**“Should Citizens Side with Apple or the FBI in the San Bernardino iPhone case?”**

*The Washington Post*

By Evan Osnos

Earlier this week, a federal judge ordered Apple to assist the FBI in hacking into the iPhone used by one of the ISIS-inspired San Bernardino shooters. The case involves an FBI request for Apple’s assistance in opening a phone once carried by Syed Rizwan Farook, who with his wife was responsible for the terrorist attack in San Bernardino, California, that left 14 dead and 22 wounded. But Apple has said it will fight this order in court.

On one level, this should be comfortable space for the government. First, the phone is owned by the County of San Bernardino, which issued it to Farook, an employee of its health department. The county, as Apple’s customer, has no problem having its phone unlocked. Second, Farook and his wife were killed in a gun battle with the police four hours after the shooting last December. Under the law, deceased individuals have no privacy rights.

But Apple is taking a stand because the government wants it to create something against its will: code that would disable a feature that erases all content after 10 failed password attempts. The company contends the government’s request would create a “back door” into iPhones that would allow authorities to access private data whenever they wished. “It would be the equivalent of a master key, capable of opening hundreds of millions of locks” and “undermine the very freedoms and liberty our government is meant to protect,” Apple CEO Tim Cook said in an open letter to customers. Cook argues that if Apple cooperates, the floodgates will open to similar law enforcement requests, putting customers’ data at risk.

Many technology experts similarly argue that the FBI wants to set a precedent that tech companies will assist law enforcement in breaking their users’ security, and the technology community is afraid that the precedent will limit what sorts of security features it can offer customers. The tech community, these experts say, sees this as a security verses surveillance debate.

But the FBI sees it as a privacy verses security debate. The phone in the San Bernardino case stopped uploading data to the cloud about six weeks before the killings. That suggests there may be information inside the device that was deliberately concealed. That could include the identities of terrorists who influenced or directed the attack. Such information could prevent future plots and ensure national security. “Maybe the phone holds the clue to finding more terrorists. Maybe it doesn’t. But we can’t look the survivors [of the San Bernardino attack] in the eye, or ourselves in the mirror, if we don’t follow this lead,” said FBI Director James Comey. “I

hope folks will remember what terrorists did to innocent Americans at a San Bernardino office gathering and why the FBI simply must do all we can under the law to investigate that," he continued. "The San Bernardino litigation isn't about trying to set a precedent or send any kind of message. It is about the victims and justice."

But the tech industry doesn't agree. What the FBI wants to do would make citizens less secure, they argue, even though it is in the name of keeping those same individuals safe from harm. Powerful governments, democratic and totalitarian alike, want access to user data for both law enforcement and social control, they say.

"Either everyone gets security or no one does. Either everyone gets access or no one does. The current case is about a single iPhone 5c, but the precedent it sets will apply to all smartphones, computers, cars and everything the Internet of Things promises," states Bruce Schneier, a data security expert. If Apple cooperates with the FBI's request, it will reduce the security of everything that is and will be computerized, most importantly users' personal data. "The FBI may be targeting the iPhone of the San Bernardino shooter, but its actions imperil us all," Schneier argues.

Political pundits are suspicious of this line of reasoning, though. They have argued that the most powerful and influential tech companies like Apple, Google, and Facebook have access to incredible amounts of user data—in some cases, far more personal than the information the federal government has access to. Democrats and Republicans alike question why tech users aren't more concerned about how these companies use their personal information.

In early 2018, for example, Facebook came under scrutiny for the misuse of personal information from as many as 50 million users. It was reported by *The New York Times* that the social media giant had allowed a third-party analytics firm to harvest personal data from Facebook users' profiles without their consent and use it for political advertising purposes. The company's stock plummeted as a result, and Facebook CEO and founder Mark Zuckerberg was forced to testify in front of Congress. During his testimony, Zuckerberg said of the scandal that "it was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here." This episode, along with recent others, seem to represent a breach of trust between tech companies and their users. But, as these pundits question, it remains to be seen if users start to feel taken advantage of by companies whose products they continue to purchase.

To make matters worse, in January 2020, following another domestic terror attack in Florida, current Attorney General William Barr publicly requested Apple to provide access to two phones used by the gunman. Barr's appeal signaled the escalation in an ongoing fight between the Justice Department and Apple pitting personal privacy against public safety. Many in

government have sided with Barr and the Justice Department. “Companies shouldn’t be allowed to shield criminals and terrorists from lawful efforts to solve crimes and protect our citizens,” Senator Tom Cotton, Republican of Arkansas, said in a statement. “Apple has a notorious history of siding with terrorists over law enforcement. I hope in this case they’ll change course and actually work with the FBI.”

The company and its defenders responded by citing that data privacy is a human rights issue. If Apple developed a way to allow the American government into its phones, its executives argued, hackers or foreign governments like China would exploit the tool.