New Court Decision: The FBI, Apple & the Company that Broke iPhone Encryption

Last year – Apple battled in court with the FBI in the aftermath of the massacre in San Bernardino, California. The FBI obtained a court order in February 2016 directing Apple to furnish an encryption key so that law enforcement could access the iPhone of the killer. The court case raged in federal court until the FBI purchased a software tool from an Israeli company that broke the iPhone's encryption security. The court case became moot because the FBI successfully hacked the iPhone without Apple's assistance.

For further background, my presentation about this important privacy and national security issue in 2016 about the case can be seen here, and my slides can be found here.

> *"The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand. This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake."*

— "A Message to our Customers" by Tim Cook, CEO of Apple, that summed up Apple's position

Last week – A federal court denied a request by the Associated Press to obtain information about the Israeli company, the price the FBI paid, and details about the tool. AP had asked the FBI under the Freedom of Information Law to provide the information. When the FBI refused, AP sued the FBI to compel it to produce the information.

AP unsuccessfully asked Judge Tanya S. Chutkan in the District of Columbia to rule that the information should be made public in accordance with FOIL and for public policy reasons.

The court was persuaded by the FBI's claims that the identity of the vendor and the cost of the tool relate to intelligence activities or intelligence sources or methods. According to the government, releasing the vendor's identity could allow foreign or terrorist adversaries to use existing public technology created by the vendor to probe for weaknesses, develop exploits, and create better encryption technology to thwart the FBI's ability to use the tool.

The FBI also expressed its grave concerns that if it identified the vendor, its classified intelligence source and method would be revealed. This could put national security at risk. Moreover, the government argued that the vendor's computing systems and technology could become vulnerable to hacking if it released the vendor's name.

As far as disclosing the price that the FBI paid to the vendor for the tool, the judge agreed with the FBI's position that adversaries might be able to learn how important the US government considers the technology and also may allow them to estimate the FBI's budget for cybersecurity.

> *"'Minor details of intelligence information,' like the price paid for the iPhone hacking tool, 'may reveal more information than their apparent insignificance suggests because, much like a piece of jigsaw puzzle, each detail may aid in piecing together other bits of information…. the court finds that this is an adequate justification for withholding the vendor's identity…and purchase price."*

Importantly, the court agreed with the FBI that the iPhone hacking tool is both an intelligence source and also an intelligence method. The court sided with the FBI, ruling that it could use the iPhone unlocking technology in future law enforcement activities, making the tool itself a law enforcement technique.

The battle to encrypt devices and data to fend off hacking has only just begun. Stay tuned.

Associated URL: NEW COURT DECISION: THE FBI, APPLE & THE COMPANY THAT BROKE iPHONE ENCRYPTION