In the wake of Apple’s very public statement regarding their denial of the FBI’s request for an iPhone security backdoor, much of the pixel-staring public is up in arms, and rightfully so. This debate is not as simple as security vs. privacy, though, and is more of a sea of rhetoric from two sides with one really trying to get what they want. Some devout patriots insist that the Bureau can and will use a backdoor security breach on the (deceased) San Bernardino shooter’s iPhone. As we can recall from earlier chapters of study, this is the argument from authority logical fallacy – insisting that authority knows best and will do best for us simply because they are authoritative. This is a very shortsighted outlook, as the FBI’s request(s) to Apple, were they to have their way, enable a lot of villainy from those inside and outside of U.S. borders. Those viewing things in a much more logical sense see some very inherent flaws with this plan, as the request does not call for a traditional backdoor. The FBI is requesting – well, more demanding, given the legal arms being drawn – that apple developers create a tool which goes around the iPhone feature that deletes all the phone’s information after ten failed password attempts.

Doesn’t sound so bad, right? Not a direct fast lane into the phone, right? Well, if you’ve got your hands on that hypothetical tool, there’s a great chance that you’re already aware and capable of the concept of brute force hacking, and circumventing the data deletion means you can automate a program to attempt each four digit password on any given iPhone until you’ve found your way into it. The potential for misuse is astronomical, especially if the tool was to reach other law enforcement agencies or clandestine groups and individuals with ill intent.
“What’s important to understand about the San Bernardino iPhone case is that its very existence is a public relations maneuver” states Brian Barrett in the wired.com article. Nate Cardozo, an attorney with the Electronic Frontier Foundation, claims that the FBI chose the case very carefully to work their request / demand for backdoor architecture. The fact that it’s a terrorism case stands to lend sympathy to law enforcement. This certainly seems to go beyond unlocking a single dead man’s iPhone (the Bureau already knows how he came to arm himself and who he was in contact with), but sets a precedent of compliance with law enforcement going forward with breaking down encryption for the sake of “security” and granting the FBI an insanely powerful tool to access certain metadata on any of millions of devices in the hands of both U.S. citizens and other nationals.

For what it’s worth, of course, the security that U.S. citizens receive from the FBI having this tool is pretty much in the negatives. At very least, its acute use in the San Bernardino investigation (lest we forget that’s their platform for demanding it) does essentially nothing for national security. The assailant is dead and his network is already known. Any outgoing metadata within U.S. borders already exists to be collected and analyzed, his phone’s MAC address is known, his iCloud backup exists for all data the phone has seen barring some weeks before the shooting took place. When we place a passcode on our cellphones, we assume that our most personal data and intellectual property (IP) – intangible creative ideas and work – stands safely behind encryption and at very least four little numbers. This very pliable backdoor would be functional not just on the iPhone 5C model but any iPhone running iOS 8.0 or later. It’s simply too easy for the method behind this tool to be replicated and fall into the wrong hands.

Just as well, self-proclaimed fans / purveyors of digital security on mobile phones (that could be anyone from a computer science student to grandma on Words With Friends) may want
to consider what happens if this fiasco goes to a trial of Apple vs United States. Should the FBI have their druthers in that scenario, a constitutional precedent would then exist that somehow determines federal authority to be able to demand total control over personal affects belonging to individuals deemed a threat to national security. In brief, a new law says the FBI and other federal agencies get full access to all encrypted metadata because they say so. Should that happen, though, we could at least hope that the courts don’t levy too harsh of a law from it to where it has a **chilling effect**, intimidating technology companies and manufacturers to comply with any and all requests from agents just based on the fact that they’re agents. We’ll have to see how it plays out, though the figure of 51% of polled citizens supporting the FBI in this fiasco is mortifying. Their public relations team is winning what should be an easily won debate of ethics and logic. Even from the most extreme possibilities, the creation of this tool isn’t warranted.

Work Cited