

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

23336 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. The investigation of case through the methodology of Value Sensitive Design reveals the stakeholders involved are the FBI, Apple, Apple’s customer and the American people. The key values held by the stake holders are shown to be national security, data security, privacy and trust. The difference in prioritization of their values leaves them at conflict.

# Table of Contents

Abstract 3

Table of Contents 3

Introduction 4

Value Sensitive Design 5

Investigation of iOS Design 5

Direct and Indirect Stakeholders 6

Benefits and Harms for Each Stakeholder Group 6

Conceptual Investigation of Key Values 7

Potential Value Conflicts 9

Technical Investigation of Cryptography in iOS 10

Discussion 12

Conclusion 13

References 14

# 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 (Zedner 2009, 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 data 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 the 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).

This paper examines the design of the technology which lead to a dispute between the FBI and Apple. An investigation of the design and the stakeholders’ values towards this case will be carried out in order to understand the various perspectives in the conflict. The overall research question of the paper is:

*How can one gain a broader understanding of the conflict between the FBI and Apple by examining the design of iOS?*

# Value Sensitive Design

When designing software there is a desire to support human values and embed them 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.” (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. Human beings can find many things to be of value, friendship, good manners, welfare, trust, etc.

Value Sensitive Design comprises of three investigative elements; conceptual, empirical, and technical. The conceptual investigation aims to define who the direct and indirect stakeholders 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 (Friedman et al. 2006, p. 3). The empirical investigation is outside the scope of this work, because it aims to examine an existing design in real-life settings, and it will not be an active part in the design investigation.

# 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

For this analysis, 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. If the FBI was to use iPhone data in their work, it would have an indirect effect on all of those involved in a crime, victim or criminal. 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. Successfully solving a case based on phone data effect relatives as they are brought justice. It can also keep potential victims out of harm’s way and bring conviction to the criminals.

## Benefits and Harms for Each Stakeholder Group

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 to a ‘dark place’, where the FBI is unable to prevent crimes because they cannot 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.

**Trust.** Trust is a relationship between people, sometimes mediated through machines. In this relationship one party is able to harm the other, but this other party believes that they will not. Trust is based on the ability to make three types of assessments. One has to be able to estimate the harms that may happen. One has to be able to assess the good will others possess towards oneself, which keeps them from doing harm. Lastly the harms that do occur has to be estimated if they lie outside the trust relationship (Friedman et al. 2006, p. 3).

**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). This means that iPhone users has to have control over the distribution of the data stored on there, in order have privacy. 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, p. 212).

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). In the effort to gain their customers trust, Apple ensures that they will not abuse them by selling information.

**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, p. 63).

Recognizing a severe threat that requires emergency action or special measures is instrumental to securitization. If people accepts the threat as being legitimate these special measures will also be accepted (Nissenbaum 2005, p. 69). In the case at hand the eminent threat is terror. These special measures typically involve deviating from the normal rules and termed matters of national security. As matters of national security they are elevated above the bounds of standard political procedure. When faced securitized threats in times of national crisis, liberal democracies accept such deviations (Nissenbaum 2005, p. 69).

## Potential Value Conflicts

Once the central values are identified it is often the case that some could be in conflict. This section attempts to identify the values in conflict and gives an account of the considerations to make when trade-offs have to be made. 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. Because of such threats, the FBI is willing to lax privacy to uphold national security, as they have experience that tells them that data stored on a phone can be used as valuable evidence in an investigation (Comey 2014). And so national security is prioritized over privacy.

According to Lyon, many attempts at procuring national security jeopardize civil liberties (Lyon 2015, p. 144). 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).

Apple prioritizes data security and privacy. Cook argues that reducing data security would leave the customers vulnerable to hackers and cyber criminals. Once an alternative version of iOS with reduced data security has been created with the FBI as the intended recipient, there is a risk that it may fall into the wrong hands. Even if the FBI’s intentions are pure and that they protect the software as best they can, even they can be victim om hackers and the “backdoor” could be compromised. If individuals of malicious intent somehow acquire access to the backdoor, it would not only be the privacy of Apple’s customers that would be compromised. Their personal safety is at risk as private information, such as health information and locations, the relatives’ information and so on can be used to harm the individual.

## 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:

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 explains how artefacts can have politics. By the invention and design of technology into artefacts it can become become an instrument for social agendas

instances in which the very process of technical development is so thoroughly biased in a particular direction that it regularly produces results counted as wonderful breakthroughs by some social interests and crushing setbacks by others (Winner 1980).

This means that the politics that is introduced by technical development in an artefact often is often seen as progress by some stakeholders, while others will consider it a setback.

In the presentation of iOS 8, the new technology is highlighted as at step forward. According to Cook, embedding encryption into iOS promotes customer privacy by protecting their data, which strengthens the trust relationship between Apple and the customer (Cook 2014). However, the same technology is considered a setback by the FBI. As the San Bernardino demonstrates, the technology is not well suited for crime prevention and investigation carried out by law-enforcement agencies. Rogaway calls encryption a ‘political tool’, which has an intrinsic moral dimension (Rogaway 2015, p. 1). Latour argues that artefacts have morals, for instance a seatbelt has a moral – you may die if you do not wear it. And so morals are imbued into artefacts (Latour 1992). A door has a lock which determines who can access the house. This way individuals no longer regulate access to the house, rather it is the locked door which only allows individuals in possession of the key to access the house. Analogously encryption can be viewed as a lock on the iPhone, to which only the owner has the key. Traditionally only the owner of the house can access it, unless the FBI has a court order, in which case they can force the door open. Contrary to a physical lock, forcing open an encrypted iPhone is impractical as it would take countless years. The delegation of regulating access to iPhone devices to a non-human like encryption, causes it to become a moral agent. This way it is out of the hands of Apple to determine if the FBI should be allowed access to any particular iPhone.

# Discussion

The source of the dispute is the difference in how the stakeholders prioritize their values. They also have differing focus on what values are reinforced by the technology.

Apple’s key values are data security and privacy for their customers and their customers trust. If Apples gives in once, they will have to do it again in another case. If Apple shows that they can be persuaded to compromise their data security for a law-enforcement investigation, Apple will have set a precedent, which the FBI can use to prompt other operating system manufacturers, such as Google, to do the same. Thousands of data extraction requests are sent to Apple by American law-enforcement agencies on a yearly basis. If Apple complies with the wishes of the American government, other governments such as China or the EU may follow suit. Cook wonders where it will end, and feels that the FBI cannot guarantee that the use of the backdoor will be limited to this single case. Without the guarantee they cannot maintain their trust relationship to the customers, because the do not have control over their data.

The FBI’s key values are national security and keeping the American people safe. To some extend this value must be protected in a manner where the end justifies the means. In the San Bernardino case, the threat of terrorist attacks has been realised and they feel compelled to follow every lead to find crucial evidence to prevent further attacks, and bring justice for the relatives of the victims (Comey 2016). However, archaic laws have not kept up with the advances in technology. This Forces the FBI to use an indelicate approach in order to keep the American people safe. They argue that what they are asking is only applicable to the single iPhone in question, this is however not technically true. They lack the technical knowledge to comprehend that their court order will have wide spread implications (Cook 2016). Concerns have also been raised regarding a pre-emptive approach to use data for preventing crime. Sadowski points out that there is no proof as to how reliable the data analysis is. Innocent citizens could be labelled as suspects in a crime they have not committed (Sadowski 2016). Rogaway criticizes that the FBI uses a ‘law-enforcement framing’, in which privacy is personal good, and security is a collective good. Here privacy and security are inherently in conflict and a balance must be found. The former balance has been destroyed by modern technology such as encryption because legislations have not kept up with the development. Because of this, the criminals may win by using technology to avoid getting caught (Rogaway 2015, p. 15). He argues that this framing is inconsistent with reality and it is used to promote fear. As Nissenbaum described, when facing securitized threats, people tend to accept deviations from the norm, even if it may harm liberal rights such as privacy (Nissenbaum 2005, p. 69). This way the FBI can use fear to protect their own interests in order to support the values that they consider the most important, which would be national security.

The key values held by the customers are that they can trust Apple to keep their data secure and private, and that they can trust the FBI to keep them safe from criminals, during national crisis and from terrorist attack. The polls revealed that the people side with the FBI in the case. They seem to value their personal safety higher than personal privacy. This could be a symptom of the fear that has been stricken into their hearts by the terrorist attack and the potential attacks to come. Maybe the problem is the fact that this matter is being presented as a choice between security and privacy. In many cases technology can be used to promote security (van den Hoven 2016). What is needed may not be an increase in surveillance, but rather a focus on how technology can be used in the advantage of the FBI and the American people to promote security.

# Conclusion

By investigating the San Bernardino case through the methodology of Value Sensitive Design, it is revealed that the stakeholders involved are the FBI, Apple, Apple’s customer and the American people. The key values held by the stake holders are national security, data security, privacy and trust. The difference in the stakeholders’ prioritization and focus of the values is what causes the conflict between the FBI and Apple. While they may hold some of the same values, they are concerned with keeping their own interests, leaving them at a stalemate.

# 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/ >

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.

Latour, Bruno (1992). “Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts”. In Wiebe E. Bijker and John Law, eds., Shaping Technology/Building Society: Studies in Sociotechnical Change (Cambridge, Mass.: MIT Press, 1992), pp. 225–258.

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 (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>

Sadowski, Jathan (2016). “Police data could be labelling 'suspects' for crimes they have not committed”. In The Guardian. Published February 4, 2016. Accessed May 26, 2016. URL = <https://www.theguardian.com/technology/2016/feb/04/us-police-data-analytics-smart-cities-crime-likelihood-fresno-chicago-heat-list >

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/>

Winner, Langdon (1980). “Do Artifacts Have Politics?”. In Daedalus, Vol. 109, No. 1, Modern Technology: Problem or Opportunity? Winter 1980. pp. 121-136.

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