Letter to the Observer

To the Editor,

Year after year encryption grows in both implementation and importance in the lives of Americans young and old. From protecting password transmission to securing online banking transactions, encryption is a mathematical triumph that keeps your information secret to all but those whom you explicitly name. Unfortunately, encryption does not distinguish between good and bad intentions. It protects criminals the same as anyone else, but there are those who believe that such protection should be revoked. Syed Farook, the man responsible for the tragic San Bernardino shootings, has an iPhone with encrypted information inside that federal investigators wish to access. The FBI currently cannot circumvent Apple's latest security measures and has requested that the West Coast tech giant write software to grant access to the phone. Apple has fought the request on the grounds of immense security risk, the precedent that would be set, and the implications that would necessarily result. The issue has piqued the interest of several global superpowers, and the outcome will shape the future of encryption entirely, and for the sake of American privacy and security, we hope that Apple will stand firm and hold out against the FBI.

One point that many people in favor of the unlock argue is that Apple should unlock just this one phone and then throw away the key. Others believe that only Apple or the FBI should be allowed to possess this key. As Apple CEO, Tim Cook's letter to customers states, "Once created, the technique could be used over and over again, on any number of devices." Those in favor of the unlock overlook the fact that a one-time fix would be nearly impossible. There is no way that Apple or the FBI could fully ensure the safety of the key. In fact, most experts on the issue agree that it would not be possible to keep the key safe. In Tim Cook's words, "While the government may argue that its use would be limited to this case, there is no way to guarantee such control."

Not only can the key not be fully secured, but use of the key on a single iPhone would create a precedent. The FBI and other government agencies could point at the San Bernardino case and say, "If we did it for that phone, why can't we do it for this phone?" This is in no way a single, one-time-only case being looked at, but rather a dangerous and slippery slope. The Manhattan DA said that he already has 175 more phones that he wants to be unlocked with this key if it is built. That is just in Manhattan, so who knows how many other thousands of phones are in line to be unlocked if the FBI forces Apple to build this key. Are we ready to say that the government should be granted access to all iPhones? Because if we allow it in this one case, we are sending a message that it is ethical, and can be done for many cases.

This message has the potential to expand even beyond the iPhone. Encryption is present in most websites that users access on the Internet. If the government is given access to iPhones, who is to say that they also will not request access to other devices, databases, or

websites? To say that this key actually would be only for this one case, or that the key would never be used for another device is ludicrous. Yet, let's say that Apple allows the FBI to have this encryption key and the FBI never gives key access to anyone else. This is still a fatal security flaw. There are two possibilities if the government keeps control of this key, and potentially many other keys in the future. An enemy of the state could either hack the FBI and retrieve these keys, or more likely, they hack into a company's data because their encryption security is now weakened by giving encryption access to the government. Such a hacker could have access to data from hundreds of companies on thousands to millions of people. There is the potential for incredible amounts of damage to the United States's national security.

Regardless of if you own an iPhone or not, the outcome of this case will drastically effect the technology you use every day. Ultimately backdoors are not secure, the request sets a dangerous precedent, and compliance with the FBI in this case could easily extend to technologies outside of Apple's jurisdiction. Weakening the defense of millions of Americans to salvage six week's worth of information on a deceased shooter is hardly a price the FBI should be willing to pay, and we ought to be more than grateful that some intelligent leadership recognized that within Apple. Fighting the government is never an easy battle, though it is rooted in American history, and we must show our support and let the government know that security is a freedom whose integrity is paramount.

Sincerely,

Christian Clark, Thomas Deranek, Jesse Hamilton, and Neal Sheehan