by S N

Submission date: 27-Jun-2021 04:06AM (UTC-0500)
Submission ID: 1612675012
File name: gal_Considerations_Associated_With_Cellphone_Investigations.docx (17.42K)
Word count: 720
Character count: 3980

Legal Considerations Associated with Cellphone Investigations

Name:

Institution:

Course:

Instructor:

Date:

Legal Considerations Associated with Cellphone Investigations

In the 2015 San Bernardino gun attack that left fourteen people dead, the Federal Bureau of Investigation (FBI) uncovered the mobile phone of one of the dead perpetrators. According to the FBI, the mobile phone contained crucial leads regarding the attackers' contacts and will help determine whether others supported their violent acts (BBC NEWS, 2016). However, the FBI could not access the dead terrorists' phone because it had a four-digit passcode. Consequently, a standoff ensued between the manufacturer and the FBI. Finally, a federal judge ordered the company to unlock the Apple iPhone to allow the FBI to obtain crucial leads in the case.

The FBI requested that Apple develop a personalized software that would deactivate fundamental security mechanisms on the iPhone. The court's decision demanded that Apple develop and configure this custom hacking software without unlocking or altering the data on the phone. Apple raised objections to the order, claiming that it is unconstitutional and illegal. Further, Apple claimed that granting the order would jeopardize the confidentiality of all Apple products and set a bad precedent for subsequent situations (Kharpal, 2016). Unfortunately, a partner discovered a way to unlock the device for the FBI before the date of the judicial process. Much to Apple's dismay, the FBI declined to explain how the foreign entity accessed the mobile device.

One of the legal issues surrounding this case is that Apple is a company that manufactures different products, and granting the court's request would provide the FBI with software capable of accessing the data in iPhones used by different entities globally (Kharpal, 2016). Therefore, the order was unlawful because private entities like Apple cannot create programs that can help the state hack into people's phones. After all, it would be a violation of both the First and Fifth Amendments. The ethical considerations in this particular case are that

Apple would be acting contrary to their consumer's expectations by siding with the government in creating a program that can help the FBI access iPhone's data.

I disagreed with the outcome of this case. I wished that it could have progressed in the courts so that Apple could sufficiently argue about their reservations in creating a program that will allow the FBI to access data on the mobile device and the dangers of allowing such happenings. I am also displeased with how the FBI accessed the mobile device's contents without involving the manufacturer. In this scenario, Apple knows that their mobile devices have a flaw that can be exploited, but they cannot pinpoint where the vulnerability lies. In addition to that, the court's orders were illegal and unconstitutional in my view since it sets a dangerous precedent. Though the case was dismissed, it should never have happened, and the judges should not have granted the orders sought by the FBI since it is against the spirit of the Fifth and Fourth Amendments. The orders are unconstitutional, and the knowledge worsens the matter that the American government can access millions of iPhones, which in theory weakens Apple products. Also, according to the Texas McCombs School of Business (2017), the order is unlawful since it violates Apple's First Amendment by forcing the company to do something it is not comfortable doing or saying.

What I would have done differently, in this case, is allow it to go to a full hearing so that both parties can argue their case. As it is, Apple never got a chance to explain their reservations and how implementing the court's orders would make the company vulnerable and allow the FBI to surveil American citizens. In addition to that, the FBI did not exhaust all the technological methods of accessing the data. For example, in the San Bernardino murder case, the authorities obtained Farook's cellular data from the service provider, including a list of the numbers called and the texts sent. This information was enough to understand what the terrorists planned.

References

BBC NEWS. (2016, March 29). *FBI-Apple case: Investigators break into dead San Bernardino gunman's iPhone*. BBC News. https://www.bbc.com/news/world-us-canada-35914195

Kharpal, A. (2016, March 29). *Apple vs. FBI: All you need to know*. CNBC. https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html

Texas McCombs School of Business. (2017, March 15). *The FBI & Apple security vs. privacy*. Ethics Unwrapped. https://ethicsunwrapped.utexas.edu/case-study/fbi-apple-security-vs-privacy

I

ORIGINALITY REPORT

1%	0%	0%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Australian Institute of Higher Education Student Paper	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		