REAL CLEAR POLICY

The Crypto Wars: Apple's Missed Opportunities

Patrick Eddington

March 2, 2016

In Apple's battle with the FBI over the locked iPhone 5c of deceased San Bernardino shooter Syed Farook, one thing has become very clear: Apple missed multiple opportunities to keep this matter from ever making it to court. The latest developments in the case help illustrate the point.

On February 25, Apple filed its response to Magistrate Judge Sherri Pym's order that Apple create and turn over to the FBI a "back door" that would effectively bypass the iPhone's passcode feature by allowing the government to electronically try as many passcode variants as necessary without triggering the usual data wipe that happens after ten failed passcode attempts**.** According to Apple CEO Tim Cook, this would make the hundreds of millions of iPhones and iPads around the world vulnerable to hackers or foreign spies if the malware were stolen.

A key part of Apple's argument was that if Congress wanted to legislatively mandate back doors, it would've done so by now. "Moreover, members of Congress have recently introduced three pieces of legislation that would affirmatively prohibit the government from forcing private companies like Apple to compromise data security," Apple's attorneys wrote. They specifically cited the Secure Data Act, as well as the End Warrantless Surveillance of Americans Act.

Absent from Apple's filing, however, are three similar pieces of legislation — the Surveillance State Repeal Act and amendments to the 2014 and 2015 Defense Department appropriations bills. The appropriations amendments passed the House by overwhelming bipartisan majorities each year they were offered. So what happened?

They were stripped out in conference with the Senate during final negotiations over the omnibus spending bills. Neither Apple nor its industry partners in the Reform Government Surveillance group weighed in urging the House-Senate conferees to retain the amendments, instead putting their energy into lobbying for passage of the virtually useless USA Freedom Act, which did nothing to address what has become Apple's greatest concern — the ability to truly protect its users' data.

The executive branch has spent the last two years very publicly making the case for back doors in mobile devices, with FBI Director James Comey being the leading public champion on the issue. Indeed, a leaked White House Encryption Working Group document lays out the administration's clear understanding of the pitfalls of encryption back doors even as it makes the argument for some form of them in modern electronics telecommunications systems and devices.

The legal wrangling on this issue will drag on, especially given that a federal judge in a different locked-iPhone case ruled Monday that the government's demand for a back door was unconstitutional. But simply stated, Apple and the tech industry as a whole have had ample

warning about the executive branch's intentions vis a vis encryption. They had two perfect opportunities to demand that the Senate join the House in banning government-mandated back doors, but when the moment for decisive action came, Apple and the rest of the tech industry sat on the sidelines. If they lose in court now, they will have nobody but themselves to blame — but all of us will pay the price in lost privacy and civil-liberties protections. It didn't have to be this way.

Patrick G. Eddington is a policy analyst in homeland security and civil liberties at the Cato Institute