Apple and the FBI: Divergent Ideas About Privacy and Security

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Sam Shankman

March 26, 2020

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 _____
Peter Norton, Department of Engineering and Society

Apple and the FBI: Divergent Ideas About Privacy and Security

On December 2, 2015, there was a shooting in San Bernardino, California. The FBI found an iPhone 5C, running iPhone Operating System (IOS) 9, that was owned by a culprit (Comey, 2016). In 2016, the FBI got a court order for Apple to disable the IOS "auto encryption feature" (Comey, 2016). Apple refused as they did not want to make an IOS version that "would create a backdoor" to encryption (Cook, 2016). Apple did not want to cause a "breach of privacy" to their users (Cook, 2016). With the FBI fighting for security and Apple fighting for privacy, divergent ideas about privacy and security in the United States were revealed. Apple and the FBI alone are not enough to establish divergent views. Instead, the reactions of many participant groups must be observed to reveal divergent views.

Privacy is often viewed as an essential part of security or as a value competing with security. There is no consensus on whether privacy or security is more important. 93% of American adults value privacy and "being in control of who can get information about them," but only 6% of American adults are "very confident" that government agencies can keep their information private (Madden & Rainie, 2016). Belanger et al. (2002) found that people value "security features" over other "trust indices" such as privacy.

Cultures differ in how much they value privacy; cultures that emphasize individuality value privacy more than cultures that value the group more than the individual (Larson & Medora, 1992). For security purposes, some countries have tried to censor citizens, control information access, and limit privacy by banning virtual private networks and Tor. (Tor Project, 2019).

In 2006, the Greek government had wiretapping capabilities put into mobile phones. This privacy reduction was meant to increase security, but became a security issue when a third-party intercepted communications between the Greek Prime Minister and other officials (Chandler, 2007). Increasing surveillance for security reasons while reducing privacy is a common response to terrorism. Examples include the United States' Patriot Act, Canada's Anti-Terrorism Act, and India's Unique Identity Project (Hiranandani, 2011). Increasing surveillance creates new attack vectors as communications can be intercepted and collected data can be stolen or leaked.

Other than Apple and the FBI, many participants are linked with divergent views on privacy and security. The National Sheriffs' Association wants law enforcement to be free to "fulfill its obligation to investigate crimes" (LaBahn et al., 2016, p. 3-4). The Electronic Privacy Information Center (EPIC) stands for consumer rights to strong encryption and they support "the protection of privacy and personal data" ("Apple v. FBI," 2016). The California State Sheriffs Association' Association, however, claims the FBI is "hampered in its efforts to provide for the public's safety" due to Apple's actions (Mayer et al., 2016, p. 4). The American Civil Liberties Union (ACLU) does not want the FBI to force Apple to "go beyond the well-established duties of citizens to aid law enforcement" (Sweren-Becker, 2016). The Electronic Frontier Foundation (EFF) does not want to set a legal precedent that makes companies undermine customer security protections (Buttar, 2016).

The 2016 iPhone case, originating in San Bernardino, California, and the following FBI investigation exposed a divide in organized groups' views of security in the United States. To the FBI and their supporters, privacy conflicts with security, but to Apple and their supporters, privacy is essential to security.

Review of Research

Madden & Rainie (2016) found that 93% of Americans value privacy and controlling who can get information about them, but only 6% of Americans are confident that government agencies can keep their information private. The researchers did not consider the relationship of privacy and security. Belanger et al. (2002), found that most Americans think security is more important than privacy. They regard privacy as a "trust index" rather than a security feature. The researchers looked at trust (and thus privacy) as a value competing with security, and did not consider trust and privacy as part of security. Ecommerce consumers have come control over their personal information. There was no similar choice in the 2016 iPhone case. Looking at the interaction between privacy and security is important in both cases.

Larson & Medora (1992) found that cultures differ in how much they value privacy. Cultures that value the individual more value privacy more while cultures that value the group more value privacy less. The study focused on American culture valuing the individual, and thus privacy, more than Indian culture.

Coley (2017) studied divergent cultural values about privacy between the European Union and the United States. The European Union holds privacy as a fundamental human right, partly due to the fear of "dangers posed by an omniscient totalitarian authority in power" (p. 1117). Americans tend to view personal data collection as an economic opportunity. The United States limits "governmental data processing, while facilitating a market-oriented allowance for data processing in the private sector" (p. 1117). According to Coley, by the standards of the European Union, U.S. privacy laws are deficient. Coley claims the stricter European laws limit freedom but promote happiness while the loose U.S. laws promote freedom and happiness. Coley interprets the European Union's stricter laws as meaning that to the European Union happiness

and freedom are opposing forces (p. 1118). Coley claims “happiness to many U.S. citizens is freedom” (p. 1118). Divergent values on privacy correspond to divergent views on happiness and freedom.

Shi (2001) studied the relationship between cultural values and political trust, finding that “cultural orientation plays a critical role in shaping people's attitudes towards their government” (p. 415). Shi found that in Taiwan, political trust is influenced more by government performance, while in the People’s Republic of China (PRC), political trust is based on traditional values. Shi contends if people trust their governments for different reasons, then “studies of political trust that do not probe its source” fail to understand the different societies (p. 415).

Law Enforcement

In its response to the 2016 iPhone case, the FBI showed it views privacy as inconsistent with security. In a speech referring to the 2016 iPhone case, James Comey, director of the FBI from September 2013 to May 2017, said the FBI had to use “all lawful tools to find out whether there was evidence on that phone” (Comey, 2016). He claimed “the notion that privacy should be absolute, … just makes no sense given our history and values.” Comey argued that there is “no such thing as absolute privacy in America,” even stating that “all of those zones of privacy can be pierced if a court finds compelling reasons to do so.” He contended the reason that courts can take away privacy “to achieve two things we all treasure, liberty and security,” and that America has had to balance privacy and security. He also claimed that high levels of privacy make it difficult for the FBI to catch criminals.

The goals of the FBI are to “protect the American people and uphold the Constitution of the United States,” thus promoting security (Mission & Priorities, n.d.). In his speech, Comey

argued that privacy may have to be compromised so the FBI can fulfill these goals. On February 16, 2016, the FBI secured a court order requiring Apple to help the FBI unlock an iPhone owned by one of the San Bernardino shooting culprits so as to "bypass or disable the auto-erase function" of the iPhone. The FBI could then test passcodes and access the iPhone without losing information on the device (Decker, 2016). The court order for a backdoor to encryption directly compromises privacy so the FBI can meet its goals.

In response to the 2016 iPhone case, United States law enforcements groups showed they view privacy as being inconsistent with security. Together, the Federal Law Enforcement Officers Association, Association of Prosecuting Attorneys, Inc., and the National Sheriff's Association submitted an amicus curiae brief in support of the FBI. These groups claimed that Apple's refusal "has far-reaching public safety ramifications" that make it hard for law enforcement to fulfill its duties (LaBahn et al., 2016, p. 3-4). This amicus curiae brief said that if Apple can refuse lawful court orders, then "public safety will suffer" (LaBahn et al., 2016, p. 4). The brief stated that making iPhones harder to search, due to the encryption and increased privacy, has been "impeding and damaging investigations in law enforcement offices around the country" (LaBahn et al., 2016, p. 4). The three groups that submitted this amicus curiae brief value doing their jobs in order to protect the public, promote safety, and promote security. They think the encryption and privacy in iPhones gets in the way of their jobs, thus privacy is inconsistent with their idea of security.

Together, the California State Sheriffs' Association, California Police Chiefs' Association, and California Peace Officers' Association also submitted an amicus curiae brief in support of the FBI. This brief said that Apple's failure to help unlock the iPhone has "hampered" law enforcement "in its efforts to provide for the public's safety" (Mayer et al., 2016, p. 4). This

brief stated the "argument that pits the privacy interests … against the needs of a government investigation" is misplaced (p. 1). The brief claimed this argument is misplaced as "Apple can be in exclusive control of the methods to unlock this iPhone," thus privacy should not be at risk (p. 2). However, the brief then claimed that a "potential disclosure" of these methods "cannot outweigh the present compelling need of the public to be protected" (Mayer et al., 2016, p. 2). These groups do not think the iPhone case directly compromises privacy in favor of security. However, they value law enforcement, even at the cost of privacy.

In February, 2016, there was an interview with Cyrus Vance, an attorney representing the Manhattan District in New York. Vance mentioned that encryption on iPhones makes law enforcement "unable to perform [its] function to protect the public" (Martin, 2016). Vance stated that due to iPhone encryption, the Manhattan District cyber lab could not access "about a quarter of the phones" evaluated (Martin, 2016). Vance then said this "affects our ability to gather all the evidence … and make the right judgement as to whether or not we can go forward" (Martin, 2016). Vance stated that "a balance between privacy and public safety" must be found (Martin, 2016). Like the two amici curiae briefs, the Manhattan District wants to do its job and promote public safety and security but believes encryption on iPhones inhibits this. Law enforcement views the privacy provided by encryption as a barrier to their jobs, thus privacy is inconsistent with security to them.

Consumer Technology Companies

In response to the 2016 iPhone case, Apple showed they view privacy as being part of security. Apple believes there are criminals who want to "access, steal, and use" the personal information of others. Because of this, Apple thinks "compromising the security of our personal

information can ultimately put our personal safety at risk" (Cook, 2016). Apple thinks the requested backdoor to encryption would "undermine decades of security advancements that protect our customers" (Cook, 2016). Apple views privacy as a key part of security in order to protect their customers.

In response to the 2016 iPhone case, consumer technology companies showed they view privacy as being part of security. Two groups of consumer technology companies submitted amicus curiae briefs in support of Apple. The first brief came from Airbnb, Atlassian, Automattic, Cloudflare, eBay, GitHub, Kickstarter, LinkedIn, Mapbox, A Medium Corporation, Meetup, Reddit, Square, Squarespace, Twilio, Twitter, and Wickr. This brief claimed that the FBI's request "threatens the core principles of privacy, security, and transparency that underline the fabric of the internet" (Roth et al., 2016, p. 3). Due to the threat of digital wrongdoers, these groups believe handling user data in a "safe, secure, and transparent manner that protects privacy" is important (p. 4). The companies claimed a forced backdoor makes companies undermine "promised security measures" that are "essential to protection of [their] users' data" (p. 5). The companies said data privacy has become "increasingly vital as more … threats have emerged" (p. 7). Identity theft is one such threat. The companies claimed making a backdoor just makes more "opportunit[ies] for criminals and hackers to exploit" iPhones (Roth et al., 2016, pp. 12-13). These consumer technology companies seem to value protecting consumers from modern digital attacks. In order to provide security against these attacks, the companies claim that privacy is necessary.

The second group that submitted an amicus curiae brief incudes Amazon, Box, Cisco, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo. These companies claimed the 2016 iPhone case forces companies to

"circumvent security features that protect their customers' sensitive information from hackers and criminals" (Maddigan & Katyal, 2016, pp. 5-6). The brief listed combating trade secret theft as a focus of data privacy and cybersecurity. It is also mentioned that any backdoors inserted "can be exploited by hackers as well" (Maddigan & Katyal, 2016, pp. 5-6). Like the first amicus curiae brief, the companies involved with the second brief do not want customers to be at risk of modern digital security threats. Privacy is a way to achieve this, thus these companies view privacy as part of security.

The second brief stated that engineers will have to make new software to "undermine security features previously designed" (Maddigan & Katyal, 2016, p. 16). They claimed making new software fundamentally alters products and the new version are no longer the same products. The companies do not wish to modify their products "for the FBI in ways that are contrary to their core values" (p. 17). The companies do not want to write new software "against their will" (Maddigan & Katyal, 2016, p. 23).

There are claims that Apple "has set up an argument that pits the privacy interests of its users' data against the needs of a governmental investigation" (Mayer et al., 2016, p. 1). For all the involved technology companies which support Apple, their customers are their livelihood. It is reasonable for the companies to favor what their customers want. Although not directly stated, these companies seem to think their customers value privacy. As mentioned by the technology companies, this is to limit various cybersecurity threats. In order to protect their customers from the threats, privacy is needed as an essential part of security.

Civil Liberties Groups

In response to the 2016 iPhone case, civil liberties groups showed they view privacy as being part of security. The Electronic Privacy Information Center (EPIC) and eight other consumer privacy organizations submitted an amicus curiae brief in support of Apple. In this brief, privacy is supported as part of security as removing encryption means "consumers will suffer" and "crime will increase" (Butler et al., 2016, p. 5). The EPIC's brief claimed victims of information theft "lose valuable personal data and face an increased risk of identity theft" (p. 8). The EPIC supports encryption as there were "significant reductions in iPhone theft following the release of the new security features" (p. 12). Epic stated that many "services can be unlocked using [iPhones]" such as control over household appliances, financial services, remote file storage, remote desktops, and medical records (Butler et al., 2016, p. 23). The EPIC does not want these services to be at risk due to lack of privacy on iPhones.

The Electronic Frontier Foundation (EFF) thinks the FBI's demand would "risk the security of millions of other devices" and their users by disabling encryption (Buttar, 2016). In the wrong hands, the EFF thinks the desired tool could "infiltrate Apple systems." The EFF was also concerned about setting a precedent where dictatorships could demand company compliance as and use it as a "new way to oppress people." The EFF mentioned powers made in response to terror attacks are "eventually abused" and they do "more damage to our security than the tragic events that prompted their creation" (Buttar, 2016). The EFF was afraid of setting precedents that allow governments to abuse powers and harm citizens. They believe the encryption on iPhones helps prevent potential abuses of people, thus they think privacy is a part of security.

The American Civil Liberties Union (ACLU) submitted an amicus curiae brief in support of Apple. The brief showed concern that the FBI's desired tool would impact "Apple's millions of customers" (Bibring et al., 2016, p. 9). The ACLU brief claimed that removing encryption in

iPhones will cause consumers to lose trust in software security updates. The ACLU believes this will have “catastrophic consequences for digital security and privacy” (Bibring et al., 2016, p. 10) They think that without trust, people will not install important security updates to their devices. Since the ACLU believes the encryption in iPhones is a part of that trust, a loss of privacy could lead to future security updates not being installed. The ACLU also is concerned about cybersecurity threats. They said President Obama identified cyber threats as one of the biggest “national security challenges we face as a nation” (Bibring et al., 2016, p. 10). The brief mentioned “three in five Californians were affected by a [cyber] security breach” since 2012 (Bibring et al., 2016, p. 11). The ACLU claimed that Apple’s encryption is vital to “protecting hundreds of millions of people from sophisticated cyberattacks” (p. 11). The ACLU thinks a backdoor to encryption would put people at a larger risk of cyberattacks. Thus, the ACLU values privacy as a part of encryption.

Conclusion

It seems that the 2016 San Bernardino case did expose a divide on the views of privacy and security. Law enforcement and the FBI viewed privacy as an opposition to security while Apple, consumer electronic companies, and civil liberties groups viewed privacy as essential to security. The reasons for these views were based upon what the different groups valued. Law enforcement groups did not dislike privacy on its own, but disliked privacy when it got in the way of doing their jobs. For them, privacy should be removed for a greater good. This is an example of the ends justifying the means.

To Apple and consumer electronics companies, privacy was essential to security. The stated reason was to protect consumers from threats due to lack of privacy. There was also the value of

doing what they believed the consumers wanted as consumers are the financial livelihood of the companies. This is an example of manifest and latent functions. The businesses say they are doing something to look out for their consumers, but they also are acting based on their financial interests.

To civil liberties groups, privacy was essential to security. They were concerned about cyber threats due to lack of privacy. This may be an example of knowing what is truly desired in the long run. These groups desire to protect people. Instead of acting based on what will protect people immediately, these groups act based on what protects people now and in the future.

This research was limited to organized social groups in the United States. Further research on unorganized social groups in the Unites States and all social groups outside the United States may be beneficial. Research on how precedent impacted this case and how it may impact future cases may be valuable. Research about security and privacy in countries that limit privacy could shed a new light on the issue. Finally, quantitative research on the risks due to lack of privacy may shed better light on this research.

References

Apple v. FBI: Concerning an Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone. (2016). epic.org/amicus/crypto/apple/.

Belanger, F., Hiller, J., & Smith, W. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3), 245-270. ScienceDirect.

Bibring, P., Abdo, A., Lye, L., & Loy, D. (2016). Brief of Amici Curiae American Civil Liberties Union, ACLU of Northern California, ACLU of Southern California, and ACLU of San Diego and Imperial Counties, in Support of Apple, Inc. Los Angeles, California.

Butler, A., Rotenberg, M., & Thomson, A. (2016). Corrected Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) and Eight Consumer Privacy Organizations. Washington, D.C.

Buttar, S. (2016). Apple, Americans, and Security vs. FBI. www.eff.org/deeplinks/2016/02/apple-americans-and-security-vs-fbi.

Chandler, J. (2007). Privacy versus National Security: Clarifying the Trade-off. *Conference Papers: Law & Society.* Law and Society Association.

Coley, A. (2017). International Data Transfers: The Effect of Divergent Cultural Views in Privacy Causes Déjà Vu. Hastings Law Journal, 68(5), 1111-1133. repository.uchastings.edu/cgi/viewcontent.cgi?article=1026&context=hastings_law_journal.

Comey, J. (2016). Expectations of Privacy: Balancing Liberty, Security, and Public Safety. FBI. www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety.

Cook, T. (2016). Customer Letter. www.apple.com/customer-letter.

Decker, E., Donahue, P., Wilkison, T., & Chiue, A. (2016). Order Compelling Apple, Inc. to Assist Agents in Search. Los Angeles, California.

Hiranandani, V. (2011). Privacy and security in the digital age: contemporary challenges and future directions. *International Journal of Human Rights, 15*(7), 1091-1106. Taylor & Francis Online.

LaBahn, D., DeMarco, J., & Sen, U. (2016). Brief of Amici Curiae Federal Law Enforcement Officers Association, Association of Prosecuting Attorneys, Inc., and National Sheriffs' Association in Support of the Government's Motion to Compel Apple, INC. to Comply with this Courts February 16, 2016 Order Compelling Assistance in Search. Washington, D.C.

Larson, J., & Medora, N. (1992). Privacy Preferences: A Cross-Cultural Comparison of Americans and Asian Indians. *International Journal of Sociology of the Family, 22*(1), 55-66. JSTOR.

Madden, M., & Rainie, L. (2016). Americans' Attitudes About Privacy, Security and Surveillance. www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance.

Maddigan, M., & Katyal, N. (2016). Brief of Amci Curiae Amazon.com, Box, Disco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo in Support of Apple, Inc. Los Angeles, California.

Martin, R. (2016). It's Not Just The iPhone Law Enforcement Wants to Unlock. NPR. www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock

Mayer, M., Touchstone, J., & Preziosi, T. (2016). Brief of Amici Curiae and Memorandum of Points and Authorities in Support of Amici Curiae Brief. Washington, D.C.

Mission & Priorities. (n.d.). www.fbi.gov/about/mission.

Roth, J., Ring, R., Blavin, J., Patashnik, J., & Green, A. (2016). Brief of Amici Curiae Airbnb, Inc.; Atlassian Pty.Ltd.; Automattic Inc.;Cloudflare, Inc.; eBay Inc.;GitHub, Inc.; Kickstarter,Pbc; LinkedIn Corporation;Mapbox Inc.; A Medium Corporation; Meetup, Inc.;Reddit, Inc.; Square, Inc.;Squarespace, Inc.; Twilio Inc.; Twitter, Inc.; and Wickr Inc. San Francisco, California.

Shi, T. (2001). Cultural Values and Political Trust: A Comparison of the People's Republic of China and Taiwan. *Comparative Politics, 33*(4), 401-419. JSTOR.

Sweren-Becker, E. (2016). Why We're Defending Apple. www.aclu.org/blog/privacy-technology/internet-privacy/why-were-defending-apple.

Tor Project. (2019). Run Tor Bridges to Defend the Open Internet. blog.torproject.org/run-tor-bridges-defend-open-internet.