The Intercept_

FBI vs. Apple Establishes a New Phase of the Crypto Wars

Dan Froomkin and Jenna McLaughlin

February 26, 2016

For over two decades, the battle between privacy-minded technologists and the U.S. government has primarily been over encryption. In the 1990s, in what became known as the Crypto Wars, the U.S. tried to limit powerful encryption – calling it as dangerous to export as sophisticated munitions — and eventually lost.

After the 2013 Snowden revelations, as mainstream technology companies started spreading encryption by putting it in popular consumer products, the wars erupted again. Law enforcement officials, led by FBI Director James Comey, loudly insisted that U.S. companies should build back doors to break the encryption just for them.

That won't happen because what these law enforcement officials are asking for isn't possible (any back door can be used by hackers, too) and wouldn't be effective (because encryption is widely available globally now). They've succeeded in slowing the spread of unbreakable encryption by intimidating tech companies that might otherwise be rolling it out faster, but not much else.

Indeed, as almost everyone else acknowledges, unbreakable encryption is here to stay.

Tech privacy advocates continue to remain vigilant about encryption, actively pointing out the inadequacies and impossibilities of the anti-encryption movement, and jumping on any sign of backsliding.

But even as they have stayed focused on defending encryption, the government has been shifting its focus to something else.

The ongoing, very public dispute between Apple and the FBI, in fact, marks a key inflection point — at least as far as the public's understanding of the issue.

You might say we're entering the Post-Crypto phase of the Crypto Wars.

Think about it: The more we learn about the FBI's demand that Apple help it hack into a password-protected iPhone, the more it looks like part of a concerted, long-term effort by the government to find new ways around unbreakable encryption — rather than try to break it.

The Court Order

The court order Apple is fighting would require it to come up with a new way to hack into an iPhone 5c belonging to San Bernardino killer Syed Rizwan Farook.

The fact is that Apple couldn't break the encryption scrambling the phone's data if it tried. But the FBI doesn't have to worry about that if it can just open the phone with the right password.

As Apple CEO Tim Cook put it, in his rebellious public response to the court order: "the 'key' to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it.'"

And it's those protections that are now under siege.

This is not a sudden move for the government. As Bloomberg News recently reported, President Obama's National Security Council last fall shaped a secret "decision memo" requesting government agencies to find both technical and legal ways to skirt encryption instead of break it.

They were instructed to figure out how much each option would cost, whether there were any laws that might need changing – and to report back.

According to a *Washington Post* story in September, an Obama administration working group spent months coming up with a list of technological methods to defeat encryption. One idea — particularly abhorrent to computer security professionals — was to force companies to send malware to suspects' phones using automatic software updates.

And despite Comey's constant complaint that law enforcement is "going dark" because of encryption, the FBI has been developing and purchasing viruses, Trojan horses, and other forms of malware to help break into digital devices – and in that way get around unbreakable encryption — for years.

They don't like to talk about it. The FBI "routinely identifies, evaluates, and tests potential exploits in the interest of cyber security," FBI spokesman Christopher Allen wrote in an email to *The Intercept* in September.

But the public record shows that the FBI has been physically hacking into computers since at least 2001, when it put a keystroke-logger on "Little Nicky" Scarfo's computer during an investigation of the American Mafia investigation.

These days, the FBI uses its own brand of malware called the Computer and IP Address Verifier (CIPAV). In 2007, agents tricked a high school kid in Washington into downloading it and exposing his identity when he was making bomb threats. The FBI has consulted with outside shops too, including the Italian firm Hacking Team—whose emails were leaked last summer, exposing their business dealings.

"I think that for many within law enforcement, the priority is to access data, point blank. That could mean installing backdoors directly into encryption standards or finding some kind of workaround," Andrea Castillo, the technology policy program manager for the Mercatus Center at George Mason University, wrote in an email to *The Intercept.*

"The first strategy failed in the court of public opinion, so it appears that they are now attempting more covert methods to get around encryption. Unfortunately, there are major security risks with both approaches," she said.

National Security Agency director Admiral Mike Rogers seems to already be pivoting away from the idea that we need to get rid of unbreakable encryption. He said in January that encryption is here to stay—and that "spending time arguing" about it is "a waste of time." When pushed by Yahoo News's Michael Isikoff on whether or not encryption is a crippling threat to the intelligence community, he deflected, suggesting that it's a bigger issue for domestic local law enforcement.

And documents in the Snowden archive show the NSA has spent years actively trying to hack Apple products and mobile devices. Its efforts to hack the iPhone date back to 2006, before it was even unveiled.

A Big Con?

"Over the past few months, I've been wondering why it is the FBI has been pushing so hard in the public forum to advocate for backdoors when almost everyone, from technologists to the tech industry to civil society to Congress, has been opposed to such an approach," Ryan Hagemann, technology and civil liberties policy analyst for the Niskanen Center wrote in an email to *The Intercept.*

"I think what we're seeing unfold here is part of a multi-pronged strategy by law enforcement, possibly with the tacit approval and support of the intelligence community."

Hagemann said the way the FBI is pursuing is much more dangerous than any legislative route. "I think we should be more fearful of the strategy the FBI is using in the courts to push their ill-advised and Constitutionally dubious agenda."

Julian Sanchez, a senior fellow at the Cato Institute, recently proposed that the government's strategy all along has been to use the push for backdoors into encryption as "a feint".

Writing for the national security law blog Just Security, Sanchez speculated that "the threat of a costly fight over legislation, even if unlikely to become law, maybe largely geared toward getting Silicon Valley, or at least a critical mass of companies, to adopt a more cooperative posture. " That means "quietly finding ways to accommodate the government".

Sanchez concluded that when the government finally admits the obvious – and gives up on fighting unbreakable encryption – it will demand some sort of "compromise" legislation.

Sanchez imagined "privacy groups celebrating a victory" when that happens, "while intel officials snicker into their sleeves at a 'defeat' according to plan."