Chapter Five: The San Bernardino iPhone Case

Tracy Mitrano, University of Massachusetts - Amherst
CHAPTER FIVE: THE SAN BERNARDINO IPHONE CASE

Introduction

The San Bernardino iPhone case burst on the scene as I was nearing the completion of this manuscript. I could not have imagined a better scenario to sum up the issues of free speech, privacy, intellectual property, and security than this case. Not least because the San Bernardino Apple iPhone case generated considerable public interest and policy debate in the United States and abroad. At stake are issues such as the balance between national security and personal privacy, tensions between global technology companies and domestic law enforcement, and the potential supremacy of technology — particularly encryption — over traditional notions of public safety, as expressed in constitutional due process. At the root of this discourse is a more fundamental, and also more abstract, notion of trust between the government and its citizens, including questions about the role consumer rights plays in light of the market manifestations of personal information as a global commodity.

Facts

The basic facts bear repeating. The Apple iPhone in question was the property of the San Bernardino county government, employer to one of the two shooters, Syed Farook, in a terrorist attack that killed 14 and wounded 22 people. Warrants for information on the phone that had not already been obtained from its iCloud backup were attached on two grounds: consent of the owner, and the obvious probable cause of criminal activity that had already occurred. In order to obtain that information, the Federal Bureau of Investigation (FBI) required technological assistance to defeat the encryption key in the Apple iPhone’s operating system. Apple designed the key to wipe the hard drive clean of content after more than ten failed attempts to access a time-sensitive, touch-screen sign-in system. In lieu of more contemporary legislation that maps legal access to encryption technologies, the FBI brought an All Writs Act demanding third-party assistance of Apple to access the phone. In immediate response to this claim, Apple Inc. CEO Tim Cook published a passionate blog post that cited fear of physical harm and loss of privacy to individual consumers if Apple were to comply. As the FBI continued to pursue its claim in U.S. Federal District Court for the Central District of California, a national and international debate arose over the issue. In the midst of that debate, and just days before oral arguments, a private security firm offered to circumvent the encryption for the FBI. Once the iPhone was “unlocked,” the FBI withdrew the Writ.

Legal Issues
Due Process

A number of legal issues inform this case. The first is the use of the All Writs Act. This law was established in the same year as ratification of the Constitution, 1789. With the establishment of a federal government arose the need for a law that would facilitate the government’s ability to obtain evidence. In this case, it involved the authority of the federal government to impose legal demands upon third parties to act in the name of that facilitation. Notably, at the same time as the promulgation of this law, James Madison, “Father of the U.S. Constitution,” submitted in the first House of Representatives a series of amendments to the Constitution that would become by 1791 the first ten amendments, or the Bill of Rights. Transcendent above any one individual amendment is the foundational concept of “due process,” while the Fourth, Fifth, Sixth, and Seventh Amendments address themselves to concrete procedures incorporating that concept. Relative to the All Writs Act, the Fourth Amendment in particular would cabin the federal government’s power to obtain evidence. The All Writs Act has remained an important tool for federal law enforcement, having the appropriate checks and balances that the Fourth Amendment jurisprudence in criminal procedures provides. And in more recent articulations, pursuant to communication technologies, the courts have approved the All Writs Act to function in this same capacity. See United States v. New York Telephone Co.

Encryption

Opponents of the government’s position distinguish between communication technologies and the security cryptography, more popularly known as encryption. Encryption uses mathematical formulas to scramble the legible content of text into illegible numbers, letters, and symbols. Authentication “keys” are required to decrypt the text. These “keys” may be in the form of passwords, fingerprints, or retina scans, etc. In this case, the user entered a four-digit code to unlock the phone. After the tenth failed attempt within a prescribed time period, the operating system would automatically wipe the phone of its contents.

Because the phone was owned by the San Bernardino county government, the FBI was in possession of the original password Syed Farook used on the phone. The FBI changed the password in order to protect the contents of the iCloud backup. But the gap in time from the last backup until the date of the shootings prompted the FBI’s desire to access the phone. Once the password was changed in iCloud, the ability to access iCloud from the phone was no longer possible, and authentication by the phone to iCloud would fail. The FBI then demanded that Apple write a code correction to its operating system software...
to disable the portion that would wipe the phone of its contents after unsuccessful attempts.

Rather than allow the legal team to handle the matter, CEO Tim Cook responded with an impassioned blog post that took the case from courtroom to public opinion. In his post, Cook drew an immediate connection between disabling the encryption and the creation of potential personal safety threats. He invoked a concern for user privacy, playing on public reaction to Edward Snowden’s revelations related to government electronic surveillance; and he increased that anxiety by referring to the use that politically oppressive foreign powers, such as the People’s Republic of China, might deploy for its own ends if offered the technical ability to access both its citizens’ and foreigners’ phones. Finally, he alleged that the government’s demand for access to this particular phone was, in essence, a tactic to achieve the strategic ends of government “backdoor” access as standard operating procedure for the industrial use of encryption technologies.

Apple’s legal team responded with five principle arguments. First, it distinguished the encryption technologies between the New York Telephone Company and other communications’ technology precedents on the grounds that the nature of the technology in question is different. Thus, from a public policy perspective, it would behoove Congress to pass legislation that would address encryption and other Internet and digital technologies directly, although it is not outside the scope of the All Writs Act to function in the absence of revised law, such as the Communications Assistance Law Enforcement Act. Second, it distinguished this case from precedent on the grounds that it would require affirmative efforts on the part of Apple and its employees to rewrite operating system code. As novel as this depiction of the demand may appear, it falls under a standard defense in Federal Code of Criminal Procedure, the “undue burden” clause. Third, Apple made a “slippery slope” argument: “[W]hat is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone’s user?” Fourth, Apple asserted a position that “code is speech.” Related to that position, and fifth, Apple posited that to rewrite the code amounts to compelled speech and viewpoint discrimination in violation of the First Amendment.

Factual Conclusion of Case
Only days before oral arguments were scheduled to begin, the FBI requested an extension. A private “white hat” hacking firm had approached the Bureau alleging they had the technical ability to defeat the encryption and to provide the FBI access to the phone’s contents. A few days later, the FBI reported that such actions had occurred. Security experts have reported that the hacker deployed a “zero-day” vulnerability in the code — which is a known flaw that Apple had yet to patch — to circumvent the encryption. With access to the phone, the FBI withdrew their request. A number of other cases throughout the country are in litigation and/or on appeal concerning access to Apple iPhones. New operating systems, featuring more sophisticated firmware and software encryption, suggest that this general fact pattern will occur again, but without publicly known “zero-day” vulnerabilities, which have placed the government in a position similar to that represented in this case.

Discussion of Legal Issues

As those cases make their way through the courts, or not, the public policy matters brought up by CEO Tim Cook and Apple’s legal team remain of interest. Whether the courts will come to regard code as speech lies with future legal action. Even if it were, it is entirely possible that, as the property of a for-profit company, courts may declare it “commercial speech” and therefore entitle it to less protection than “political” speech. The “slippery slope” argument remains an important one. One distinction that the government might make is to note that in this case, they were asking for stored information and not for on-going surveillance; future cases will be challenged to draw careful lines of demarcation, and perhaps create specific tests for particular circumstances, in order to cabin the threat of government overreach. As a legal matter, the “undue burden” position is the most supported by precedent. Because it is a factual matter, it would have probably been the most discussed at oral argument. As a result of the premature termination of the case, however, it remains open for use in other cases without precedent. Nevertheless, the government will likely demonstrate the relative ease with which the independent hacker firm was able to circumvent the encryption, as support against a defense of undue burden, at least in its traditional sense of the effort that a government request makes upon a third party under the All Writs Act.

Public policy and legal questions surrounding encryption technologies continue to animate discourse over this case. From a purely technological perspective, Apple’s contention that code designed to defeat encryption would render the value of encryption useless bears weight. This point has market, brand, personal privacy, political, and government surveillance associations tied to it. Personal safety affects everyone from, for example, a gay or transgendered person who lives in a hostile environment, or, for that matter, a political dissident. Market
concerns about the viability of Apple’s brand in the face of devalued encryption surely play a role, one that did not escape the notice of the other four major Internet technology companies: Microsoft, Facebook, Amazon, and Google, all of which signed onto briefs in support of Apple. Whether or not a win of this case on the part of the government would open the floodgates and would result in a “back-door” access remains a serious public policy consideration, especially in light of the Obama administration’s decision not to pursue such regulation over Internet and technical security industries.

The notion of “evidence-free zones” transcends more legalistic arguments made on the government’s behalf. This notion suggests that to make a technology immune to legal due process results not only in a legal precedent hitherto unknown in U.S. law, but also sets a dangerous one that terrorists and criminals will exploit, with national security and public order hanging in the balance. Moreover, an objection to “evidence-free zones” complements the Obama administration’s decision not to pursue “backdoor” encryption. The abandonment of that policy, in effect, states that the government will not compel Internet companies to supply a “master key” that defeats encryption proactively, and applies across-the-board to all encryption technologies, but only on the assumption that in properly served, specific cases such access can and will be made available. Herein lies the question of “precedent,” widely touted in the media as a concern in support of Apple’s defense. In fact, precedent is a neutral concept and can operate either to support the government or Apple in this, or any other, case. It matters only in exactly what kind of precedent is set and how in future cases it is deployed. To most observers, neither extreme of “evidence-free zones” nor a default “backdoor” master key are satisfactory conclusions. Reliance on the courts to make the appropriate legal distinctions, and ultimately the correct decisions taking the Constitution and its principles of due process into account on a case-by-case basis, is the only practical approach that U.S. society can make on this question.

The final word goes to “trust.” Many a commentator on this case, from industry and the public to privacy advocates including legal scholars, eschewed more traditional legal arguments about the case in favor of using this case as the platform to express deep, ongoing concern over government surveillance. In the aftermath of the Snowden revelations, and very little corrective government action to show for it — including the watered down Freedom Act of 2015 that was originally designed to fix some of the most glaring concerns over the bulk collection of metadata — this case popped the lid off of simmering anxieties about governmental overreach into the privacy of people’s activities and lives. It is critical that politicians and government officials take note of the degree of that mistrust and enact the many reforms that could begin to right the balance. Such reforms might include breaking up the National Security Administration and putting it under greater degrees of transparency and public scrutiny; abolishing
the Foreign Intelligence Surveillance Act and its “secret, ex parte courts”; and more robust legislation and federal agency regulation of the industry’s collection, sale, and use of personal data and information.

Until such time as the larger questions about citizen and consumer expectations of privacy are addressed as being of central importance in our democratic republic, individual cases such as the Apple iPhone case will continue to act as flashpoints for these concerns. And it would be a pity if that remained the case. The unintended consequences of laying all that concern onto the outcome of a specific case may come to have a detrimental effect on the society overall, particularly if it results in extreme directions, such as either “evidence-free zones” or “back-doors.” It has never been more important to be precise and on point about matters related to privacy and the personal autonomy that privacy supports in both citizens and consumers. To be sure, being thoughtful and on point is difficult work. It takes time, intelligence, and effort to separate the issues and address them each in kind. But just as the old saw about “democracy” goes — that it is better than the alternative — so too with this exercise. Not to do so could be an invitation to undermine one of the most precious gifts that the United States has historically offered the world: a never perfect but nonetheless shining example of the rule of law.