Early in the podcast, Comey mentions that the FBI has a sworn duty to try to keep every American safe from crime and terrorism, with technology becoming the main choice for dangerous people. He mentions “Going Dark” as the term used to describe laws not keeping pace with technology, which creates a significant public safety problem, because those who are in charge of helping to keep us safe are unable to access the evidence needed in order to help prevent terrorism and prosecute criminals, even with lawful authority. Comey describes how after the Snowden revelations that even though the public may think the government or law enforcement has access to all and any of our information across every single app or phone service, it is indeed not the case. Personally, this and the previous point about laws not keeping pace with technology are surprising especially because the world has become more tech centric and continues to do so. I always felt like our government had kept up laws geared toward technology as technology itself continued to boom and people have begun to use it more than ever. The podcast itself and the articles really dive into how difficult it is for the FBI to obtain information that is necessary to help prevent terrorism and solve a crime, even more so when it is encrypted. I believe certain laws should be enacted to help keep up with technology, especially because as the years go by, even more people and organizations will become tech centric. The main challenge with encrypted information is that the FBI has to, in a way, struggle to even obtain said information, because it is in essence, locked away, and there are legality issues with decrypting.

Encryption is often used as a mean to block law enforcement or government officials from accessing information about suspects or information related to a criminal case. When the criminal actor uses encryption to block said information, law enforcement must find a workaround, whether that be finding a way to decrypt the information or finding a way to access copies of the information. Several recent developments in cybercrime laws within the past year have come about due to the legal issues prompted by encryption workarounds. The debate now mainly centers around as to whether or not the workarounds are legal. One of the main challenges is whether the All-Writs Act is a valid method of allowing the government to require a company, such as Apple, to encrypt the information for their case, such as Apple vs. FBI. Eventually, a magistrate judge ruled that the government was not allowed to use the All-Writs Act to do so. In one case, the government was able to obtain a warrant to insert malware into a system in order for them to attempt to search the computers for information that Tor was hiding as a workaround, due to the IP addresses being encrypted. Litigation over the Playpen warrant as it was called, concerns the legality of the warrant and the techniques it authorized.