Shane Avery

Professor Jordan

Law 017

May 22, 2016

Do Lawyers Dream of Digital Sheep?

Introduction

Thesis Statement

Apple, Inc. cannot allow the FBI access to the San Bernardino terrorists' cell phones because it violates the First and Fourth Amendments of the United States Constitution.

Society has seen many stages: the dark ages, the industrial age, the technology age and now the digital age. Adaptations by populations during each age were necessary to continue a functional and civil way of life. One of the most important civil areas that require being ahead of the curve to secure our civility in an ever-changing world is the judicial branch. Why is the level of government power in a digital era so important? In this day and age in America, I believe we may take our innate rights for granted due to having them from our first breath. Believe it or not, only a third of the world has the right to free press, speech and religion. It's 2016. We are fortunate that we have enjoyed these freedoms for a couple of centuries, but the majority of the world still does not. We need to treat those rights as being sacred and be wary of any power trying to interrupt or intercept them.

Scope of the Paper

The dilemma of this situation is obvious and makes it controversial and tough to pick a side. On one side you have persons who fear for the safety of our nation against terrorists; a seemingly endless

battle. They would allow the representatives of the government (in this case the FBI) to force an entity (Apple, Inc.) against its will to rewrite software to decrypt an item belonging to a known terrorist. It makes sense, I get it. You want to gain all evidence possible to convict all members involved in this tragic attack and quite possibly prevent any future attacks by giving the government the power to break-in the individual's cell phone.

However, situations like this are never cut so clear. Black and white? No. A big gray void to be exact. The consequences when you dig deep can get very foggy and convoluted, which is why there is such a strong resistance to allowing the government that power. The concern is that it will set a precedent of power. Big Brother, which can at times push its weight around very willingly will seize an additional opportunity to tap into the personal lives of its citizens if Apple doesn't fight back against this proposition. What will stop the FBI from demanding AT&T, or T-Mobile, or Sprint, etc. from breaking into your phone if you are suspected of anything? Maybe, you are curious to learn more about Muslim culture and you use your phone to browse the internet. Perhaps, you made a college friend who happens to be Muslim and you stay in touch with them. What if the FBI becomes suspicious of your activities? What will stop them from demanding access to big corporate's customers' information. I paint this hypothetical scenario and play devil's advocate because it very well could happen. Maybe, the idea is extreme, but there's that old saying, "Give'em an inch and they'll take a mile." If Apple gives-in on this it makes it easier down the line for government entities to ask and put pressure on these corporations. If that happens, then soon enough they will become omniscient knowing every step you take. There will be no boundaries. Information will flow to them freely on demand. Nothing will be sacred. There will no longer be freedom to (…fill-in..). You will no longer be a free citizen; it will be a masked totalitarian society.

First Amendment on Two Fronts

Hardly with any limits, and standing sturdy 200 plus years later; the foundation of which America's modern civilization lies on is the First Amendment of our Bill of Rights: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; ***or abridging the freedom of speech,*** or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[1]

Front #1: Where does the line get drawn in the digital age for what is considered protected speech? Back in 2001, the Second District Appellate Court gave us some idea of that line in *Universal Studios v. Corley* where they determined that "computer code" is considered a form of protected version of speech.

Code as Speech

"Communication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in 'code,' *i.e.,* symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment. If someone chose to write a novel entirely in computer object code by using strings of 1's and 0's for each letter of each word, the resulting work would be no different for constitutional purposes than if it had been written in English. The 'object code' version would be incomprehensible to readers outside the programming community (and tedious to read even for most within the community), but it would be no more incomprehensible than a work written in Sanskrit for those unversed in that language. The undisputed evidence reveals that even pure object code can be, and often is, read and understood by experienced programmers. And source code (in any of its various levels of complexity) can be read by many more. Ultimately, however, the ease with which a work is comprehended is irrelevant to the constitutional inquiry. If computer code is distinguishable from

conventional speech for First Amendment purposes, it is not because it is written in an obscure language." [2]

Apple argues that their programming code is protected speech under the First Amendment; and *Corley* surely supports that argument.

"We conclude that encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine." [3]

Apple, Inc. is correct in fighting the FBI in their demand to reveal their encrypted computer program. The FBI is demanding that Apple rewrite their speech so that it may have access to their information. This violates Apple's protected speech, which in this case is in the form of computer code.

Front #2: Though Apple's original argument against the FBI does not have any regard to the possible violation of citizen's speech; I believe it cannot be ignored in the expanding technological world. Citizen's and free speech is very revered in the free world and technology with the internet and cell phones allow an expansive platform to which an individual can access with ease. "The First Amendment has survived plenty of change in 225 years as it has adapted to telegraph, print, radio and television. But those who follow the topic most closely say the information age is a whole new era." [4]

Citizen Speech

"The First Amendment to the United States Constitution protects more than simply the right to speak freely. It is well established that it safeguards a wide spectrum of activities, including the right to distribute and sell expressive materials, the right to associate with others, and, most importantly to this case, the right to receive information and ideas." [5] Cell phones these days are realistically mini-computers. And there is good chance that all your activities are in there, stamped forever. Think

personal texts, internet searches and documents. Would you want every private correspondence of yours broadcasted to the world? Where is the line drawn in the digital age? What limits the government from knowing everything about us?

The following statement is from the 1953 case *United Sates v. Rumely* and was relating to the purchase of books and a person's catalog activity in the library. Ironically, the digital age has killed off the book in the form that we used to know it; however, the declaration I feel correlates to the idea of protecting free speech in the digital world. "Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of everyone who reads.... Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold. Some will fear to read what is unpopular, what the powers-that-be dislike.... [F]ear will take the place of freedom in the libraries, book stores, and homes of the land. Through the harassment of hearings, investigations, reports, and subpoenas government will hold a club over speech and over the press." [6] We must resist at every opportunity of allowing the government easy access to our digital devices as they hold, and can reveal so much about us.

An excerpt snagged from Nancy Leong's Huffington Post article a couple of years ago, *Constitutional Rights in the Digital Age* reads, "So if searches of cell phones are different from searches of ordinary physical objects, then should online speech be analyzed differently from offline speech? The logical answer is yes. Just as cell phones are different from ordinary physical objects, the Internet is dramatically different from earlier speech mediums. And the Court should acknowledge those differences in determining the scope of First Amendment protection for speech." [7]

"It is through speech that our convictions and beliefs are influenced, expressed, and tested. It is through speech that we bring those beliefs to bear on Government and on society. It is through speech

that our personalities are formed and expressed. The citizen is entitled to seek out or reject certain ideas or influences without Government interference or control."[8]

Fourth Amendment

"Outside the context of obscenity, few federal cases have discussed this collision between the Fourth Amendment and the First Amendment. However, the Supreme Court has made clear that, when expressive rights are implicated, a search warrant must comply with the particularity requirements of the Fourth Amendment with 'scrupulous exactitude'." [9] In this instance with Apple the FBI has properly attained a search warrant and seized the terrorist's phone; however, the FBI can't read what is on the phone because the very information they want is encrypted.

"Encryption is a security feature that some modern cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that renders a phone all but 'unbreakable' unless police know the password." [10] Now if the suspect in this case were still alive could the FBI demand they give the password to open the phone? Probably not. So how can they ask the same of Apple, Inc.?

"Similarly, the opportunities for officers to search a password-protected phone before data becomes encrypted are quite limited. Law enforcement officers are very unlikely to come upon such a phone in an unlocked state because most phones lock at the touch of a button or, as a default, after some very short period of inactivity. See, *e.g.,* iPhone User Guide for iOS 7.1 Software 10 (2014) (default lock after about one minute). This may explain why the encryption argument was not made until the merits stage in this Court, and has never been considered by the Courts of Appeals." [11] Again, normally the police or government would not have access to this information. So the question again, if the suspect was alive could the FBI demand Apple, Inc. to break the phone open?

Though *Riley* concerns illegal searches against the Fourth Amendment during an arrest and it is decided a warrant is required to search a cell phone during and after an arrest; the concern here is that the demand by the FBI to break into a phone violates the amendment. Unfortunately there have not been any trials to discuss the amendment issues as of date. The Apple v. FBI would have been a valuable review that would serve the future of society and law enforcement equally for proper protocol.

The fact that the FBI ended up breaking into the phone without Apple's help should possibly concern a violation of the Fourth Amendment. I believe not, as they procured a legal search warrant and can compare it to entering the locked house of a suspect on the grounds of the search warrant.

"Indeed, the character of that threat implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to rummage at will among a person's private effects." [12] As the digital world continues to expand, these two sides are on a collision course in the near future… what will be decided then?

FBI Perspective

All Writs Act

The FBI is relying on a Judiciary Act from 1789 by a newborn Congress that was written in by George Washington. You did not read that wrong: George Washington! As in our beloved countries inaugural President. You know cherry-tree choppin' George? Yeah that one! I believe it is fair to say that this Act which was in itself part of the birth of justice in the Land of Opportunity is at 227 years old and a bit outdated. We are talking about a time that relied on horseback for travelling and today we have rockets that go to space stations. It is a very pompous move by the government to push this Jurassic act in a case in the digital age. As intelligent as George Washington was, he would not even be able to fathom the oddity of ones and zeros and source code.

"One of the modern uses for the All Writs Act is helping to 'effectuate warrants'—that is, to give them teeth and make them more than some nice words on a piece of paper. It has been used in the past to compel the sharing of phone records and CCTV footage. In this case, a California court is using it to compel Apple to come up with the backdoor that the FBI wants." [13] Below, see the All Writs Act:

28 U.S. Code / 1651 - Writs

(a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

(b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction. [14]

The All Writs Act is the FBI's explanation to might Apple to create a backdoor that would compromise the security of every iPhone everywhere.

Read the powerful excerpt from the letter that Apple's current CEO, Tim Cook, released in response to the FBI's demand, "All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data.

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.

For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."[15]

1807

In, *United States v. Burr*, Chief Justice John Marshall forced the clerk of Aaron Burr to decipher an encrypted letter after Burr was charged with treason. The FBI is using this ancient decision to demand Apple do the same, "Apple should be forced to write new software to load onto the iPhone at hand to help FBI investigators unlock it, partly because Chief Justice John Marshall once forced Aaron Burr's clerk to 'decipher a coded letter' the third vice president had written after Burr was charged with treason."[16]

"But, on hearing the question more particularly and precisely stated, and finding that it refers only to the present knowledge of the cipher, it appears to the court that the question may be answered without implicating the witness, because his present knowledge would not, it is believed, in a criminal prosecution, justify the inference that his knowledge was acquired previous to this trial, or afford the means of proving that fact."[17]

The FBI argues the decryption will not incriminate Apple; therefore, they shall serve the best interest in government with this burden. I am sure much of the society is like me and the only reference they have of Aaron Burr is that classic "Got Milk?" commercial; which ironically was the subject of a prize-winning radio trivia question in the commercial because that's how obscure Aaron Burr is to modern society. The FBI is using analog arguments in a digital world and it is coming across very weak. Besides, Apple is not concerned with incriminating themselves; that was never their fear. Their alarm is to protect the privacy and personal information of all its clients.

Conclusion

Sure my thesis is specific to the San Bernardino situation; however, like much common law it invites the discussion of the bigger picture and does not always have a narrow focus to the case on hand. If the FBI did not resourcefully find a workaround for breaking into the i-Phone then we very well

may have seen many complex issues in the digital age come to light and decided by our courts and setting the precedent for the inevitable conflicts the future holds.

Who is advocating for public interest in the digital world? Though this paper may not be in the eyes of very many; I am sure across America there are many papers arguing similarities. And we are advocates for public interest. We and many among us will agree that Apple, Inc. cannot allow the FBI to break into the San Bernardino terrorists' cell phones because it violates sections of the First and Fourth Amendments of our founding Fathers.

Even though technology creates more challenges to the free world in the eyes of the courts and for national security, the challenges are the price we pay to prevent the suppression of our rights. Most countries all over the world use technology to suppress its citizen's rights. We do not have to have the problem and it is in our hands to never allow it to happen. Technology expands freedom worldwide and America can be that world model in preventing big government from bullying us from the fruits of our rights. It is in every citizen's civil duty to secure our right to free speech, press, religion, petition and assembly… or not, that is your right as well.

Endnotes

[1] Cornell Law School. Legal Information Institute. U.S. Constitution. https://www.law.cornell.edu/constitution/first_amendment [retrieved May 9, 2016].

[2] *Universal City Studios, Inc. v. Corley*, 273 F. 3d 429 - Court of Appeals, 2nd Circuit (2001).

[3] *Bernstein v. US Dept. of Justice*, 176 F. 3d 1132 - Court of Appeals, 9th Circuit (1999).

[4] Anders Gyllenhaal. "Will the First Amendment Survive the Information Age?" Milwaukee-Wisconsin Journal Sentinel (12 March 2016). http://www.jsonline.com/news/opinion/will-the-first-amendment-survive-the-information-age-b99680956z1-371850661.html. (retrieved April 28, 2016).

[5] *Tattered Cover, Inc. v. City of Thornton*, 44 P. 3d 1044 - Colo: Supreme Court 2002

[6] *United States v. Rumely*, 345 US 41 - Supreme Court (1953).

[7] Nancy Leong, "Constitutional Rights in the Digital Age," The Huffington Post (14 July 2014). http://www.huffingtonpost.com/nancy-leong/constitutional-rights-in-first-amendment_b_5601216.html. (retrieved March 20, 2016).

[8] *United States v. Playboy Entertainment Group, Inc.*, 529 US 803 - Supreme Court (2000).

[9] *Zurcher v. Stanford Daily*, 436 US 547 - Supreme Court (1978).

[10, 11] *Riley v. California*, 134 S. Ct. 2473 - Supreme Court (2014).

[12] *Arizona v. Gant*, 129 S. Ct. 1710 - Supreme Court (2009).

[13] Eric Limer, "Why Is the FBI Using a 227-Year-Old Law Against Apple?," PopularMechanics (24 February 2016). http://www.popularmechanics.com/technology/a19483/what-is-the-all-writs-act-of-1789-the-225-year-old-law-the-fbi-is-using-on-apple/. (retrieved May 1, 2016).

[14] Cornell Law School. Legal Information Institute. 28 U.S. Code 1651 - Writs. https://www.law.cornell.edu/uscode/text/28/1651 [retrieved May 19, 2016].

[15] Tim Cook, "A Message to Our Customers," Apple, Inc. (16 February 2016) http://www.apple.com/customer-letter/. (retrieved May 19, 2016).

[16] Priya Anand, "Why the government is citing Aaron Burr in its fight against Apple," MarketWatch (11 March 2016). http://www.marketwatch.com/Story/Story/?guid=%7BC695ED84-E712-11E5-B585-51929C806474%7D. (retrieved April 29, 2016).

[17] *United States v. Burr*, 25 F. Cas. 38, 39-40 (C.C. Va. 1807).