SLATE

Remember the Apple-FBI Fight?

Julian Sanchez

April 3, 2018

As the Department of Justice relaunches its perennial campaign to demand backdoor access to encrypted data and communications, a new report from the Department of Justice's inspector general has shed unflattering light on the most famous recent battle of the long-running Crypto Wars: the FBI's aborted 2016 effort to compel Apple's assistance to unlock an encrypted iPhone.

Many privacy advocates at the time regarded the FBI's effort with a cynical eye. Though the FBI says it has thousands of encrypted phones it would like to access in connection with criminal inquiries, it chose to pick a very public fight with Apple to test a legal strategy for compelling assistance in a uniquely high-profile case: the investigation into the December 2015 terrorist mass shooting in San Bernardino, California. Even at the time, there was little reason to think much useful evidence would be gleaned from the deceased perpetrator's work-issued iPhone. The shooter had destroyed his personal phone, yet left the work-issued iPhone intact, and in any event, there was no indication the attack itself had been orchestrated or directed by any larger group.

Nevertheless, this was the occasion on which the FBI and Department of Justice decided to try out a novel and aggressive legal tactic: They sought and (initially) obtained an order under the All Writs Act of 1789, compelling Apple to assist the bureau in executing a lawful search warrant by writing and authenticating a custom version of the iOS operating system that, once installed on the deceased shooter's phone, would allow investigators an unlimited number of attempts to guess his pass code. Conspicuously, the government opted not to file its application under seal, as it routinely does, and as one might expect if it were attempting to conceal the state of investigation from potential co-conspirators. When Apple exercised its legal right to push back, DOJ ratcheted up the rhetoric, blasting the company for putting its "brand marketing strategy" above the public interest in preventing lethal terrorist attacks. There was no subtlety here: DOJ lawyers clearly hoped to leverage an emotionally charged, high-profile case to set a friendly legal precedent, garnering sympathy from legislators and the public in the process

Of course, for the government to propose pressing Apple's engineers into involuntary service, it had to establish that such conscription was the only feasible means by which they could access the phone. The Justice Department asserted as much repeatedly, claiming in its initial

application that “the assistance sought can only be provided by Apple” because the company possessed “the exclusive technical means which would assist the government in completing its search.” Variants on that claim would recur in each of the increasingly hostile legal briefs Apple and DOJ exchanged over the following month until, abruptly, the government dropped its suit, announcing that one of its outside vendors had developed an exploit that would grant it access to the iPhone after all.

Which brings us to the inspector general’s report released last week. It is the result of an inquiry opened at the urging of a senior FBI official, executive assistant director Amy Hess, who “became concerned” that the head of FBI’s cryptanalytic unit “did not seem to want to find a technical solution, and that perhaps he knew of a solution but remained silent in order to pursue his own agenda of obtaining a favorable court ruling against Apple.” That should, in itself, seem rather extraordinary. And what the IG found suggests her concerns were well founded: The FBI unit tasked with breaking into the San Bernardino iPhone had made only halfhearted efforts to solicit help from other units, stressing that the information was sought for a criminal investigation—which was internally perceived as discouraging other units from offering up classified intelligence tools that might be exposed in a criminal court proceeding. It was only days before DOJ filed its request to compel Apple’s assistance that a broader request for “any” method—classified or unclassified—was circulated.

As the IG explains, the head of FBI’s Remote Operations Unit, another part of the bureau’s Technical Surveillance section, had known all long that one of its outside vendors was 90 percent done with an exploit that would have obviated the need to compel help from Apple. In response to this final request for “any” method, the ROU chief finally requested that the outside vendor prioritize work on that exploit—which they finished in just a few weeks.
And yet, far from celebrating this development, the ROU chief described the head of FBI’s cryptanalysis unit as “definitely not happy” that its perfect test case—the lawsuit Hess had described as the “poster child” in the FBI’s legal fight against unbreakable encryption—had to be abandoned.

Technically, the IG report absolves the FBI and DOJ of formal wrongdoing: The officials pushing the legal campaign to conscript Apple had not had concrete knowledge of an alternative way into the iPhone when the Justice Department made its representations that Apple’s assistance was necessary. Technically, DOJ lawyers had not lied to the court, and then–FBI Director James Comey had not lied in testimony to Congress, when they claimed that the FBI had no method to access the phone absent Apple’s help. But the inescapable impression left by the report is that they did not know because they did not care to. Here, finally, was the ideal case: not some petty drug dealer but a terrorist shooter who’d left stacks of bodies in his wake. The courts, cowed by the invocation of national security, would be at their most deferential; the public, at its most skittish. Legislators of both parties would dutifully lambast Apple for placing corporate profits over the need to prevent terrorist attacks. It was a public relations opportunity too perfect to squander by finding some mundane technical solution—and so only the most cursory effort was made to do so. If the government had considered it as urgent to access the iPhone as it pretended in its court filings—urgent enough to put out a clear request for methods

at the outset—it seems likely it could have had its solution well before the date it first turned to the courts.

None of this is to suggest FBI officials aren't sincere in their more general belief that it's vital it be granted some legal mechanism for "exceptional access" to encrypted communications. But the IG's report provides good reason to regard some of their more sensational arguments with a healthy dose of skepticism.

Julian Sanchez is a senior fellow at the Cato Institute.