

IT UNIVERSITY OF COPENHAGEN

REFLECTIONS ABOUT IT

# PRIVACY AND SECURITY AS VALUES IN DESIGN

*Author:* Niels Andreas Østman

*Course manager:* Judith Simon

IT UNIVERSITY OF COPENHAGEN

Copenhagen, Denmark

27<sup>th</sup> of May 2016

Characters

# ABSTRACT

## TABLE OF CONTENTS

<b>ABSTRACT .....</b>	<b>3</b>
<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>INTRODUCTION .....</b>	<b>4</b>
<b>PRIVACY AND SECURITY .....</b>	<b>4</b>
<b>VALUES IN DESIGN .....</b>	<b>4</b>
<b>FBI VS. APPLE ANALYSIS .....</b>	<b>4</b>
<b>REFERENCES .....</b>	<b>6</b>

## INTRODUCTION

In 2014, Apple released their iPhone operating system iOS 8. One of the key features highlighted was increased security:

For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess. (Cook 2014).

From then on, Apple no longer has access to the information stored on iPhone devices. Seeing as they are unwilling to create a backdoor for government agencies, they are no longer able to extract data for law-enforcement. Following the iOS 8 unveil, James B. Comey, director of the FBI, expressed his concerns for the encryption trend Apple started:

Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. (Comey 2014).

During the aftermath of a terrorist attack in San Bernardino in December 2015, Comey's concerns were manifested, as the iPhone belonging to the perpetrator, Syed Rizwan Farook, was encrypted. The FBI was unable to access the iPhone's encrypted content and in the hopes of gaining crucial evidence about the attack (Decker 2016), a court order was issued. Apple was compelled to assist the FBI in decrypting and unlocking the phone by writing a custom firmware file. (Decker 2016). In an open letter Tim Cook, CEO of Apple Inc., responded that they would not comply with the court order, because doing so would be a threat to data security and set a dangerous precedent. (Cook 2016).

Viewing the case as a question of values such as privacy and security will investigate the considerations made by each organisation and illuminate how the conflict is an expression of differences in values.

## PRIVACY AND SECURITY

What is security and privacy?

## VALUES IN DESIGN

Before the case is analysed, the notion of values and value sensitive design will be introduced. What is a value, how can it be analysed and used? – Stakeholder analysis. Benefits and harms. Who introduced the idea of values in design, what does it mean and how can it be used? What do different people think of it?

Nissenbaum, Friedman, Brey, Winner

## FBI VS. APPLE ANALYSIS

Why did Apple do this? And why did the FBI react the way they did?

Stakeholder analysis of FBI, Apple, the people and the terrorists. Present the considered stakes.

**FBI:** National security, protection from terrorists. [SEE Comey's letters, and FBI court order]. Taking people's security against terrorists into consideration. They claim that encryption harms security.

**Apple:** Customers' trust. Taking the people's privacy into consideration. [See Apple's letters]. [Comey says that encryption is a marketing trick – while that may be the case, there is a reason why Apple wants to sell it.]. They explain why it is important in their letters, but Rogaway has some of the same views. [Critiques of privacy]

“Parent's view, only when others acquire undocumented personal information about an individual”

Analyse

FBI claims that by trading some privacy, we can gain in national security. With the information gained by accessing the phone, future attacks may be prevented. Moore (2000) finds this problematic. Nissenbaum also has something to say about privacy. Etzioni and Marsh (2003) provides examples.

iPhones with cryptography is an IT artefact, which holds ethics of design independent of the user. It is a value of design placed by Apple. Their reasoning can be found in the security documentation, and open customer letter. Brey believes that technologies promote moral values, in this case Apple values customer privacy.

Privacy and security dichotomy invalid.

## REFERENCES

Comey, James B. (2014). “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” Speech at the Brookings Institute, October 16, 2014. Accessed May 24, 2016. URL = <<https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>>

Cook, Tim (2014). “Apple’s commitment to your privacy”/“Government Information Requests”. In Apple website. Apple Inc. Published September, 2014. Accessed May 24, 2016. URL = <<http://www.apple.com/privacy/>>

Cook, Tim (2016). “A Message to Our Customers”. In Apple website. Apple Inc. Published February 16, 2016. Accessed May 24, 2016. URL = <<http://www.apple.com/customer-letter/>>

Decker, Eileen M. (2016) “Order Compelling Apple, Inc. to Assist Agents in Search”. NDAA, National District Attorneys Association. Published February 16, 2016. Accessed May 24, 2016. URL = <<http://www.ndaa.org/pdf/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf>>

Decker, Eileen M. (2016) “Government’s Ex Parte Application For Order Compelling Apple Inc. To Assist Agents in Search”. NDAA, National District Attorneys Association. Published February 16, 2016. Accessed May 24, 2016. URL = <<https://www.documentcloud.org/documents/2714000-SB-Shooter-MOTION-Seeking-Asst-iPhone.html>>

Farivar, Cyrus (2014). “Apple expands data encryption under iOS 8, making handover to cops moot”. In Ars Technica. WIRED Media. Published Sep 18, 2014. Accessed May 24, 2016. URL = <<http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/>>