The Right to Privacy is Sacrosanct unless you live in a Big Brother State -- Welcome to America

by Michael Riley & Jordan Robertson via james - Bloomberg *Monday, Feb 22 2016, 6:03am*
international / prose / post

Secret Memo Details US' Broader Strategy to Crack Phones

> Silicon Valley celebrated last fall when the White House revealed it would not seek legislation forcing technology makers to install "backdoors" in their software -- secret listening posts where investigators could pierce the veil of secrecy on users' encrypted data, from text messages to video chats. But while the companies may have thought that was the final word, in fact the government was working on a Plan B.

In a secret meeting convened by the White House around Thanksgiving, senior national security officials ordered agencies across the U.S. government to find ways to counter encryption software and gain access to the most heavily protected user data on the most secure consumer devices, including Apple Inc.'s iPhone, the marquee product of one of America's most valuable companies, according to two people familiar with the decision.

The approach was formalized in a confidential National Security Council "decision memo," tasking government agencies with developing encryption workarounds, estimating additional budgets and identifying laws that may need to be changed to counter what FBI Director James Comey calls the "going dark" problem: investigators being unable to access the contents of encrypted data stored on mobile devices or traveling across the Internet. Details of the memo reveal that, in private, the government was honing a sharper edge to its relationship with Silicon Valley alongside more public signs of rapprochement.

On Tuesday, the public got its first glimpse of what those efforts may look like when a federal judge ordered Apple to create a special tool for the FBI to bypass security protections on an iPhone 5c belonging to one of the shooters in the Dec. 2 terrorist attack in San Bernardino, California that killed 14 people. Apple Chief Executive Officer Tim Cook has vowed to fight the order, calling it a "chilling" demand that Apple "hack our own users and undermine decades of security advancements that protect our customers." The order was not a direct outcome of the memo but is in line with the broader government strategy.

White House spokesman Josh Earnest said Wednesday that the Federal Bureau of Investigation and Department of Justice have the Obama administration's "full" support in the matter. The government is "not asking Apple to redesign its product or to create a new backdoor to their products," but rather are seeking entry "to this one device," he said.

Security specialists say the case carries enormous consequences, for privacy and the competitiveness of U.S. businesses, and that the National Security Council directive, which has not been previously reported, shows that technology companies underestimated the resolve of the U.S. government to access encrypted data.

"My sense is that people have over-read what the White House has said on encryption," said Robert Knake, a senior fellow at the Council of Foreign Relations who formerly served as White House Director of Cybersecurity Policy. "They said they wouldn't seek to legislate 'backdoors' in these technologies. They didn't say they wouldn't try to access the data in other ways."

"Backdoors" refer to security holes that are intentionally inserted into software to create the equivalent of a skeleton key for law enforcement -- what wiretapping systems are for telephone lines, for instance. The problem with backdoors in computer networks is they create vulnerabilities for any hacker to find.

What the court is ordering Apple to do, security experts say, does not require the company to crack its own encryption, which the company says it cannot do in any case. Instead, the order requires Apple to create a piece of software that takes advantage of a capability that Apple alone possesses to modify the permanently installed "firmware" on iPhones and iPads, changing it so that investigators can try unlimited guesses at the terror suspect's PIN code with high-powered computers. Once investigators get the PIN, they get the data.

Knake said that the Justice Department's narrowly crafted request shows both that FBI technical experts possess a deep understanding of the way Apple's security systems work and that they have identified potential vulnerabilities that can provide access to data the company has previously said it can't get.

In this case, the government wants Apple's help in exploiting such weaknesses. But experts say they could find ways to do it themselves, and the NSC "decision memo" could lead to more money and legal authorization for a smorgasbord of similar workarounds.

National Security Council spokesman Mark Stroh declined to comment on the memo. But he provided a statement from a senior Obama administration official: "We should not preemptively conclude that technical and policy options to address this challenge are out of reach. While creating mechanisms for accessing encrypted information does create vulnerabilities, there may be technical and process steps that can be implemented to limit such risks."

The memo was approved by the NSC's Deputies Committee, according to the people familiar with it. While the deputies' committee changes depending on the subject matter, it typically includes at least a dozen sub-cabinet level officials, among them the deputy attorney general, the vice chairman of the joint chiefs of staff, and the deputy national security adviser.

Such memos can have lasting impact. A similar decision memo was used in the early years of the Iraq war to address the problem of Improvised Explosive Devices, which were then killing hundreds of U.S servicemen. The response ultimately led to new anti-IED technology and expanded intelligence capabilities to disrupt the cells building and planting the bombs.

Silicon Valley and Washington have had a decades-long distrust of each other over encryption, stemming from a failed Clinton administration push in the 1990s for a government backdoor in telecommunications networks. In that case, the National Security Agency developed a technology called the Clipper Chip, which the White House approved as a government standard. Security experts assailed it as insecure and a violation of privacy.

Security experts say the U.S.'s insistence on finding ways to tap into encrypted data comes in direct conflict with consumers' growing demands for privacy.

"The government's going to have to get over it," said Ken Silva, former technical director of the National Security Agency and currently a vice president at Ionic Security Inc., an Atlanta-based data security company. "We had this fight 20 years ago. While I respect the job they have to do and I know how hard the job is, the privacy of that information is very important to people."

In addition to the demands against Apple, the FBI will almost certainly seek more money and expanded legal authorization to track suspects and access encrypted data, without the involvement of companies that make the technologies, several experts say. Intelligence services already have sophisticated tools for cracking encryption, and the White House's efforts will likely lead to broader use of those techniques across the government, even in ordinary criminal investigations that don't involve foreign intelligence or national security.

The workarounds could involve trying to force companies like Apple to develop their own tools to help law enforcement or enlisting government hackers to find previously unknown software vulnerabilities that enable the decryption of large amounts of data flowing across networks.

Apple infuriated law enforcement when it announced in 2014 that it would encrypt data stored on users' iPhones and iPads with a PIN code that the company could not access, even if ordered to by a judge. Prior to that decision, the FBI and local police agencies routinely sent seized devices to Apple to extract data relevant to their investigations.

To security experts, creating hacking tools -- capabilities to gain access to encrypted data -- is simply a matter of money and focused effort.

"My guess is you could spend a few million dollars and get a capability against Android, spend a little more and get a capability against the iPhone. For under $10 million, you might have capabilities that will work across the board," said Jason Syversen, a former manager of advanced cyber security programs at the Defense Advanced Research Projects Agency (DARPA), and now the CEO and co-founder of Siege Technologies in Manchester, New Hampshire.

This week's federal court order undermines years of effort by Apple to design a system that makes accessing encrypted data impossible without the participation of the phone's legitimate user. Company officials appeared to believe the enhanced encryption would remove Apple from the efforts of any government to sabotage the security of their customers. Instead, federal agents have detailed in a public document several ways in which that encryption can be bypassed.

"Apple has two options now: They can go back to the judge and say this isn't possible. Or they can service the warrant," said James Lewis, a senior cyber security fellow at the Center for Strategic and International Studies in Washington. "I don't think they can say it's not possible, because it looks like it is."

http://www.bloomberg.com/news/articles/2016-02-19/secret-memo-details-u-s-s-broader-strategy-to-crack-phones

---

Jungle Drum Prose/Poetry. http://jungledrum.lingama.net/news/story-2129.html