ECE 518 Homework 1

Alan Palayil

Due Date: 9/30/2022

What is the “Going Dark” problem?

The “Going Dark” problem is the situation where a law enforcement and intelligence agencies can effectively screen or monitor criminals and suspects when they have obtained the legal authority to access and search through their electronic devices and communications, but do not have the technical capability to do so as a result of the utilization of encrypted communications. With the advent of strong encryption, suspects and criminals can communicate using methods that are very challenging for the law enforcement agencies to screen as this presents a serious challenge for the agencies, as they cannot accumulate the knowledge needed to prevent illegal activities and crime. One of the primary ways that law enforcement and intelligence agencies gather data is through the interception of communications. This is possible through various methods, such as wiretapping telephone lines, intercepting emails, and checking social media activity.

In any case, the drawback has become a lot more current due to the utilization of encoding spreading worldwide and has been increased by the occasion of end-to-end encryption that are not even feasible for the suppliers of communications services to decrypt messages making it inadequate for interception methods. The other issue agencies face are the suspects and criminals utilize VPNs and darknets to communicate and send their encrypted data via private networks and special software’s. Regardless of whether the agencies were able to intercept the message, the decryption would be very difficult without the encryption key.

Who are participating in the “Going Dark” debate?

The “Going Dark” debate is between law enforcement and the technological industry. Law enforcement and intelligence agencies have long expressed their concerns on the "Going Dark" drawbacks, and where they are losing the capabilities to gather knowledge and investigate crime because of the rising utilization of encryption conventions by tech companies. With the expanded utilization of encryption protocols for the privacy of the users and the security of internet means that assuming if the law enforcement has a warrant, they wouldn’t be able to access the data without the user’s collaboration.

The effect of encryption is influential for the point that law enforcement has put cases on tech companies like Apple and Google to have them unlock the criminals’ phones with the companies refusing to do so. Encryption has made it challenging to accumulate knowledge and investigate crime. With the statement that encryption is vital for the security of the internet and safeguards businesses from cyber-attacks, it additionally makes suspects and criminals conceal their activities which are difficult to track. Encryption allows individuals to communicate with no fear of surveillance as encryption has become an essential right for data communications.

What are their opinions?

The “Going Dark” debate surrounds the law enforcement and intelligence agencies’ with encrypted information and communications. The opinions surrounding this debate varies a lot. Some believe that law enforcement and intelligence agencies ought to have access to encrypted information and communications due to which they would be able to track down suspects and criminals with ease. They also state that encryption is often used by suspects and criminals to hide their communications from law enforcement and intelligence agencies, and that rising access to encrypted information and communications would help to avert this.

While others believe that access to encrypted information and communications would be an infringement of privacy rights. They state that law enforcement and intelligence agencies should find alternate ways of gathering the information they require, without infringing the privacy rights of individuals. They also state that rising access to encrypted data and communications would make it more accessible for suspects and criminals to gather this information, and that this would eventually make it harder for law enforcement and intelligence agencies to track them down.

The "Going Dark" debate is ongoing, and there is no reasonable agreement regarding this problem.