IT UNIVERSITY OF COPENHAGEN

REFLECTIONS ABOUT IT

ENCRYPTION 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

ABSTRACT **3**

TABLE OF CONTENTS **3**

INTRODUCTION **4**

VALUE SENSITIVE DESIGN **4**

INVESTIGATION OF IOS DESIGN **5**

DIRECT AND INDIRECT STAKEHOLDERS 5

BENEFITS AND HARMS FOR EACH STAKEHOLDER GROUP 5

CONCEPTUAL INVESTIGATION OF KEY VALUES 6

POTENTIAL VALUE CONFLICTS 7

TECHNICAL INVESTIGATION OF CRYPTOGRAPHY IN IOS 8

DISCUSSION **8**

CONCLUSION **8**

REFERENCES **9**

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).

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 part in the design development.

INVESTIGATION OF IOS DESIGN

The conflict in this case revolves around the implementation of encryption in Apple's operating system iOS and how it affects those who are dependent on it. Here it will be investigated who the stakeholders are, what their values are and how they may be benefitted or harmed by the new technology.

DIRECT AND INDIRECT STAKEHOLDERS

Friedman et al. gives an account of how to identify stakeholders:

> Direct stakeholders refer to parties – individuals or organizations – who interact directly with the computer system or its output. Indirect stakeholders refer to all other parties who are affected by the use of the system. (Friedman et al. 2006, p. 13).

The stakeholders involved are the ones who interact directly with the system and those who will be affected by the use of it. Because there are several contexts of use in regards to iPhones, the case is complex with different stakeholders in different use cases.

Intended use.

In the context of using iPhone within its intended use case Apple's customers are direct stakeholders. Here Apple is a stakeholder as a business who depends on customers to buy their products.

Additional uses.

The FBI is a direct stakeholder in the case where they depend on the output that can be gained from the system. Comey gives an account of how the FBI has previously has been able to use the contents of a phone to convict a felon. (Comey 2014). In that case Apple would be the one facilitating the transfer of such data. This also means that even without using iPhones themselves, victims, potential victims, their relatives and criminals are indirectly affected by the use of such devices.

BENEFITS AND HARMS FOR EACH STAKEHOLDER GROUP

(Apple, Comey, Rogaway, Barrett)

The benefits and harms for the stakeholders caused by the system is dependent on the context of use.

Intended use.

According to Apple, the built in encryption protects personal data stored on devices so that it is never shared without permission as "We empower you to make your own choices about what you share and with whom." (Cook 2014). Marking data security as a value. This could be labelled privacy by design, which Cavoukian describes in terms of "data protection needs to be viewed in proactive rather then reactive terms, making privacy by design preventive and not simply remedial" (Cavoukian 2010). This is a benefit to the costumers who will be in control of their personal information, appealing to the value of privacy. Personal information is data that can be linked to individual persons. This privacy proposition will in turn benefit Apple who will gain the trust of their customers, by guaranteeing that only the customer is in

position of their personal data. The trust of their customers is a value that is very important to Apple. (Cook 2014).

Additional use.

Comey explains how protecting personal data by encryption harms both the FBI and the potential victims:

> those of us in law enforcement and public safety have a major fear of missing out - missing out on predators who exploit the most vulnerable among us...missing out on violent criminals who target our communities...missing out on a terrorist cell using social media to recruit, plan, and execute an attack. (Comey 2014).

He is worried that encryption threatens to lead lead to a dark place, where the FBI is unable to prevent crimes because they are unable to access data on encrypted devices. Focusing on the impedance of the protection of the people by the introduction of encryption shows the value held by the FBI is that of national security.

Conceptual Investigation of Key Values

The key values revealed by identifying the stakeholders 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. The discussion of privacy is co-dependent on the use of technology. It was first argued that privacy is the right to be let alone. The debate of privacy has evolved alongside the development of information technology. (van den Hoven 2016). Friedman et al. describes that privacy is the right of an individual to control what personal information is communicated to others. (Friedman et al. 2006, p. 17). As surveillance has made its entry, technology has allowed for collection, storage, and analysis of information, and enabled profiling, data mining and data aggregation. This begs the question of whether information technology has eliminated the private sphere. Nissenbaum observes that

> Where previously, physical barriers and inconvenience might have discouraged all but the most tenacious from ferreting out information, technology makes this available at the click of a button or for a few dollars. (Nissenbaum 1997).

Subsequent to when this was written, services like Google and Facebook has made its mark, by automating the gathering of data and making it cheaper to make a profit by selling personal information. Nissenbaum argues that privacy should be protected.

Apple highlights that they do not sell customer information, which has otherwise become common practice for many IT companies. As Cook puts it, “when an online service is free, you’re not the customer. You’re the product.” (Cook 2014).

Security. Technical experts working on computer security has traditionally been working on protecting computers and their users from three different categories. Protection from attacks that render systems unavailable, such as denial of service attacks. Attacks that threaten the integrity of data, by corrupting or destroying it. Attacks that threaten the confidentiality of data by unauthorized access. (Nissenbaum 2005).

‘What is essential (to securitization) is the designation of an existential threat requiring emergency action or spe- cial measures and the acceptance of that designation by a significant audience.’’24 These ‘‘special mea- sures’’ typically involve bending rules of normal governance, and as matters of national security they are lifted – presumably temporarily – outside, or beyond the bounds of political procedure. In the face of securitized threats and times of national crises, even liberal democracies accept breaks from
can be seen as data and national. Data 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)

Potential Value Conflicts

How should **trade-offs** be made? (Zedner 2009, Agamben 2013, Moore 2000, Etzioni & Marsh, Cook, Comey, Barrett). (THIS IS A BIG ONE!)
(Zedner 2009, p. 135-136) (Etzioni 2003)
Comey argues that privacy and security are treasured values, but they are in conflict:

> Although this case is about the innocents attacked in San Bernardino, it does highlight that we have awesome new technology that creates a serious tension between two values we all treasure: privacy and safety. (Comey 2016).

He believes that the privacy gained by encryption reduces the national safety, as illustrated in the case of the San Bernardino attack.

According to Lyon, many attempts at procuring national security jeopardize civil liberties. (Lyon 2015). Zedner gives a warning of depicting such matters as being a balance between security and privacy. The threat posed by terror and the consequent fear will bring the balance in favour of security. (Zedner 2009, p. 135). He points out that balancing the two suggests that there is an existing imbalance. He warns that “terrorist attacks create a political climate of fear that is not conducive to sober assessment of the gravity of the threat posed” (Zedner 2009, p. 135), and that accurately assessing security threats is a challenge. This means that the scale pan of security is inaccurate and marked by fear, and trying to balance the scale based on this is nonsensical.

Comey points out that the design should not depend on the values of Apple and the FBI as they both are biased with each their own agenda.

> That tension should not be resolved by corporations that sell stuff for a living. It also should not be resolved by the FBI, which investigates for a living. It should be resolved by the American people deciding how we want to govern ourselves in a world we have never seen before. (Comey 2016).

Instead he believes that it should be up to the American people to decide what values should be accommodated for in the system. Numerous polls have been conducted to reveal how the people feel about the case. The polls reveal that the results are depending on the group asked. (Elmer-DeWitt 2016). The poll carried out by Pew Research showed results in favour of the FBI with 51% voting that Apple should unlock the iPhone. (Pew 2016). However, the polls

conducted on more technologically inclined groups had a tendency to answer in favour of Apple not unlocking the iPhone. (Elmer-DeWitt 2016).

Technical Investigation of Cryptography in iOS

Cryptography has been used as a technology for protecting information since the time of the Roman empire. (van den Hoven 2016). The modern cryptography is essential to all systems that aim to protect personal data. The technology does not protect from data breaches on its own. Only when it is applied in a correct way can it secure personal data. Because of the way it works, a key is needed to decipher any encrypted message. If this key was to get in the wrong hands, the security will have been breached.

Friedman et al. argues that technologies can hold properties that will promote certain values: (Rogaway 2015, Apple)

> The interactional position holds that while the features or properties that people design into technologies more readily support certain values and hinder others, the technology's actual use depends on the goals of the people interacting with it. (Friedman et al. 2006, p. 13).

This means that by implementing a certain technology into a system, some values may be supported, while others may be impeded. However, the use scenario depends on what the user decides. While a screwdriver is suitable for turning screws, it can still be used as a poker, but it is not well suited for use as a wheel. (Friedman et al. 2006, p. 13).

Winner believes that politics can be built into artifacts, while Nissenbaum argues that technology can be biased. Brey believes that technologies promote moral values, in this case Apple values costumer privacy. Latour speaks about Actor-network-theory, in which

What values are embedded into the technology?

> At Apple, your trust means everything to us. That's why we respect your privacy and protect it with strong encryption, plus strict policies that govern how all data is handled. (Cook 2014)

Discussion

Not only do the companies hold and prioritize different values, but they also have different views on what artefacts can hold values.

Conclusion

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/>

Cavoukian, A. (2009) “Privacy by Design” In Ottowa: Information and Privacy Commissioner of Ontario, Canada. Published 2009. Accessed May 25, 2016. URL = <http://www.ipc.on.ca/images/Resources/privacybydesign.pdf >

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 >

Elmer-DeWitt, Philip (2016). “Apple vs. FBI: What the Polls Are Saying”. In Fortune, Time Inc. Published February 23, 2016. Accessed May 25, 2016. URL = <http://fortune.com/2016/02/23/apple-fbi-poll-pew/ >

Etzioni, A., Marsh, J. (2003). “Rights vs. Public Safety after 9/11”. In Lanham, MD: Rowman & Littlefield. Published 2003.

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.

Lyon, D. (2015). “The Snowden Stakes: Challenges for Understanding Surveillance Today”. In Surveillance & Society 13(2): 139-152. Published 2015. Accessed May 25, 2016. URL = <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/snowden_stakes/stakes>

Nissenbaum, Helen (1997). “Toward an Approach to Privacy in Public: Challenges of Information Technology,”. In Ethics and Behavior, 7(3): 207–219. Published 1997. Accessed May 25, 2016. URL = <http://www.nyu.edu/projects/nissenbaum/papers/toward_an_approach.pdf>

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 >

Pew Research (2016). “More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone”. In Pew Research Center. Published February 22, 2016. Accessed May 25, 2016. URL = <http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/>

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>

van den Hoven, Jeroen, Blaauw, Martijn, Pieters, Wolter and Warnier, Martijn (2016). “Privacy and Information Technology”. In The Stanford Encyclopedia of Philosophy (Spring 2016 Edition), Edward N. Zalta (ed.). Accessed May 25, 2016. URL = <http://plato.stanford.edu/archives/spr2016/entries/it-privacy/>

Zedner, Lucia (2009). “Security”. In New York and London. Routledge. Published 2009.