The Observer
P.O. Box 779
Notre Dame, IN 46556

An Open Letter on the Importance of Encryption

To the Observer and all of its readers,

People in America and around the world have been hearing the word “encryption” thrown around quite a bit, especially in the last few months. In this letter we hope to define exactly what encryption means and clarify how not only is it nothing to fear, but that it is beneficial for all users.

Encryption is basically transforming data into a form that is unreadable by anyone who does not have a matching decryption key. Doing so ensures privacy by keeping information hidden from anyone but its intended recipients. For example, people who work with sensitive information such as financial statements or classified government documents will most likely encrypt the hard drives on their computers to prevent unauthorized users from reading their data. Encryption also allows for secure communication along insecure channels, such as wireless communication between two Facebook users.

In regards to debates over encryption, such as the ongoing one between Apple and the FBI, encryption has been vilified as a tool used by bad guys and terrorists to avoid detection, and that the average computer user with “nothing to hide” need not worry about it. In reality, everyone uses encryption on a daily basis, and likely without even realizing it. Any connection to a website that requires even the slightest amount of secrecy will use encryption in the form of HTTPS: bank sites, social media logins, etc. In fact, more and more sites are switching to the more secure HTTPS, even if it is unlikely that sensitive data will be sent or received. iMessage and FaceTime between Apple devices use encryption by default. No matter what a user is doing on their computer or phone, they will certainly make use of encryption behind-the-scenes. Encryption has become a crucial part of the technological landscape of our world today and vital to the protection of consumers.

When the topic of encryption comes up, it’s inevitable that someone will say “I have nothing to hide, therefore I have nothing to fear.” This idea is dangerously naive. Everyone has sensitive information that would be disastrous to lose. Even if one doesn’t feel the need to keep secrets from possible government eavesdropping, it would be unwise to broadcast sensitive information like passwords, bank information, or social security numbers. Encryption allows this information to be safely stored and transmitted, without fear of eavesdroppers. Without some form of encryption, it would be impossible to use almost any internet service without a severe risk of an eavesdropper gaining the means to access sensitive information, steal an online identity, etc. In the Apple case, for example, the creation of a back-door for the iPhone will allow for the circumvention of encryption on the mobile device, thus exposing millions of iPhone users to the risk of attack. Without encryption, users will be vulnerable to malicious attacks from those exploiting their lack of protection.

The Apple case also has the potential to set a dangerous precedent in terms of data privacy. Apple does not have access to its users encrypted, private information and had complied with the government to provided all of the non-encrypted information they had on the San Bernardino shooter. If it is ruled that the government does have the right to force Apple to create a backdoor for the iPhone, it sets a dangerous precedent where the government can ask any company to bypass whatever encryption and privacy measures it has in place, defying the very purpose of encryption and data privacy for terrorist information that may not even be on the phone!

Up to this point it may sound as if encryption, while allowing for users to protect their data privacy, makes it difficult or even impossible for law enforcement to carry out their jobs. This is definitely not the case. First, the Internet relies on data gathered from its users in order to power its targeted advertising, so not all companies and not all applications, even those being run on encrypted devices, are going to encrypt data if they want to keep making money. Even if all companies and applications embrace encrypting all of their data, metadata, or information about communication will not be encrypted. Law enforcement will always have access to phone numbers, email addresses, etc. since you cannot send messages without a destination. Finally, as more and more devices and sensors are connected to the network to expand the "Internet of Things," law enforcement will be gaining new opportunities for surveillance outside of intercepting communications between users by using data from sources like smart thermostats, cars connected to the Internet, wearables, etc.

As the debate between Apple and the government continues and as more and more devices are connected to the network, it is important to remember that the overarching debate about encryption comes down to the balance we as a society strike between security and privacy. As Rousseau mentioned in the *Social Contract*, we as the governed have elected to give up some of our freedoms to our government, who in exchange protects our remaining rights. Perhaps this debate over encryption is merely a sign that the time has come for both sides of this social contract to reevaluate the terms in light of all of the advances made in technology. Until then, we hope this letter has shed some light as to what encryption really is and why it is important.

Sincerely,

Dinh Do
Chris Ray
Nathan Vahrenberg