Directions:

 1 – Highlight areas which confuse you and about which you want clarification.

 2 – Demonstrate evidence of a close reading, by providing reactions, questions, and mini-summaries

Here's Apple's best argument against hacking the San Bernardino shooter's iPhone

Updated by Timothy B. Lee on February 26, 2016, 9:40 a.m. ET tim@vox.com

Apple has filed its official reply to the FBI's demand that it write software to help the bureau access the iPhone of San Bernardino terrorism suspect Syed Farook. Consistent with its earlier public statements, Apple condemns the FBI's request as an unprecedented expansion of government power that would endanger the privacy of Apple users. I expressed some skepticism of this argument last week, but I found Apple's latest response pretty persuasive.

One danger is that an FBI win could set a legal precedent that puts us on a slippery slope to the routine use of smartphones for government surveillance. If Apple can be compelled to update the software on a dead suspect's iPhone to help the FBI access encrypted data, it's not obvious why the company couldn't also be compelled to modify the software on a live suspect's iPhone to listen in on his conversations or track his location.

But let's say you're confident that the courts can draw a reasonable distinction between the FBI's current request to unlock an encrypted iPhone and more outlandish surveillance scenarios. There's still a big practical problem that the FBI and its allies haven't really grappled with.

iPhone hacking software will be a magnet for bad guys

Every new version of the iPhone operating system goes through an extensive testing process before it's signed by Apple. That's critical because an iPhone will refuse to install software updates that haven't been mathematically blessed by Apple. Given how dangerous it would be if someone tricked Apple into signing malware, we can assume that Apple takes extreme precautions to make sure that doesn't happen.

But it will be hard for Apple to maintain high security standards if it is forced to create the hacking software the FBI has demanded. In its legal filing, Apple notes that "there are hundreds of demands to create and utilize the software waiting in the wings. If Apple creates new software to open a back door, other federal and state prosecutors — and other governments and agencies — will repeatedly seek orders compelling Apple to use the software to open the back door for tens of thousands of iPhones."

Manhattan District Attorney Cyrus Vance alone has said there are at least 175 iPhones he'd like to have unlocked.

Apple argues that if it is forced to create a hacked version of its software, that would "force Apple to take on the task of unfailingly securing against disclosure or misappropriation the development and testing environments, equipment, codebase, documentation, and any other materials relating to the compromised operating system."

The statement continued: "Given the millions of iPhones in use and the value of the data on them, criminals, terrorists, and hackers will no doubt view the code as a major prize and can be expected to go to considerable lengths to steal it, risking the security, safety, and privacy of customers whose lives are chronicled on their phones."

We can assume that once Apple created the iPhone hacking software the FBI wants, hackers and foreign intelligence agencies would work to gain access to it. We can also expect that foreign governments will try to hack into the database Apple uses to track these requests — just as China hacked into a Google database that tracked Gmail surveillance requests. They might try to impersonate obscure local law enforcement agencies and submit forged court orders. Apple would need to hire new employees to process and investigate the growing volume of law enforcement requests — which would mean more people who could be subject to bribery or blackmail.

Apple is a sophisticated company with a lot of security expertise. Maybe it will be able to withstand all these attacks and emerge with users' privacy unscathed. But it's a pretty big risk to take.

Directions for reflections:

Write three one-paragraph reflections, each one placing the issue in a different context. Label each paragraph according to its context. Choose from the list of contexts below:

Cultural Health & Safety Social

Academic Generational Economic

Historical Religious Environmental

Political Moral Medical

Gender Legal Self-expression