Going Dark – Apple vs. FBI

Ryan Scott

Grand Canyon University  
ITT-306 Information Security II

Prof. Christine Bakke

## Legal Precedent

Legal precedent forms the basis of most laws. A legal precedent can be established in this case by a judge that may serve as a basis for similar requests in the future. This is a consequence of the precedent, also known as a "precedential consequence." Should the court grants the FBI's request, the decision may serve as a legal basis for other law enforcement agencies to request similar access to encrypted devices in the future, (Al Jazeera English, 2016).

Under the All-Writs Act of 1789, federal courts are authorized to issue "any writs appropriate or necessary to aid their respective jurisdictions and in accordance with the principles and usages of law, (Al Jazeera English, 2016)." This law was used by the FBI to request that Apple create a method for unlocking the phone, arguing that the court could order Apple to cooperate. Apple, however, argued that the All-Writs Act could not force them to create technology that undermined the security of their devices, (Al Jazeera English, 2016). After the FBI was able to unlock the phone without Apple's assistance, the court case was dismissed.

As reported by Cindy Kohn, Apple assisted the FBI by providing it with all the information it had, including all the metadata, so they could access all of the information. Verizon also provided information regarding all of the call data, as well as metadata, regarding the phone's calls, (Al Jazeera English, 2016).

For Cindy, the level of cooperation that Apple is willing to provide is unacceptable. She argues that the government's request for Apple to create new technology and provide access to encrypted data goes beyond the authority of the All Writs Act, is unconstitutional, and would negatively impact the security of devices and the privacy rights of customers, (Al Jazeera English, 2016). Cindy Kohn and the EFF believe that compelling Apple to create new technology or provide access to encrypted data poses a threat to civil liberties in the digital world, (Al Jazeera English, 2016).

**“Ubiquitous as Possible”**

According to Marlinspike, the encryption techniques developed for the Signal App are also being used by other popular applications (such as WhatsApp, Facebook Messenger, Zoom, etc). He stated that the goal is to make this technology as widespread and open-source as possible, meaning that it would be widely used across multiple products and platforms, (Al Jazeera English, 2016).

I support the use of strong end-to-end encryption for personal communications because it provides a high level of security and privacy for personal communications. However, I also recognize that it has its downsides, such as making it more difficult for law enforcement agencies to access information that could be used in criminal investigations. It's important to strike a balance between protecting personal rights and freedoms and ensuring that law enforcement agencies have the tools they need to keep citizens safe, (LastWeekTonight, 2016).

The Fourth Amendment to the US Constitution protects citizens against unreasonable searches and seizures, and the Fifth Amendment protects citizens against self-incrimination. The idea that "the FBI has access to everything" could be seen as a violation of these rights as it implies that the government would have unrestricted access to citizens' personal information without due process or oversight, (IntelligenceSquared Debates, 2017). Citizens are also guaranteed due process and equal protection under the law under the Fourteenth Amendment, and the idea that "the FBI has access to everything" could also be considered a violation of this right, since it implies the government could target certain groups or individuals unfairly, (IntelligenceSquared Debates, 2017).

**Going Dark?**

Marquis from First Look Media presents a more well-rounded argument on the "going dark" problem. He points out that despite the use of encryption, law enforcement agencies still have access to a wealth of data from other sources such as cloud-based data, social media data, and data from cameras, (Al Jazeera English, 2016). This means that encryption is not making it impossible for law enforcement agencies to access data, as they have other means of obtaining the information they need for investigations. Additionally, Marquis emphasizes the importance of protecting citizens' rights and privacy by using encryption as a tool to ensure personal data is secured from unauthorized access, (Al Jazeera English, 2016).

On the other hand, the FBI's argument presents a one-sided perspective, and portrays themselves as victims of the encryption technology, without recognizing the other sources of data that are available to them, and the importance of protecting citizens' rights and privacy, (Computerphile, 2017). Compared to the FBI’s view, Marquis' argument provides a broader, more nuanced view of the "going dark" issue. Furthermore, Professor Ross Anderson stresses that a back door would serve as a prime target for hackers and nation-states, placing everyone's data at risk, (Computerphile, 2017). In addition, he points out that historically these “nobody but us” backdoors have always been found and exploited by others, (Computerphile, 2017).

**Backdoor Removes the Door!**

Bill Marczak argues for strong encryption without a back door. In his opinion, the implementation of a back door would compromise the security of encryption for everyone, including the FBI. Furthermore, he stresses that a back door would serve as a prime target for hackers and nation-states, placing everyone's data at risk. In addition, he points out that encryption is a global standard, and creating a back door for the FBI would be a dangerous precedent to set, (LastWeekTonight, 2016).

In a similar vein, Ted Lieu, a representative of the US Congress, emphasizes that strong encryption should be maintained without any back doors. His view is that a backdoor would undermine encryption security, as well as violate the Fourth Amendment of the United States Constitution (which protects citizens from unreasonable searches and seizures), (LastWeekTonight, 2016). Furthermore, he points out that a back door would be an open invitation to hackers and cybercriminals. In his view, encryption is a critical tool for ensuring privacy and online security, and should never be compromised to facilitate law enforcement access, (LastWeekTonight, 2016).

## 

## Conclusion

| **Rating** | **Statement** |
| --- | --- |
| **1** | The government should restrict the types of encryption technology that the general public is allowed to use. |
| **4** | Companies should be forced to comply with court-ordered search warrants when vital information is needed to conduct an investigation. |
| **2** | Governments should have unique access to otherwise strongly encrypted communications and data storage. |

# Two Column Summary

| **Apple – Security should be strong.** | **FBI – Government should have a back door.** |
| --- | --- |
| 1. Strong security is essential. 2. Encryption is a universal standard. 3. Back door = no door. Hacker incentive! | 1. We want a back door. 2. Data encryption makes law enforcement useless. 3. Back door is a necessary evil for public safety. |

**References**

Al Jazeera English. (2016, October 25). *Crypto Wars: Behind the Encryption Debate | Fault Lines*. YouTube. <https://youtu.be/j7VA4H8m4uk>

Computerphile. (2017, March 4). *The Golden Key: FBI vs Apple iPhone.* Retrieved from <https://youtu.be/6RNKtwAGvqc>

IntelligenceSquared Debates. (2017, June 12). *Debating The Constitution: Technology and Privacy*. Retrieved from <https://youtu.be/tJ5wZprbSos>

LastWeekTonight. (2016, March 13). Encryption: *Last Week Tonight with John Oliver (HBO)*. Retrieved from <https://youtu.be/zsjZ2r9Ygzw>