Investigation of Relevant Social Groups in the FBI vs. Apple Dispute

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Steven Yi

23 April, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____
Rider Foley, Department of Engineering and Society

Introduction

Software technology is becoming an increasingly important part in our lives. As we grow to rely on technology more and more, it becomes an increasingly useful tool for law enforcement and other tools—devices that have effectively become surveillance tools (Grossman, 2016). This results in "serious tension" between privacy and safety, values that "we all treasure." (Comey, 2016) As a result, there is often controversy between government and other parties about what access the government should have to people's data. One of the most famous recent examples of this is the dispute between Apple and the FBI over the San Bernadino shooter's iPhone. Using that dispute as a case study, this paper seeks to analyze the reasons why groups either support or oppose encryption and privacy technologies.

Case Context: FBI vs. Apple Dispute

On December 2nd, 2015, a terrorist attack occurred in San Bernadino, California. Two perpetrators, Syed Rizwan Farook and Tashfeen Malik, entered a workplace holiday party and opened fire, killing 14 people and wounding 22. Afterwards, they fled the scene and were later killed by police officers in a shootout (Grossman, 2016). Once law enforcement officers searched the perpetrators' possessions, they found an iPhone running iOS 9, and it was passcode-locked. While the phone was technically owned by San Bernadino County, they did not have the passcode, and they could only attempt 10 passcodes (out of 10,000 possible combinations) before the data on the phone was wiped (Grossman, 2016). As a result, the FBI turned to Apple for assistance in unlocking the phone, asking for an updated version of the iOS operating system that would allow the FBI to attempt passcodes until the phone was unlocked (Blankstein, 2016).

Apple strongly refused this court order, and the dispute escalated, filing a court order in opposition (Just Security, 2016). Both the FBI and Apple continued to file opposing court orders,

with the FBI eventually invoking the All Writs Act in an attempt to force Apple to comply. Outside of the court, both sides published articles justifying their position. Tim Cook, the CEO of Apple, published a public letter on the company website detailing the company's position. He argued that the FBI's request would weaken encryption for everyone, opening iPhones to potential attacks. Additionally, Cook stated that the FBI's actions set a "dangerous precedent" and a gross overreach of government power in bypassing Congress (Cook, 2016). He was even quoted in an interview calling the FBI's request the "software equivalent of cancer." (Wagner, 2016)

The FBI's then-current director, James Comey, also publicly spoke up about the issue. He speculated that the data found on the iPhone could potentially lead to "finding more terrorists." (Comey, 2016) He invoked the duty of the FBI in investigating the issue to the fullest possible extent, but ultimately left the decision to the American populace.

This dispute between Apple and the FBI was closed on March 29, 2016, when the Department of Justice announced that they were able to bypass the passcode lock, accessing the data without Apple's assistance. As a result, they dropped all of the court orders (Segall et. al, 2016).

STS Theory

The Social Construction of Technology framework (SCOT), developed by Trevor Pinch and Wiebe Bijker, seeks to shed light on the development process of technology, and how the "tug-of-war" between social groups and their values leads to the resolution of any controversies surrounding the technology. A relevant social group is defined as some institution, or a group of individuals (organized or unorganized) that "share the same set of meanings, attached to a specific artefact." (Pinch and Bijker, 1984) Additionally, the framework heavily features the

concept of interpretive flexibility, where the interpretation and societal view of technological artifacts is fluid and can affect the design of technological artifacts. By this framework, there is no singular, ideal design for any given technology. Instead, "each participating group has its own, unique view of how the artifact should be made, based on its interpretation of the problem that the artifact is supposed to solve" ("Social Construction of Technology," n.d.).

The SCOT framework also can shed light on the end of any technological controversy, referred to as "closure and stabilization." In Pinch and Bijker's 1984 paper, they expound on two types of closure in the technological case: rhetorical closure and closure by redefinition of problem. In rhetorical closure, the problem is "seen" as solved, rather than being actually solved—essentially, the public interpretation has been changed, but the technology is unchanged. In the case of closure by redefinition of the problem, the technology is instead reinterpreted to solve a different problem than the one originally considered (Pinch and Bijker, 1984).

In the case of the Apple vs. FBI dispute, the controversial technology is Apple's iOS installed on iPhones. The most obvious relevant social groups are Apple and the FBI, both of which have separate and sometimes conflicting interests that affect their interpretation of iOS. As the FBI values the ability to obtain information it needs, it sees the ideal "artifact" (iOS) as a system that allows for the FBI to access information without direct assistance from the owner of the phone (or whoever knows the passcode). Apple, valuing privacy and thus an airtight system to protect iPhone data, sees the ideal iOS as one with no loophole previously stated by the FBI. A form of rhetorical closure was reached when the FBI was able to access the iPhone, bypassing Apple. As a result, they saw the problem (iPhone access in spite of a passcode) as solved.

Research Design

The research in this paper seeks to answer the question: How do different values of entities affect their interpretation of the case between the FBI and Apple over the San Bernadino shooter's iPhone? While this dispute between the FBI and Apple has been resolved for over five years, I believe analyzing this case can shed light on past, present, and future controversies of a similar nature.

The primary source of data was from *amici curiae* (also referred to as "amicus briefs"), a type of legal document filed by third parties, that were filed either in support of Apple or the FBI. Due to the relatively low number of *amici curiae* found, as well as the argumentative nature of each document, this research calls for more of a qualitative, rather than quantitative, analysis. All of the documents were of a similar format, where *amici* gave self-descriptions, sometimes also including brief descriptions of the party's values, followed by substantive arguments in support of their viewpoint to the case. As a result, analysis takes note of involved parties (and some description), then take note of arguments and notable points in the arguments, repeating for each legal brief.

For this research paper, I analyzed four amicus briefs—two in support of the FBI and two in support of Apple. One of the amicus briefs in favor of the FBI was written by three special interest groups: the Federal Law Enforcement Officer's Association (FLEOA), Association of Prosecuting Attorneys (APA), and National Sherriff's Association (NSA), while the other was written by lawyers on behalf of "close relatives of those killed." (Clayborn et. al, 2016) The two briefs written in support of Apple were written by the American Civil Liberties Union (ACLU), and the other was written by a group of private software technology companies, including Mozilla and Amazon.

Results

In analyzing the amicus briefs through the social construction of technology framework, there was a clear divide in values between those in support of the FBI and those in support of Apple. Social groups in support of the FBI primarily valued public safety and closure of criminal cases, and consequently supported the FBI's desire to obtain as much information as possible. Social groups in support of Apple, on the other hand, primarily valued individual privacy and a limited government, and thus saw the FBI's wishes as an overreach of government authority and a violation of individual privacy rights. In short, those supporting the FBI saw aggregate benefit as the greatest good, while those supporting Apple saw universally applied individual rights as the greatest good. Both groups, in accordance with their interests, focused on different aspects of the dispute, interpreted the FBI's legal authority to invoke the All Writs Act differently, and used slippery-slope arguments in favor of their position. Interestingly, both groups had some overlap in their arguments, and addressed concerns of either side.

Involved Parties	**Description**
FLEOA	"Monitors legislative and other legal issues that may impact federal officers."
APA	Advocates for attorneys on emerging issues
NSA	Represents sheriffs, deputies and other law enforcement and public safety professionals.
"Close relatives of those killed"	Desire for "no stone be left unturned"

Table 1. List and brief description of parties listed in amicus briefs filed in support of the FBI.

Looking at the parties listed in the table, there is clear overlap in interests. Three organizations work directly with law enforcement, and thus have an obvious interest in allowing law enforcement officers and those who are part of criminal investigations to be able to do their jobs well. The other group, those directly affected by the shooting, also have a stake in the FBI having the ability to gather as much information as possible. Since they want closure in the aftermath of the shooting, they want to know if the iPhone yielded any further information on the

shooting, whether people were “purposefully targeted,” or if the information pointed to a possible “unknown terrorist cell” or another perpetrator (Clayborn et. al, 2016).

Arguments	
"Apple's Refusal to provide reasonable assistance to the government hinders everyday law enforcement and endangers public safety"	"The All Writs Act Analysis Takes into Account the Extraordinary Circumstances Underlying the United States' Request"
"A ruling in favor of Apple here will have a chilling effect on public assistance to law enforcement"	"Apple’s Constitutional Arguments Are Unsupported by Both Case Law and the Facts"
"This Case is Not About Privacy"	"The United States' Request is Modest in Scope"

Table 2. List of all headers in the arguments section of two amicus briefs in favor of the FBI

There is a clear influence from the social groups’ values on the arguments they used to justify their position. As all of the social groups desire for the FBI to have more investigative powers, they see the technology as a hindrance to their values. They do not see the FBI’s request as an overreach of government authority, and see the All Writs Act as a valid legal justification for their position. Additionally, their interpretation of iOS and the issues raised by Apple were affected. While they concede that privacy is important, they do not see the All Writs Act and the FBI’s request as an infringement or potential infringement of individual privacy. This is in direct response to Apple, which raised significant concerns about user privacy as a major component of their argument for refusal.

Involved Parties	Description
ACLU	Appears in court cases “implicating Americans’ right to privacy”
Dropbox	“products are built on trust…[people] can trust [their data is] secure”
Mozilla	“mission…recognizes, among other things, individuals’ security and privacy…are fundamental”
Summary of companies	“customers…trust *amici* to safeguard their data”

Table 3. An abridged list of parties that filed amicus briefs in favor of Apple. Due to the large number of companies, most were cut out of this table.

In the parties in support of Apple, there are two clear relevant social groups. The first group is the political interest groups—the ACLU. As their name suggests, they are champions for individual rights ("civil liberties"), and thus highly value rights such as privacy. Corporations, on the other hand, have a profit motive (although it is worth mentioning that Mozilla is a non-profit, most of the other companies listed in the amicus briefs are for-profit organizations) and thus are obligated to cater to customers. As they believe that customers value data security and privacy, they also are obligated to value data security and privacy. This means that they have a significant stake in preventing the government from having direct access to customer data.

<table>
<tr><th colspan="2">Arguments</th></tr>
<tr><td>"The Government's Interpretation of the All Writs Act Is Unprecedented and Unnecessary"</td><td rowspan="2">"The All Writs Act does not authorize the government to compel Apple to create and authenticate software that would allow the government to break into Apple's customers' devices."</td></tr>
<tr><td>"The Law Does Not Allow Federal Agents to Conscript Companies into Defeating Their Own Security Safeguards and Product Designs"</td></tr>
<tr><td>"The Canon of Constitutional Avoidance Counsels Against the Government's Expansive Interpretation of the All Writs Act"</td><td>"The order the government seeks violates the Fifth Amendment"</td></tr>
</table>

Table 4. A list of argument headers in amicus briefs filed by the two groups in favor of Apple

The arguments are consistent with the values listed by the parties responsible for writing these amicus briefs. While not listed here, the opposition still believes the FBI should be able to investigate crimes—Apple has stated that they comply with what they believe to be valid legal orders (Cook, 2016)—however, they believe that the FBI has no more investigative authority than what is already afforded to them by the status quo. According to their values of individual privacy and security, these parties' interpretation of Apple's iOS is that it adequately protects privacy as it is, and any adjustments made to weaken that privacy is improper.

Discussion

The social construction of technology framework helps uncover a lot of the details surrounding this case, especially when using the concept of interpretive flexibility. In this case, we see a prime example of interpretive flexibility on iPhone security features. In the case of the ACLU and Mozilla et al., their ideal version of iPhone and its security features would ideally be impenetrable any party, whether governmental or not. On the other side, the government and shooting victims and relatives see their ideal form of iPhone security as one that is impenetrable to malicious parties, but theoretically accessible by government institutions with a kind of "master key" developed by Apple. In this, a "tug-of-war" happens in the counterarguments and debate as to whether a technology like that is feasible. As seen from the amicus briefs filed by companies in support of Apple, the government's proposal of a "master keyed" iPhone lock is unfeasible, as there would be no way to ensure that only governments that need the information in legal cases are the entities that can be granted access (ACLU et al., 2016).

This case study fits very well into a much broader debate on privacy and security. Many other controversies have occurred, such as the EARN IT act, a bill that was recently introduced in Congress. A similar debate occurred, and though some of the social groups changed (instead of victims of the San Bernadino shootings, the new relevant social group was those invested in ending child sexual exploitation), a lot of the arguments remained the same. Advocates in support of the EARN IT Act thought that the technology advocates' arguments were overblown ("What the EARN IT Act Does," 2020). Similarly, those in opposition to the EARN IT Act noted the possible threats to overall privacy, seeing as there is no feasible way to prevent malicious parties from using the same backdoors (ACLU and AFP, 2020).

The research conducted for this paper, though extensive, had its limitations. Most notably, the number of relevant social groups I could find was severely limited in number due to issues finding different amicus briefs. Different websites list nearly 20 amicus briefs in support of Apple ("A Reader's Guide," 2016), but a number of them could not be found. While four amicus briefs were enough to uncover a lot of information on the case, I firmly believe that being able to access some of the other amicus briefs would be able to open up even more insight into this case study.

The single most important improvement I believe I could make to this research paper is to broaden the scope of information I collected. Beyond being able to find the previously mentioned amicus briefs, I think expanding the types of information I collected would be insightful, too. If I were able to conduct interviews with relevant parties or otherwise collect more specific and detailed information beyond what I was able to find in the amicus briefs, I think I would be able to gain a much more pointed insight into this case.

This case study, regardless of its limitations, will have significant effects on my own engineering practice as I graduate and work professionally. Cybersecurity is becoming an increasingly relevant topic as software technology becomes an ever more prevalent part of our lives. When it comes to designing and building software, it's important to think of its social repercussions, and it is something I will need to be significantly more aware of when I build my own software. In addition, it would be important to me to stay informed on this greater privacy vs. security debate. Though it may never be resolved, I think it is, again, something to be very aware of in my own engineering practice, and perhaps may motivate me in what software I work on.

Conclusion

It is important to remember that this specific instance is just one example of many of larger disputes between technology and government (in this case, law enforcement). Based on my research, it shows that it is sometimes possible that there is no one right answer, or at least the "ideal" technology is likely unfeasible. As a result, controversies like the dispute between Apple and the FBI may continue to pop up. Awareness, and the humility to understand that the ideal solution that pleases everyone doesn't always exist, is something I believe to be very important in cases like this, and is something that should extend to all software engineers.

The research methods and concepts can definitely be expanded. Many cases exist where technology companies are at odds with government, and it's not always obvious that one side is in the right. I hope that this analysis can be a springboard into further analyses of different case studies.

Technology, in many cases, is not inherently "good" or "bad;" rather, its "goodness" lies in its uses. While a technology can bring a small amount of good to a large amount of people, it may also do a large amount of harm to a small group of people. Whether this is enough to deem something "good" or "bad" is a decision best left to each case. I hope this case study has proven a point—nothing is as clear-cut as we engineers may often want.

Works Cited

ACLU and AFP to congress: “EARN IT” act jeopardizes every Americans’ private communications. (2020, March 5). Americans for Prosperity. https://americansforprosperity.org/aclu-and-afp-to-congress-earn-it-act-jeopardizes-every-americans-private-communications/

Brief for American Civil Liberties Union et al. In Support of Apple, Inc, FBI v. Apple, Inc, (no. 5:16-cm-10-SP)

Brief for Federal Law Enforcement Officers Association et al. as Amici Curiae Supporting Government, FBI v. Apple, Inc, (no. 5:16-cm-10-SP)

Brief for Greg Clayborn et al., FBI v. Apple, Inc, (no. 5:16-cm-10-sp)

Brief of Amici Curiae Amazon.com et al. in Support of Apple, Inc, FBI v. Apple, Inc, (no. 5:16-cm-10-sp)

Comey, J. (2016, February 26). *We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead*. Lawfare. https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead.

Cook, T. (2016, February 16). *Customer Letter*. Apple. https://www.apple.com/customer-letter/.

Crocker, S. C., Aaron Mackey, and Andrew. (2020, March 31). The earn it act violates the constitution. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution

Graham, L. (2020, July 20). Text—S. 3398—116th Congress (2019-2020): EARN IT act of 2020 [Webpage]. https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

Grossman, L. (2016, March 17). *Apple CEO Tim Cook: Inside His Fight With the FBI*. Time. https://time.com/4262480/tim-cook-apple-fbi-2/.

Just Security. A readers' guide to the Apple All Writs Act cases. (2016, April 23). Retrieved April 23, 2021, from https://www.justsecurity.org/29634/readers-guide-magistrate-judge-writs-act-cases/

Newman, L. (2020, March 5). The earn it act is a sneak attack on encryption. Wired. https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption/

Perlroth, N. (2019, November 19). What is end-to-end encryption? Another bull's-eye on big tech. The New York Times. https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html

Pfefferkorn, R. (2020, March 5). The earn it act is here. Surprise, it's still bad news. /blog/2020/03/earn-it-act-here-surprise-it%E2%80%99s-still-bad-news

Pinch, Trevor J., and Wiebe E. Bijker. "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other." Social Studies of Science, vol. 14, no. 3, 1984, pp. 399–441. JSTOR.

Rozenshtein, A. (2020, March 10). The revised earn it act proposes a better process for encryption policy. Lawfare. https://www.lawfareblog.com/revised-earn-it-act-proposes-better-process-encryption-policy

Social construction of technology (SCOT). (n.d.). Retrieved February 23, 2021, from https://web.archive.org/web/20180410205247/http://www.stswiki.org/index.php?title=Social_construction_of_technology_%28SCOT%29

Wagner, L. (2016, February 25). *Apple CEO Tim Cook: Backdoor To iPhones Would Be Software Equivalent Of Cancer*. NPR. https://www.npr.org/sections/thetwo-way/2016/02/24/468016377/apple-ceo-tim-cook-back-door-to-iphones-would-be-software-equivalent-of-

cancer#:~:text=Debate%20Over%20Encryption-,Apple%20CEO%20Tim%20Cook%3A%20Backdoor%20To%20iPhones,Be%20Software%20Equivalent%20Of%20Cancer&text=Ariel%20Zambelich%2FNPR-,Apple%20CEO%20Tim%20Cook%20says%20creating%20new%20software%20to%20break,News%20Tonight%20with%20David%20Muir.&text=%22Some%20things%20are%20hard%20and%20some%20things%20are%20right.

What the EARN IT Act Does. (n.d.). NCOSE. Retrieved October 18, 2020, from https://endsexualexploitation.org/wp-content/uploads/What-the-EARN-IT-Act-Does.pdf