

《美国成功解锁苹果手机，避免法律诉讼》

美国成功解锁苹果手机，避免法律诉讼

??

SAN FRANCISCO - The US Justice Department said on Monday it had succeeded in unlocking an encrypted iPhone used by one of the San Bernardino shooters and dropped its legal case against Apple, ending a high-stakes legal battle but leaving the broader struggle over encryption unresolved.

The abrupt end to a confrontation that had transfixed the tech industry was a victory for Apple, which vehemently opposed a court order obtained by the Justice Department that would have required it to write new software to get into the iPhone.

But the larger fight over law enforcement access to encrypted information is by no means over. The technology industry is adamant that anything that helps authorities bypass the security features of tech products will undermine security for everyone.

Government officials are equally insistent that all manner of criminal investigations will be crippled without access to phone data.

At issue in the Apple case was a county-owned iPhone used by Rizwan Farook, one of the husband-and-wife shooters in the December rampage in San Bernardino, California, in which 14 people were killed and 22 wounded. The couple died in a shootout with police after the attack.

After saying for weeks in court filings and congressional testimony that Apple possessed the "exclusive technical means" to unlock Farook's phone, the Justice Department unexpectedly announced on the eve of a court hearing last week that an unidentified outside party had presented it with a technique that might open the phone without help from Apple.

In a two-page court filing on Monday, the Justice Department said the government had "successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple." It asked a federal magistrate in Riverside, California, to withdraw the order compelling Apple to assist.

Apple had argued that the government request and resulting court order were a massive overreach that would give courts unlimited authority to force private companies to work as their agents. It argued that Congress had specifically declined to give the government such powers when it comes to electronic surveillance and data collection.

Tech industry leaders including Google, Facebook and Microsoft and more than two dozen other companies filed legal briefs supporting Apple. The Justice Department received support from law enforcement groups and six relatives of San Bernardino victims.

Apple had no immediate comment on Monday.

THORNY ISSUES

The Justice Department's apparent discovery of an iPhone hacking technique presents thorny questions about how that knowledge will be shared.

If the government tells Apple about the details, the company would presumably fix whatever vulnerability was used and thus render the method ineffective. If the government withholds the information, Apple could face a public perception problem about the security of its phones.

There are also a number of pending cases across the country where law enforcement officials are asking for access to iPhones. It is not clear if they will have access to the break-in technique.

In one New York case, Justice Department officials have to respond by Tuesday to an Apple request to delay the proceedings. That could provide clues as to how the government intends to deal with other iPhone cases.

On a conference call for reporters on Monday, a senior US law enforcement official said it was too soon to say whether the government's technique would work on other iPhones, or if it would share information with Apple or other law enforcement agencies.

The official also declined to elaborate on what party provided the solution, except to say it did not come from within the US government. He also declined to comment on what had been found on the San Bernardino phone.

'ALL AVAILABLE OPTIONS'

The Justice Department suggested on Monday it would keep seeking unorthodox means of getting information, including through the courts when needed.

"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," Justice Department 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."

On Capitol Hill, critics of the Justice Department's efforts called for further vigilance.

"Those worried about our privacy should stay wary - just because the government was able to get into this one phone does not mean that their quest for a secret key into our devices is over," said Representative Darrell Issa, a California Republican who sits on the House Judiciary Committee.