, but in a manner outside of the watchful eyes and ears of our enemies. With it being a presidential election year, the national commission's work could be done by the end of the year, thereby allowing the next Congress and President to act on the recommendations. It isn't a panacea, but it is far better than piecemeal decisions from courts or impulsive congressional action should another terrorist attack occur.