In the Wake of FBI vs Apple...

By Gregory Peterson, JD

When the U.S. Dept. of Justice obtained a court order compelling Apple Inc. to assist FBI agents in cracking an iPhone 5C used by San Bernadino terrorist Syed Rizwan Farook, the stage was set for controversy. So when Apple refused to comply, long-simmering concerns quickly came to the fore. *At issue: Balancing the dynamic — and often competing — issues of privacy, law enforcement, and security.*

In the weeks that followed the court's order, Americans engaged in a spirited public conversation. Social media, editorial pages, television and radio talk shows all were consumed by a debate between ardent (and seemingly irreconcilable) views.

Then, on March 29th, the U.S. v Apple controversy came to an abrupt halt — when the DOJ filed a status report in the US District Court, asking the court to vacate its order. This status report stated:

> The government has now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple Inc. mandated by the court's original order.

With that document, the FBI ended the case — leaving many questions (and no legal precedent) in its wake.[1]

In the Wake of the Standoff...

With FBI vs Apple now behind us, there has been no landmark court decision offering clear guidance and setting legal precedent for similar matters yet to come. Nevertheless, this highly visible dispute has advanced the discourse, altered the policy landscape, and spurred technological developments related to privacy, encryption, and security matters. Among these significant changes:

---

[1] "The Anti-Climactic End to Apple v. DOJ" Lawyerist (https://lawyerist.com/107208/anti-climactic-end-apple-v-doj/)

1) Increased public awareness of government surveillance, encryption technology, data privacy practices, and cybersecurity practices.

When Edward Snowden's extensive disclosures of classified government documents became front-page news in 2013, Americans gained a new understanding about the extent of domestic surveillance activities. Although U.S. v Apple's underlying fact pattern is markedly different from the Snowden matter, this recently concluded case has similarly invigorated public awareness of privacy issues.

The U.S. v Apple case took discussions about encryption out of the "geek" realm and made these concerns an issue for everyday people. Issues that once seemed abstract and intangible were suddenly real, and close-to-home. With so personal a device at the heart of this dispute, these once-abstract matters became issues the public could grasp — both literally and figuratively. What's more, these issues could come to mind every time a iPhone user answered a call, sent a text, or accessed an app.

2) Greater knowledge (both in law-breakers and lawmakers) about the iPhone's encryption capability and vulnerability

For years, the iPhone has enjoyed an industry-leading reputation for protecting digital communications. After this year's highly publicized court case, however, questions have been raised about the newly disclosed chink in the iPhone (the 5C model, at least) encryption armor. The case's broader issues, however, transcend any particular manufacturer, mobile device, or software platform; these matters are relevant to every citizen, every consumer, every technology company, and every government.

3) A renewed intensity in the "arms race" for encryption (and breaking encryption)

There's an "arms race" among the players with a stake in the outcome of the ongoing contest between privacy interests and security interests. Technology manufacturers; government bodies; hackers; privacy advocates; foreign governments; law-enforcement agencies; businesses; and private citizens all have a portfolio of interests in how the encryption battles ultimately are resolved. Apple (which has promoted its brand's resistance to hacking) has every incentive to quickly discover the vulnerability that allowed its iPhone to be hacked — and to develop yet stronger encryption algorithms. Similarly, other technology companies (some of which filed amicus briefs in support of Apple) are striving to improve their encryption capabilities.

4) Growing concerns among law enforcement and national security agencies

Unlike tech companies and privacy advocates, law enforcement and national security personnel see compelling interests in being able to *defeat* encryption. These officials express growing concerns about the number of companies “going dark" (engaging in cybersecurity practices that effectively prohibit outside intrusions — both from cyber-criminals *and* law enforcement agents).

"It remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety, either with cooperation from relevant parties or through the court system when cooperation fails," DOJ's spokeswoman Melanie Newman said. "We will continue to pursue all available options for this mission, including seeking the cooperation of manufacturers and relying upon the creativity of both the public and private sectors." [2]

5) Action in Congress — as well as the courts

“This conflict is not over; there will be another case. At some point, the courts are going to have to decide," said Fred Kaplan, Slate columnist and author of “The Dark Territory: The Secret History of Cyber War."

Meanwhile, there is a growing sentiment that encryption and privacy issues should be settled by elected officials — not by courts. Consequently, encryption matters now are gaining ascendency on Congressional agendas. Two bills, in particular, are under discussion:

The McCaul/Warner bill (considered to be a “moderate" approach) proposes establishment of a commission — composed of experts in technology, civil liberties and law enforcement — to make policy representations. (Co-sponsors are House Homeland Security Committee Chairman Rep. Michael McCaul (R-Texas) and Senate Intelligence Committee member Sen. Mark Warner (D-Virginia).

The Burr/Feinstein bill, in contrast, would seek to provide federal judges with the power to compel tech companies to assist law enforcement agencies in accessing encrypted data.

---

[2] “The FBI Has Successfully Unlocked The iPhone Without Apple's Help” National Public Radio http://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help

(A recent story in Reuters[3] reported that the proposed legislation does not create specific penalties for non-complying companies — leaving this discretion to individual judges.)

Which bill is more likely to gain traction? Here's one view:

> "The Burr/Feinstein bill, which is sure to be widely reviled by the tech industry, digital rights advocates, and reasonable policymakers alike, is likely to be the poster child for just the sort of knee-jerk legislative response that the commission idea is intended to block." Kevin Bankston, Director of the Open Technology Institute[4]

(Also worth noting: The House Energy and Commerce Committee and the Judiciary Committees recently formed a joint working group on encryption.)

Although the San Bernadino iPhone case now is off the front pages, the encryption issues raised by U.S. vs Apple are far from being resolved. "...There's every reason to expect that there will be another phone with a similar issue very soon... There's already a bunch of other phones on lesser cases that are in dispute right now. Everyone expects that this fight will only continue." Devlin Barrett, who covers the Justice Department for *The Wall Street Journal.*[5]

For the time being, anyone with an older version iPhone (the 5C) should know this: At present, it is unclear whether the hackers exploited a software bug or discovered a flaw in that particular phone's hardware design. What is clear? At least one third party (and now, the FBI) has the ability to thwart the encryption on the iPhone 5C device. Unless and until Apple has a way to "patch" this vulnerabilities...Time will tell.

# # #

---

[3] "Senate proposal on encryption gives judges broad powers" Reuters, Mar 21, 2016 (http://www.reuters.com/article/us-apple-encryption-legislation-)

[4] "A Tale of Two Encryption Bills," Morning Consult (https://morningconsult.com/2016/03/a-tale-of-two-encryption-bills/)

[5] "FBI cracks the locked iPhone, but legal questions remain unanswered" PBS News Hour with Gwen Ifill (http://www.pbs.org/newshour/bb/fbi-cracks-the-locked-iphone-but-legal-questions-remain-unanswered/)