

# Reflections About IT

Privacy, Security and Trust in Value Sensitive Design

*Author:* Niels Andreas Østman

*Course manager:* Judith Simon

# IT University of Copenhagen

Copenhagen, Denmark

27th of May 2016

Characters

# Abstract

When designing at system, values of the stakeholders can frequently be in conflict. This paper examines the apparent dichotomy of the values privacy and security in the San Bernardino case between the FBI and Apple.

# Table of Contents

Reflections About IT 2

IT University of Copenhagen 2

Abstract 3

Table of Contents 3

Introduction 4

Privacy and Security 4

Values in Design 4

What is a Value? 4

FBI Vs. Apple Analysis 5

References 6

# Introduction

When designing software, it is common that design values are in conflict. The values of security and privacy frequently occur in the discussion of whether or not the two are contradictory (Moore 2000, Zedner 2009, Agamben 2013, Rogaway 2015). This issue has been highlighted once more in the wake of the San Bernardino case between the FBI and Apple. (Barrett 2016).

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 release, James B. Comey, director of the FBI, expressed his concerns about 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.

# Value Sensitive Design

When designing software there is a desire to embed and support human values into the system. Value Sensitive Design is a theoretical and methodical approach developed for handling human values in design. In a broad naturalistic sense Friedman et al. defines value as “what a person or group of people consider important in life.” (Friedman et al. 2006, p. 2). This means that values are not based on facts, but rather on the interests and desires of individuals in a social environment.

Value Sensitive Design comprises of three investigative elements; conceptual, empirical, and technical. (Friedman et al. 2006, p. 3). The conceptual investigation aims to define who the direct and indirect stake holders are, how they are affected, what values are implicated, and how trade-offs between competing values should be made. The empirical investigation makes use of social science research tools, including observations, interviews, surveys, etc. to assess the success of a design. The technical investigation focuses on the technology itself, and how its properties align with the desired design values. The empirical investigation is outside the scope of this work, because it aims to examine an existing design, and it will not be an active party in the design development.

# Privacy and Security

The main values of interest in the San Bernardino case are those of privacy, security and trust. This section will discuss these values implicated in the system design of iOS.

**Privacy** is… The notion of privacy and what is private is ever-changing as technology keeps advancing. (Nissenbaum 1998)

**Security** can be seen as personal and national. Personal security may increase informational privacy. (Nissenbaum 2005)

**Trust** in a relationship between people, sometimes mediated through machines. They propose that people trust when they are vulnerable to harm from others, yet believe those others would not harm them even though they could. (Nissenbaum 2001)

# Investigation of iOS Design

## Conceptual Investigation of iOS

Who arethe **direct, and indirect stake holders?** (Apple, Comey)

How are they **affected**? (Apple, Comey, Rogaway, Barrett)

What **values** are implicated? (Apple, Comey)

Multiplicity of and Potential Conflicts among Human Values.

How should **trade-offs** be made? (Zedner 2009, Agamben 2013, Moore 2000, Etzioni & Marsh, Cook, Comey, Barrett). (THIS IS A BIG ONE!)

## Technical Investigation of iOS

**Cryptography** (Rogaway 2015, Apple)

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 costumer privacy.

Privacy and security dichotomy invalid.

# References

Barrett, Brian (2016). “The Apple-FBI Fight Isn’t About Privacy vs. Security. Don’t Be Misled”. In Wired, February 24, 2016. Accessed May 24, 2016. URL = <https://www.wired.com/2016/02/apple-fbi-privacy-security/>

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>

Comey, James B. (2016). “We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead”. In Lawfare. The Lawfare Institute, February 21, 2016. Accessed May 24, 2016. URL = <https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead>

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 >

Friedman, B., P. H. Kahn, et al. (2006). “Value Sensitive Design and Information Systems.” In Human-Computer Interaction in Management Information Systems: Foundations. P. Zhang and D. Galletta. New York, M.E. Sharpe: 348-372. Published 2006.

Nissenbaum, Helen (1998). “Protecting Privacy in an Information Age: The Problem of Privacy in Public”. In Law and Philosophy, 17: 559-596. Published 1998. Accessed May 24, 2016. URL = < http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf>

Nissenbaum, Helen (2001). “Securing Trust Online: Wisdom or Oxymoron”. In Boston University Law Review, Volume 81, No.3 635-664. Published June 2001. Accessed May 24, 2016. URL = < http://www.nyu.edu/projects/nissenbaum/papers/securingtrust.pdf >

Nissenbaum, Helen (2005). “Where Computer Security Meets National Security”. In Ethics and Information Technology, Vol. 7, No. 2., 61-73. Published June 2005. Accessed May 24, 2016. URL = < http://www.nyu.edu/projects/nissenbaum/papers/ETINsecurity.pdf >

Rogaway, Phillip (2015): “The Moral Character of Cryptographic Work”. In Cryptology ePrint Archive. Published 2015. Accessed May 24, 2016. URL = <http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf>