

Journal of Law & Commerce

Vol. 39, No. 2 (2021) • ISSN: 2164-7984 (online)
DOI 10.5195/jlc.2021.209 • <http://jlc.law.pitt.edu>

NOTES

ALL POWERFUL? HOW THE FBI'S REQUEST OF APPLE TO
UNLOCK AN iPhone USING THE ALL WRITS ACT FAILS THE
NEW YORK TELEPHONE TEST

Alyssa Zottola



This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License.



This site is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program, and is cosponsored by the University of Pittsburgh Press.

NOTES

ALL POWERFUL? HOW THE FBI'S REQUEST OF APPLE TO UNLOCK AN iPhone USING THE ALL WRITS ACT FAILS THE NEW YORK TELEPHONE TEST

*Alyssa Zottola**

INTRODUCTION

Smartphones, Alexa, Google Homes, and smart watches. All are examples of technology that are now ubiquitous in American society. As of February 2019, 81% of Americans own and use a smartphone.¹ However, smartphones are more than just communication devices: for many individuals, these phones contain highly personal information, ranging from daily schedules, private intimate conversations, to even health information.² With the increasing frequency of data breaches and hacking of electronic records,³ companies are taking steps to ensure that their systems and devices are secure in an effort to maintain public trust.

To protect against these breaches, technology companies use end-to-end encryption; while lauded by customers, the use of end-to-end encryption has frustrated the government in its attempts to access data from criminals' phones and other devices. With few other options, and the necessity of

* JD Candidate, University of Pittsburgh, 2021; B.A. Italian Studies; B.A. History, *magna cum laude*, University of Pittsburgh 2018.

¹ *Mobile Fact Sheet: Mobile Phone Ownership Over Time*, PEW RSCH. CTR.: INFO. & TECH. (June 12, 2019), <https://www.pewresearch.org/internet/fact-sheet/mobile/>.

² *Apple iOS Health*, APPLE, <https://www.apple.com/ios/health/> (last visited Jan. 13, 2021).

³ Joseph Johnson, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 1st Half 2020*, STATISTA (Jan. 25, 2021), <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>.

smartphones as a source of information in criminal investigations, the government has turned, with increasing frequency,⁴ to the little known All Writs Act (“AWA”), to try and force companies, such as Apple and Google,⁵ to unlock personal devices or provide data from devices against the companies’ will.⁶

The potential consequences of allowing the government to manipulate the AWA to serve its purpose of conscripting private companies to work for the government are staggering. There is nothing within the AWA to suggest that the government would be limited in using the Act just for the purpose of unlocking phones.⁷ On at least sixty occasions,⁸ both Apple and Google have been forced to provide technical assistance to agencies such as the FBI, Department of Homeland Security, and U.S. Postal Inspection Services,⁹ ranging from bypassing phones’ lock screens to extracting the data from devices.¹⁰ The open-ended nature of the AWA suggests that the government could potentially use the Act as a means to force other private companies to perform similar actions.¹¹

⁴ As of March of 2016, there were at least approximately seventy-six requests; the ACLU, through their own investigation, uncovered sixty-three confirmed cases involving requested uses of the AWA, as well as one potential case in Massachusetts (due to a lack of publicly available information, the ACLU was unable to positively confirm the use of the AWA), and Apple identified twelve pending cases where there was a request to use the AWA. Eliza Sweren-Becker, *This Map Shows How the Apple-FBI Fight Was About Much More Than One Phone*, ACLU (Mar. 30, 2016, 9:00 AM), <https://www.aclu.org/blog/privacy-technology/internet-privacy/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone?redirect=blog/speak-freely/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone>.

⁵ *All Writs Act Orders for Assistance from Tech Companies*, ACLU, <https://www.aclu.org/issues/privacy-technology/internet-privacy/all-writs-act-orders-assistance-tech-companies> (last visited Jan. 23, 2020).

⁶ See Ian Samuel, *The New Writs of Assistance*, 86 *FORDHAM L. REV.* 2873, 2888–89 (2018).

⁷ The FBI has not only used the AWA to force Apple to unlock phones: it also used the AWA to unlock an iPad to access an online internet account. Jose Pagliery, *Here are the Places the Feds are Using a Controversial Law to Unlock Phones*, CNN BUS. (Mar. 30, 2016, 11:28 AM), <https://money.cnn.com/2016/03/30/technology/phones-all-writs-act/index.html>.

⁸ *All Writs Act Orders for Assistance from Tech Companies*, *supra* note 5.

⁹ *Id.*

¹⁰ *Id.*

¹¹ During a murder investigation in 2015, the government asked Amazon, using the AWA, to provide data from an Amazon Alexa Echo device. While the suspect eventually gave the government the Alexa willingly, and the government was able to access the data without the help of Amazon, this suggests that the AWA could be used for more than just unlocking cell phones. Samuel, *supra* note 6, at 2874–75. Google has also previously been subject to requests by the government to unlock Android devices pursuant to the AWA. *All Writs Act Orders for Assistance from Tech Companies*, *supra* note 5.

Perhaps the most recognizable instance of such attempted action is the FBI's bid to force Apple to unlock the San Bernardino shooter's iPhone. In *In re Search of An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*,¹² Magistrate Judge Sheri Pym¹³ signed an order, pursuant to the AWA, to compel Apple to supply the FBI with the necessary technical assistance to access the iPhone.¹⁴ The order was eventually withdrawn for mootness, as the FBI was able to access the information without the assistance of Apple.¹⁵ The well-publicized legal bid catapulted the AWA into the public eye, creating a large public debate about whether Apple and other technology companies should be forced to comply with such orders to provide technical assistance in law enforcement investigations.¹⁶ More importantly, the dispute between the FBI and Apple highlights the inappropriateness of the AWA as an instrument in a criminal investigation.

There is little case law that specifically addresses the use of the AWA as a tool to compel private companies into assisting the government in investigations. Therefore, the precedential AWA case, *United States v. New York Telephone Co. ("New York Telephone")*,¹⁷ provides crucial guidance to courts in interpreting the AWA and what they must evaluate when determining whether or not to grant the request. The Court in *New York Telephone* provides three elements for consideration (what the author refers to hereinafter as the "New York Telephone test") to guide courts in evaluating AWA requests. The elements are as follows: (1) the degree of separation

¹² *In re Search of An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Ca. License Plate 35KGD203*, 2016 WL 618401 (C.D. Cal. 2016) [hereinafter *In re Search of An Apple iPhone*].

¹³ See Eric Lichtblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, N.Y. TIMES (Feb. 16, 2016), <https://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html>.

¹⁴ Order Compelling Apple, Inc. to Assist Agents in Search at 2, *In re Search of An Apple iPhone*, 2016 WL 618401 (C.D. Cal. 2016) [hereinafter Order Compelling Apple].

¹⁵ Order Vacating February 16, 2016 Order at 1, *In re Search of An Apple iPhone*, 2016 WL 618401 [hereinafter Order Vacating].

¹⁶ Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?postshare=9501485386886260&tid=ss_mail&utm_term=.72ab40da8569.

¹⁷ *United States v. N.Y. Tel. Co.*, 434 U.S. 159 (1977).

between the third-party and the controversy;¹⁸ (2) the burden the request places upon the third-party;¹⁹ (3) the ability to complete the task without the third party's assistance.²⁰

This Paper assesses the AWA in the framework of the San Bernardino investigation and the subsequent legal battle. It argues that the decision to grant the order, pursuant to the AWA, to compel Apple to provide technical assistance was improperly decided. Furthermore, it argues that the AWA should not be used in future criminal investigations to compel technology companies' assistance. This Paper proposes that the proper solution to the problem must balance the need for information in a criminal investigation against a company's right to be free from compelled service. Such solution is legislation with input from both the technology industry and federal (perhaps even local) law enforcement agencies that allows for the agencies to have access to data and conduct a proper investigation, pursuant to a lawful warrant or subpoena, while also ensuring the technological security of the American people. The author argues that many of the factors assessed in the San Bernardino case about the burden, degree of separation, and ability to complete the task without third-party assistance were not unique to that litigation and would weigh against the government in future applications for use of the AWA.

Part I of this Paper provides a provides a timeline of events for the San Bernardino shooting. Part II gives a history and legal framework of the AWA, focusing on the Supreme Court's decision in *New York Telephone*, which provides the analytical framework for assessing AWA requests. Part III describes the history of the AWA, with subsections describing the *New York Telephone* case and the *New York Telephone* test (as applied to the San Bernardino litigation). Part IV analyzes proposed solutions and Part V provides a conclusion.

¹⁸ *Id.* at 174.

¹⁹ *Id.* at 175.

²⁰ *Id.*

I. THE SAN BERNARDINO SHOOTING

On December 2, 2015, at 10:59 a.m.,²¹ eighty members of the San Bernardino Environmental Health Department gathered in a large conference room at the Inland Regional Center (IRC) for a training event²² were gunned down and massacred by two shooters dressed in all black.²³ The shooters were in and out of the room within two to three minutes.²⁴ In total, thirty-six people were shot, twenty-two people were injured, and fourteen people were killed.²⁵ The suspects, later identified as Rizwan Farook and Tashfeen Malik,²⁶ were killed in a shoot-out with police officers and FBI agents hours later within a suburban area of San Bernardino in their rental car.²⁷ Within the rental car, agents found the now infamous iPhone²⁸—later at the center of the controversy between the FBI and Apple.

II. BACKGROUND INFORMATION ON THE ALL WRITS ACT

A. *History of the All Writs Act*

The AWA, in its current form, states: “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.”²⁹ The current form of the Act has its origins in the Judiciary Act of 1789, which helped delineate the powers given to federal

²¹ RICK BRAZIEL ET AL., BRINGING CALM TO CHAOS: A CRITICAL INCIDENT REVIEW OF THE SAN BERNARDINO PUBLIC SAFETY RESPONSE TO THE DECEMBER 2, 2015, TERRORIST SHOOTING INCIDENT AT THE INLAND REGIONAL CENTER 25 (2016), <https://www.justice.gov/usao-cdca/file/891996/download>.

²² *Id.*

²³ *Id.*

²⁴ *Id.* at 27.

²⁵ *Id.* at 25.

²⁶ *See id.* at 26, 37; Adam Nagourney et al., *San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead*, N.Y. TIMES (Dec. 2, 2015), <https://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html>.

²⁷ BRAZIEL ET AL., *supra* note 21, at 38–40.

²⁸ Josh Gerstein & David Perera, *Feds Get Order to Force Apple to Unlock San Bernardino Shooter's Phone*, POLITICO (Feb. 16, 2016, 11:05 PM), <https://www.politico.com/blogs/under-the-radar/2016/02/san-bernardino-apple-shooters-219357>.

²⁹ 28 U.S.C. § 1651(a) (2018).

district courts in the United States.³⁰ The two relevant sections of the Act, Sections 13 and 14, provide the basis for the current iteration of the AWA, and were combined (and subsequently codified) in the Judicial Code in 1948 to form 28 U.S.C. § 1651.³¹ Section 13 provided, in pertinent part, that the district courts may issue writs of mandamus.³² Section 14, which remained largely the same in the 1948 amendment, dictates that the courts of the United States “shall have power to issue writs of *scire facias*, *habeas corpus*, . . . and all other writs not specially provided for by statute, which may be necessary for the exercise of their respective jurisdictions, and agreeable to the principles and usages of law.”³³ The only major change between the two versions of the AWA is the removal of the phrase “not specially provided for by statute” in the 1948 codification.³⁴ There is very little legislative history regarding the removal of the phrase “not specifically provided for by statute”;³⁵ however, the interpretation of the AWA remains the same regardless of the change in wording.³⁶

B. New York Telephone: *The Case*

Any attempted use of the AWA by the government to compel assistance from third-parties in criminal investigations is evaluated using the three-part *New York Telephone* test.³⁷ In *New York Telephone*, the FBI applied for, and received, a warrant to install a pen register (a type of listening device) on the telephone line of a suspected illegal gambling operation.³⁸ New York Telephone Company was to supply any and all necessary technical assistance so that the pen register could be installed unobtrusively and to lease a telephone line to the FBI, allowing the FBI to listen to the conversations at a

³⁰ Jennifer X. Luo, *Decoding Pandora's Box: All Writs Act and Separation of Powers*, 56 HARV. J. LEGIS. 257, 261–62 (2019).

³¹ *Id.* at 262.

³² Judiciary Act of 1789, ch. 20, § 13, 1 Stat. 73, 80–81.

³³ *Id.* at 81–82.

³⁴ Luo, *supra* note 30, at 262.

³⁵ *Id.* at 262–63.

³⁶ *See id.* at 263–64.

³⁷ *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 174–76 (1977).

³⁸ *Id.* at 161–62.

remote location;³⁹ the FBI was to compensate New York Telephone for these services at the standard monetary rate.⁴⁰

New York Telephone agreed to help the FBI install the pen register but refused to lease the FBI a telephone line.⁴¹ New York Telephone moved to quash the order requiring their forced assistance with the pen register, arguing the AWA did not give the District Court the authority to issue such a writ.⁴² However, the District Court for the Southern District of New York disagreed, finding that the AWA and its inherent powers gave the Court the authority to force New York Telephone to comply with the order.⁴³ The Second Circuit Court of Appeals affirmed in part and reversed in part the District Court's decision, noting that the District Court had the power to authorize pen registers but abused its discretion by finding that the AWA authorized the courts to force New York Telephone to provide technological assistance.⁴⁴ In so holding, the Court of Appeals "expressed concern that: 'such an order [for compelled assistance] could establish a most undesirable, if not dangerous and unwise, precedent for the authority of federal courts to impose unwilling aid on private third parties' and that 'there is no assurance that the court will always be able to protect [third parties] from excessive or overzealous Government activity or compulsion.'"⁴⁵

The Supreme Court reversed the Second Circuit's decision.⁴⁶ The majority opinion, authored by Justice White, did address the Court of Appeals' concern regarding the potential for unintended consequences, noting that "[w]e agree that the power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be imposed."⁴⁷ However, in the same breath, they implicitly repudiate such concerns by stating: "[t]he power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the

³⁹ *Id.* at 161.

⁴⁰ *Id.*

⁴¹ *Id.* at 162.

⁴² *Id.* at 163.

⁴³ *Id.*

⁴⁴ *Id.* at 164.

⁴⁵ *Id.*

⁴⁶ *Id.* at 178.

⁴⁷ *Id.* at 172.

implementation of a court order or the proper administration of justice.”⁴⁸ Although Justice Stewart agreed that the District Court had the authority to order the installation of the pen register,⁴⁹ he joined in Part II of Justice Stevens’⁵⁰ more convincing dissent.

Justice Stevens does a more faithful job of using the text and the history of the AWA to interpret the proper role and use of the statute. He highlights how “[t]he statute does not contain, and has never before been interpreted as containing, the open-ended grant of authority to the federal courts that today’s decision purports to uncover.”⁵¹ Instead, he notes that, “in the language of the statute itself, *there are two fundamental limitations on its scope*. The purpose of any order authorized by the Act must be *to aid the court in the exercise of its jurisdiction*; and the means *must be analogous to a common-law writ*.”⁵²

C. New York Telephone: *The Test*

Following the Court’s decision in *New York Telephone*, any case involving the use of the AWA to compel third-party assistance with the execution of an order should be assessed against the elements outlined in *New York Telephone*, in what the author refers to as the *New York Telephone* test.⁵³ The test uses three elements as a guide when examining the facts of a specific case in determining whether or not the court should use its power under the AWA to grant an order compelling service. The elements are as follows: (1) the degree of separation between the third-party and the controversy;⁵⁴ (2) the burden the request places upon the third-party;⁵⁵ and (3) the ability to complete the task without the third party’s assistance.⁵⁶

Taking each element in turn, the Court in *New York Telephone* first reasoned that *New York Telephone* was not too far removed from the

⁴⁸ *Id.* at 173–74.

⁴⁹ *Id.* at 178.

⁵⁰ *Id.* (Stevens, J. dissenting, joined by Brennan and Marshall, JJ.).

⁵¹ *Id.* at 187.

⁵² *Id.* (emphasis added) (footnote omitted).

⁵³ *See id.* at 174–75.

⁵⁴ *Id.* at 174.

⁵⁵ *Id.* at 175.

⁵⁶ *Id.*

controversy “that its assistance could not permissibly be compelled” because there was sufficient evidence to suggest the company’s facilities were used to perpetuate a criminal enterprise.⁵⁷ More importantly, New York Telephone was a “highly regulated public utility,” for which the Court argued “it hardly can be contended that the Company . . . had a substantial interest in not providing assistance.”⁵⁸ Regarding the issue of the burden placed on New York Telephone, the Court believed that the financial compensation and the “minimal effort” required by New York Telephone to comply with the order did not place an undue burden on the company.⁵⁹ Finally, the Court notes that there is no way the FBI would have been able to conduct its surveillance from a remote location without the assistance of New York Telephone, as the FBI conducted an extensive search and was unable to find a suitable location for such surveillance without New York Telephone’s assistance in providing the leased line.⁶⁰

As applied to the San Bernardino dispute, based on the totality of these factors, it is clear that the use of the AWA amounts to improper compulsion of assistance from Apple by the FBI. It is a prime example of what the majority in the Second Circuit Court of Appeals and the dissent in *New York Telephone* feared would occur:⁶¹ unfettered government ability to force third parties to become unwilling government agents. Using the dispute between Apple and the FBI over the San Bernardino shooter’s phone as a case study, it is clear that the AWA is an improper tool to access data on encrypted phones as, taken together, the three elements of the *New York Telephone* test balance in favor of Apple rather than the FBI.

D. Applying the New York Telephone Test to the Apple v. FBI Dispute

1. Procedural history of the San Bernardino Apple v. FBI dispute

A note about the procedural history of the case *In re Search of An Apple iPhone* (i.e., the San Bernardino case). The FBI applied *ex parte* to

⁵⁷ *Id.* at 174.

⁵⁸ *Id.*

⁵⁹ *Id.* at 175.

⁶⁰ *Id.*

⁶¹ *Id.* at 187.

Magistrate Judge Sheri Pym⁶² on February 16, 2016 for an order compelling Apple to aid the FBI in unlocking the San Bernardino shooter's iPhone.⁶³ The Magistrate granted the order on the same day, finding that the U.S. Attorney had shown good cause for the order.⁶⁴ The order gave Apple five days following its issuance to apply to the Magistrate Court for relief if "Apple believes that compliance with this Order would be unduly burdensome."⁶⁵ Apple responded with a Motion in Opposition nine days later on February 25, 2016, outlining why it opposed the Order compelling its assistance to the FBI.⁶⁶ A hearing was set for March 22, 2016 to hear arguments on the case.⁶⁷ However, on March 29, the order was vacated by Judge Pym for mootness, as the FBI was able to gain access to the phone without Apple's assistance.⁶⁸ Therefore, unlike in *New York Telephone*, there was not a full-blown court case, comprising oral arguments on motions, cross examination of witness, or an opinion from Judge Pym about her reasoning for granting the order and reasoning for her verdict (if the case were heard as a bench trial). The most insight comes from the original order granting the request, pursuant to the AWA, to compel Apple's assistance.

The February 16, 2016 order does not use the specific elements of the *New York Telephone* test; the only reference to the elements of the test is the judge allowing Apple to apply for relief if it "believes that compliance with this Order would be unduly burdensome."⁶⁹ The bulk of the order details the type of technical assistance Apple was to provide, the methods by which Apple could comply with the order, how Apple should advise the government

⁶² Lichtblau, *supra* note 13.

⁶³ Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search at 1, *In re* Search of An Apple iPhone, 2016 WL 618401 [hereinafter Government's Ex Parte Application].

⁶⁴ Order Compelling Apple, *supra* note 14, at 1, 3.

⁶⁵ *Id.* at 3.

⁶⁶ Declaration of Nicola T. Hanna in Support of Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist in Search, and Opposition to Government Motion to Compel Assistance at 1, 7, *In re* Search of An Apple iPhone, 2016 WL 618401 [hereinafter Declaration of Nicola T. Hanna].

⁶⁷ Elizabeth Weise, *Apple, FBI to Head to Court March 22*, USA TODAY (Feb. 20, 2016, 11:44 PM), <https://www.usatoday.com/story/tech/news/2016/02/19/apple-fbi-court-march-22-riverside-march-22/80635402/>.

⁶⁸ Order Vacating, *supra* note 15, at 1; Alina Selyukh, *The FBI Has Successfully Unlocked the iPhone Without Apple's Help*, NPR (Mar. 28, 2016).

⁶⁹ Order Compelling Apple, *supra* note 14, at 3.

regarding the cost of “providing this service,” and releasing Apple from the responsibility of holding on to a copy of the data.⁷⁰

While the litigation between Apple and the FBI in the San Bernardino case did not produce an opinion, or make it to the stage of hearing arguments on the motions, a previous dispute between Apple and the FBI in the Eastern District of New York did produce an opinion.⁷¹ Importantly, the opinion was not issued until *after* the FBI applied, using the AWA, for Apple’s assistance in unlocking the phone in California.⁷² This author purposefully chose to focus on the California case, instead of the New York case, because the iPhone in the San Bernardino case was running on iOS 9,⁷³ meaning that Apple could not break into the phone, as phones using iOS 8 and above require that the user know the password to access the data;⁷⁴ Apple is incapable of accessing the data on the phone without the password.⁷⁵ In comparison, the iPhone in the New York case ran on iOS 7,⁷⁶ which Apple could theoretically “break into”⁷⁷ without creating the backdoor the FBI argued it needed in the San Bernardino case.⁷⁸ As such, the legal arguments about the elements of the *New York Telephone* test, while similar, still are different, as Apple would be attempting something it has never done before.⁷⁹ The New York opinion, however, does provide excellent analysis of why the AWA is the inappropriate instrument to force Apple to assist the FBI.⁸⁰

⁷⁰ *Id.* at 2–3.

⁷¹ *In re* Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341 (E.D.N.Y. 2019).

⁷² The AWA order in the San Bernardino shooting was issued on February 16, 2016. The Opinion was issued on February 29, 2016.

⁷³ Memorandum of Points and Authorities, Government’s Ex Parte Application, *supra* note 63, at 4 [hereinafter Memorandum of Points and Authorities].

⁷⁴ Declaration of Erik Neuschwander in Support of Apple Inc’s Motion to Vacate Order Compelling Apple Inc. to Assist in Search, and Opposition to Government Motion to Compel Assistance at 3, *In re* Search of An Apple iPhone, 2016 WL 618401 [hereinafter Declaration of Erik Neuschwander].

⁷⁵ *Id.*

⁷⁶ *In re* Order Requiring Apple Inc. to Assist, 149 F. Supp. 3d at 345.

⁷⁷ Transcript of Argument at 7, 58–59, *In re* Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court, 149 F. Supp. 3d 341 (E.D.N.Y. 2019) [hereinafter Transcript of Argument]; Joel Rose, *The Seeds of Apple’s Standoff With the DOJ May Have Been Sown in Brooklyn*, NPR (Feb. 22, 2016, 5:16 AM), <https://www.npr.org/2016/02/22/467602161/the-seeds-of-apples-standoff-with-doj-may-have-been-sown-in-brooklyn>.

⁷⁸ See Rose, *supra* note 77.

⁷⁹ Declaration of Erik Neuschwander, *supra* note 74, at 10.

⁸⁰ See *In re* Order Requiring Apple Inc. to Assist, 149 F. Supp. 3d at 364–76.

2. *The New York Telephone Test applied to the San Bernardino Dispute*

As applied to the facts of the San Bernardino dispute between Apple and the FBI, the first factor of the test (the degree of separation between the third-party and the controversy)⁸¹ clearly indicates that the use of the AWA is inappropriate. Apple is far removed from the controversy between the FBI and the San Bernardino shooter. The only connection between the two is that Apple sold the phone used by the shooter. Arguing that a retailer who sells hundreds of millions of devices⁸² is close enough to a controversy, just because it sold a device used by a drug dealer or a mass shooter, has unimaginable consequences. Companies such as Apple and Google would find themselves entangled in millions of such controversies.

However, the Court in *New York Telephone* argued that the mere fact a criminal enterprise used New York Telephone's facilities was enough to connect the company to the controversy.⁸³ The author believes that such an interpretation is incorrect, as it potentially subjects large companies, such as Apple, to an unfathomable number of requests for assistance. The author's view is also supported by Magistrate Judge James Orenstein, who noted in the New York dispute between Apple and the FBI, "Apple is too far removed from [the defendant in the New York case's] criminal conduct to have any obligation to assist the DEA's investigation. To the extent that Feng used his iPhone in committing crimes, he used *his own property*, not Apple's."⁸⁴ Apple is a retailer that simply *sold* the device used in the offense; its involvement in the crime ended at the point of sale, as it no longer controls the device. Further separating Apple from the San Bernardino incident is the fact that the *employer*, not the shooter himself, was the owner of the phone,⁸⁵ meaning that Apple was not even directly responsible for selling the phone to the shooter.

Further distinguishing the separation between New York Telephone and its controversy, as compared to Apple and the San Bernardino shooting, is

⁸¹ *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 174.

⁸² Lionel Sujay Vailshery, *Apple iPhone Sales Worldwide 2007–2018*, STATISTA (Jan. 22, 2021), <https://www.statista.com/statistics/276306/global-apple-iphone-sales-since-fiscal-year-2007/>.

⁸³ *See N.Y. Tel. Co.*, 434 U.S. at 174.

⁸⁴ *In re Order Requiring Apple Inc. to Assist*, 149 F. Supp. 3d at 364 (emphasis added).

⁸⁵ Declaration of Erik Neuenschwander, *supra* note 74, at 11.

that New York Telephone was a “*highly regulated public utility with a duty to serve the public*.”⁸⁶ Apple is not bound by the same constrictions: its primary goal is, arguably, keeping its customers happy, thereby ensuring a steady revenue stream. While Apple is not a private company, rather a public company with shareholders,⁸⁷ it still does not owe the same duty that is assigned to a “highly regulated public utility with a duty to serve the public.”⁸⁸ Therefore, Apple is far enough removed from the controversy that the government and FBI’s request fails the first prong of the *New York Telephone* test.

The second prong, the burden the request places upon the third party,⁸⁹ again clearly weighs in Apple’s favor, as the burden of complying with the government’s request is unfathomably high. Measuring whether something is reasonable or not should not just be an economic calculation; one must examine all of the potential consequences of coercing Apple to supply technical assistance against its will against the totality of the circumstances. In other words, the court should weigh all of the potential consequences of ordering Apple to comply with the court order and supply technical assistance to the FBI against its will. Weighed against the totality of the circumstances, it is clear that the coerced assistance is an unreasonable burden on Apple.

Financially speaking, the cost of the requested remedy is likely astronomical; Apple would need to hire paralegals, engineers, and additional Apple law enforcement compliance officers, not to mention the cost of labor in designing and writing the code itself.⁹⁰ Apple’s total sales in 2016 measured around \$214.23 billion;⁹¹ the theoretical cost of complying with such an order is unlikely to deplete Apple’s coffers. However, as Erik Neuenschwander, Apple’s Manager of User Policy, notes, this would be the

⁸⁶ *N.Y. Tel. Co.*, 434 U.S. at 174 (emphasis added).

⁸⁷ *Investor Relations: Frequently Asked Questions*, APPLE, <https://investor.apple.com/faq/default.aspx> (last visited Jan. 3, 2021).

⁸⁸ *N.Y. Tel. Co.*, 434 U.S. at 174.

⁸⁹ *Id.* at 175.

⁹⁰ Declaration of Lisa Olle in Support of Apple Inc’s Motion to Vacate Order Compelling Apple Inc. to Assist in Search, and Opposition to Government Motion to Compel Assistance at 3–5, *In re Search of An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Ca. License Plate 35KGD203*, 2016 WL 618401 [hereinafter Declaration of Lisa Olle].

⁹¹ *Apple*, MARKETWATCH, <https://www.marketwatch.com/investing/stock/aapl/financials> (last visited Jan. 27, 2020).

first time that anyone, specifically Apple, has attempted such a task.⁹² It is likely that unforeseen complications will result in higher than anticipated costs.

Beyond the pure financial cost to Apple of providing assistance, the manpower required for such endeavor *is* unduly burdensome. As both Apple's Manager of its Global Privacy and Law Enforcement Compliance Team,⁹³ as well as its Manager of User Policy⁹⁴ pontificated, to complete the requested task, Apple would need to dedicate six to ten engineers specifically to the project for a span of time ranging from two to four weeks.⁹⁵ In addition, should the request be granted, a team of employees ranging from paralegals to engineers would need to be hired and dedicated to specifically handle all AWA requests.⁹⁶ Further adding to the burden, what the government is asking Apple to do is something that has never been attempted before.⁹⁷ The estimates regarding the amount of time, manpower, and costs are all hypotheticals, as is the idea that any attempt to decrypt the phone would be successful. If a technology company, like Apple or Google, is forced to supply technological assistance to the government, the burden analysis must also take into account First Amendment considerations.

In cases where Apple (or another company) would be forced to build a "backdoor" into its system, there are First Amendment and compelled speech considerations:⁹⁸ Should an individual be forced to create a code, which some appellate courts have ruled is speech,⁹⁹ that they vehemently protest against?

⁹² Declaration of Erik Neuenschwander, *supra* note 74, at 10.

⁹³ Declaration of Lisa Olle, *supra* note 90, at 2.

⁹⁴ Declaration of Erik Neuenschwander, *supra* note 74, at 2.

⁹⁵ *Id.* at 5.

⁹⁶ Declaration of Lisa Olle, *supra* note 90, at 4.

⁹⁷ Declaration of Erik Neuenschwander, *supra* note 74, at 10.

⁹⁸ Other authors have considered that the act of coding, which some appellate courts have ruled to be speech, would be forced speech and should be taken as compelled speech. Steven R. Morrison, *Breaking iPhones under CALEA and the All Writs Act: Why the Government Was (Mostly) Right*, 38 CARDOZO L. REV. 2039, 2077 (2017); see Adrianna Oddo, *Being Forced to Code in the Technology Era as a Violation of the First Amendment Protection Against Compelled Speech*, 67 CATH. U. L. REV. 211, 214 (2018).

⁹⁹ While the Supreme Court has not ruled on the matter of whether computer code is indeed speech deserving of First Amendment protection, at least two appellate courts have held that computer code is indeed speech and should be protected under the first amendment. *Universal Studios v. Corely*, 273 F.3d 429, 445–46 (2d Cir. 2001) ("Communication does not lose constitutional protection as 'speech' simply because it is expressed in language of computer code."); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir.

Furthermore, while the government argues that the “backdoor” would only be used on the target phone,¹⁰⁰ is there a way to ensure that this remains the case? Regardless of the hypotheticals, the greatest burden that the compelled action places upon Apple is the abhorrent precedent it sets.

Domestically, there are numerous requests of Apple and Google to unlock devices.¹⁰¹ Apple previously provided technical assistance to law enforcement agencies in accessing devices (using already available methods and subject to warrants or subpoenas);¹⁰² however, as illustrated in the New York dispute between Apple and the FBI over unlocking an unrelated iPhone, creating a “backdoor” would open the flood gates for request for assistance.¹⁰³ It is not beyond the stretch of the imagination that, should a court enforce the order, pursuant to the AWA, compelling Apple to provide technical assistance to the FBI, that those seventy requests¹⁰⁴ would become a veritable tsunami of requests that would consume the company. Such scenario is foreshadowed in the statements of Manhattan District Attorney Cyrus Vance, who insinuated that he would use such precedent to force Apple to help unlock the (at that time) 423 inaccessible phones¹⁰⁵ connected to criminal cases in his jurisdiction.

Beyond Apple, it requires no stretch of the imagination to see how another tech company, perhaps Microsoft or WhatsApp, could be placed in the same position as Apple if an order pursuant to the AWA is granted and enforced. After the FBI was able to access the data on the San Bernardino iPhone (without the assistance of Apple), a Department of Justice spokeswoman implied that the precedent of Judge Pym granting the order, although not enforcing it, would be used to force tech companies into action “through the court system when cooperation fails.”¹⁰⁶

2000) (“Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.”).

¹⁰⁰ Memorandum of Points and Authorities, *supra* note 73, at 7.

¹⁰¹ *All Writs Act Orders for Assistance from Tech Companies*, *supra* note 5.

¹⁰² *In re* Order Requiring Apple Inc. to Assist, 149 F. Supp. 3d at 346.

¹⁰³ *Id.* at 348.

¹⁰⁴ Transcript of Argument, *supra* note 77, at 8.

¹⁰⁵ Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We On Encryption?*, NPR (Dec. 3, 2016, 1:00 PM), <https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption>.

¹⁰⁶ David Kravets, *US Says it Would Use “Court System” Again to Defeat Encryption: Feds Say They Can Force Entire Tech Sector, Not Just Apple, to Disable Security*, ARS TECHNICA (Mar. 29, 2016, 12:19 PM), <https://arstechnica.com/tech-policy/2016/03/us-says-it-would-use-court-system-again-to-defeat-encryption/>.

Looking beyond the domestic frontier, however, one could argue that if the United States government could successfully compel Apple to create a “backdoor” for an iPhone, other countries—perhaps those that are notorious for spying on their own citizens—would feel emboldened to ask that such a feature be included as a standard feature on *all phones* prior to sale in their respective countries.

The use of the AWA to compel a company like Apple into government service to forcefully decrypt the phone would set an appalling precedent that would inundate it with requests for assistance from prosecutorial and governmental agencies and divert its efforts away from business and instead towards forced government service. The combined monetary and precedential effects of forcing Apple to unlock the phone at the behest of the government demonstrates that the government’s request fails the second prong of the *New York Telephone* test (whether the request places an undue burden on the third party)¹⁰⁷ and places an undue burden on Apple.

The third and final prong of the *New York Telephone* test is assessing whether the government could successfully accomplish its task without assistance from the third party.¹⁰⁸ There is a strong argument that the government *could* have accessed the data *without the assistance of Apple*. In the oral argument of the New York dispute between Apple and the FBI, Judge Orenstein noted that in another case, the government asserted that it *was able* to unlock the defendant’s phone that was running on a later version of iOS.¹⁰⁹ Even if, *arguendo*, the government was unable to use the technology alluded to in the other case addressed by Judge Orenstein, there were alternative methods available to the government that would have allowed them to access the data without the assistance of Apple, meaning that the government’s request still fails the third prong of the *New York Telephone* test.

While the *New York Telephone* test dictates that the reviewing court must consider whether the government would be able to accomplish its goal without the assistance of the third-party, the author argues it should also take into account whether the government has made a good-faith effort to achieve

¹⁰⁷ United States v. N.Y. Tel. Co., 434 U.S. 159, 175 (1977).

¹⁰⁸ *Id.*

¹⁰⁹ Transcript of Argument, *supra* note 77, at 3–4 (the case referenced was United States v. Djibo, 151 F. Supp. 3d 297, 304 (E.D.N.Y. 2015), in which the government asserted it was able to unlock the seized phone without help from Apple).

its goal before resorting to the AWA. If such consideration were applied to the litigation in the San Bernardino shooting, then the FBI's request would clearly fail the third prong of the test. The FBI's actions hindered the smooth accessing of data and necessitated the invocation of the AWA. The FBI requested that the shooter's employer, the San Bernardino County Public Health Department ("SBCPHD"), change the iCloud password associated with the shooter's account.¹¹⁰ If the FBI had not ordered the SBCPHD to change the iCloud password on the shooter's iPhone, it is possible that the government would have been able to recover the data without the help from Apple.¹¹¹

Furthermore, a lack of communication between divisions in the FBI resulted in delayed attempts by other divisions within the FBI (who were directly involved with the San Bernardino shooting investigation) to contact their vendors about a potential solution.¹¹² The FBI was unaware, at the time of the original filing of the AWA request, that one of its divisions within the investigative branch had contacts who could be solicited to help with unlocking the iPhone;¹¹³ however, the FBI was aware that the division was reaching out to its contacts at the time the FBI was scheduled to argue against Apple's Motion to Dismiss. As such, the information should have debased the FBI's claim that it was unable to access the information on the shooter's iPhone without Apple's help.¹¹⁴

Taken together, it is clear that the *New York Telephone* test elements ((1) the degree of separation between the third-party and the controversy;¹¹⁵ (2) the burden the request places upon the third-party;¹¹⁶ (3) the ability to complete the task without the third party's assistance)¹¹⁷ support the

¹¹⁰ Declaration of Erik Neuenschwander, *supra* note 74, at 11.

¹¹¹ *Id.* at 11–12.

¹¹² U.S. DEP'T JUST. OFF. INSPECTOR GEN., A SPECIAL INQUIRY REGARDING THE ACCURACY OF FBI STATEMENTS CONCERNING ITS CAPABILITIES TO EXPLOIT AN IPHONE SEIZED DURING THE SAN BERNARDINO TERROR ATTACK INVESTIGATION (Mar. 6, 2018), <https://oig.justice.gov/reports/2018/o1803.pdf>.

¹¹³ Susan Landau, *Revelations on the FBI's Unlocking of the iPhone: Maybe the Future isn't Going Dark*, LAWFARE (Mar. 30, 2018, 7:00 AM), <https://www.lawfareblog.com/revelations-fbis-unlocking-san-bernardino-iphone-maybe-future-isnt-going-dark-after-all>.

¹¹⁴ *Id.*

¹¹⁵ *United States v. N.Y. Tel. Co.*, 434 U.S.159, 174 (1977).

¹¹⁶ *Id.* at 175.

¹¹⁷ *Id.*

conclusion that the use of the AWA to compel Apple's assistance was improper (and would be improper in the future). The distance between Apple and the controversy¹¹⁸ (the San Bernardino shooting) is staggering: Apple is a retailer of devices and sells hundreds of millions of devices each year.¹¹⁹ To say that it is connected to a controversy because one of its devices was used in a crime would potentially subject Apple to hundreds of millions of legal disputes, which logically could not be the case. What distinguishes Apple from the New York Telephone Company is that New York Telephone Company was "a highly regulated public utility with a duty to serve the public,"¹²⁰ while Apple is a public company¹²¹ with a primary responsibility of ensuring the financial stability of its stock for its shareholders.

Looking at the second prong, which asks whether the request places an unreasonable burden on the third party,¹²² it is readily apparent that the FBI's request placed an unreasonable burden upon Apple when it demanded Apple to make a backdoor for the shooter's phone. The precedent of granting and enforcing the order is in and of itself an undue burden on Apple. Domestically, Apple would likely face a veritable tidal wave of requests from other law enforcement and prosecutorial agencies (notably the Manhattan District Attorney's office),¹²³ in effect transforming Apple from a technology retail company into a government pawn. While more tangential and less of a burden, but still deserving of consideration, is the effect of the invocation and enforcement of an order under AWA to compel other technology companies to assist the government.

While the government vehemently expressed that only the target phone and Apple would be subject to the writ,¹²⁴ this clearly is a farce. Google also had received requests to unlock devices,¹²⁵ pursuant to the AWA, prior to the San Bernardino litigation, and the FBI and other prosecutorial agencies' comments following the government's success in unlocking the iPhone

¹¹⁸ *Id.* at 174.

¹¹⁹ Vailshery, *supra* note 82.

¹²⁰ *N.Y. Tel. Co.*, 434 U.S. at 174 (emphasis added).

¹²¹ *Investor Relations: Frequently Asked Questions*, *supra* note 87.

¹²² *N.Y. Tel. Co.*, 434 U.S. at 175.

¹²³ Selyukh, *supra* note 105.

¹²⁴ Memorandum of Points and Authorities, *supra* note 73, at 4; James Comey, *We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead*, LAWFARE (Feb. 21, 2016, 9:03 PM), <https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead>.

¹²⁵ *All Writs Act Orders for Assistance from Tech Companies*, *supra* note 5.

suggest that the government would not hesitate to use the AWA in a future dispute between a tech company and government agency.¹²⁶ What the FBI asked of Apple in the San Bernardino litigation, and potentially in future litigation, is an unreasonable demand upon the company.

Finally, the third prong of the test asks whether the government would be able to accomplish its task without the assistance of the third-party.¹²⁷ There is evidence to indicate that the FBI could have accessed the data on the San Bernardino shooter's phone without the assistance of Apple.¹²⁸ Had the FBI not requested the SBCPHD change the iCloud password on the shooter's phone, it is possible that the Bureau could have accessed the information without having to even ask for Apple's assistance.¹²⁹ Furthermore, there is reason to believe that other government agencies potentially possessed software that could be used to unlock the shooter's phone.¹³⁰ Similarly, had the FBI engaged in better communication within its own departments, it would have realized at an earlier date that its elite cyber unit, the ROU, had the capability of procuring contractors to unlock the phone.¹³¹

Using the facts specific to the San Bernardino litigation, it is clear that the government's request to use the AWA to unlock the shooter's phone fails the *New York Telephone* test. Any future scenarios in which a technology company's assistance is requested by a government agency would have to be analyzed on a case-by-case basis; however, certain elements that weighed against the government in the San Bernardino dispute would still weigh against the government in future disputes.

Apple is still far removed from the controversy and, unlike *New York Telephone*, which was a public utility,¹³² is a publicly traded company¹³³ with a duty to its shareholders rather than the public. Other technology companies potentially subject to the use of the AWA in the future, such as Alphabet

¹²⁶ Kravets, *supra* note 106; Selyukh, *supra* note 105.

¹²⁷ *N.Y. Tel. Co.*, 434 U.S. at 175.

¹²⁸ Declaration of Erik Neuenschwander, *supra* note 74, at 11.

¹²⁹ *Id.*

¹³⁰ Transcript of Argument, *supra* note 77, at 3–4.

¹³¹ DEP'T JUST. OFF. INSPECTOR GEN., *supra* note 112, at 9; Landau, *supra* note 113.

¹³² *N.Y. Tel. Co.*, 434 U.S. at 174.

¹³³ *Investor Relations: Frequently Asked Questions*, *supra* note 87.

(Google's parent company),¹³⁴ Microsoft,¹³⁵ or Amazon,¹³⁶ are publicly traded companies that have duties to their shareholders rather than the public. Had the government enforced the court's order and compelled Apple to create a "back-door," it would have had a chilling domino effect upon the technology industry.

There is nothing to suggest that the government would stop with Apple in its campaign to conscript the technology industry in its crusade to fight encryption; in fact, there is significant evidence to suggest that the opposite is true.¹³⁷ Such effect would potentially have the practical result of stymieing development of greater and stronger encryption methods, the net effect of which is the endangering not only the average American citizen but also members of our intelligence communities and armed forces. The precedential effect of forcing technology companies, pursuant to the AWA, to either unlock devices or decrypt data has potential serious international consequences. If, domestically, the United States government can force Apple or other companies to unlock devices, what is to stop foreign countries from forcing these companies to install backdoors and mechanism to monitor its citizens communications?

It is unclear whether the FBI (or other government agencies) would be able to access information using the same method the FBI did to access the information on the San Bernardino shooter's phone. Following the dispute between Apple and the FBI, two companies have emerged that have specialized in creating devices that allow law enforcement agencies to access encrypted phones: Israeli forensic firm Cellebrite¹³⁸ and Grayshift, a company allegedly run by experienced U.S. security contractors and a former

¹³⁴ *Alphabet Replaces Google Publicly Traded Company*, FOX BUS.: TECH. (Oct. 2, 2015), <https://www.foxbusiness.com/features/alphabet-replaces-google-as-publicly-traded-company>; Avery Hartmans & Mary Meisenzahl, *All the Companies and Divisions Under Google's Parent Company, Alphabet, Which Just Made Yet Another Shake-Up to its Structure*, BUS. INSIDER (Feb. 12, 2020, 10:58 AM), <https://www.businessinsider.com/alphabet-google-company-list-2017-4>.

¹³⁵ *Frequently Asked Questions: Investor Relations*, MICROSOFT, <https://www.microsoft.com/en-us/Investor/FAQ.aspx> (last visited Jan. 1, 2020).

¹³⁶ *Investor Relations: Frequently Asked Questions*, AMAZON, <https://ir.aboutamazon.com/faqs/default.aspx> (last visited Jan. 3, 2021).

¹³⁷ Selyukh, *supra* note 105; Kravets, *supra* note 106.

¹³⁸ Jack Nickas, *Apple to Close iPhone Security Hole That Law Enforcement Uses to Crack Devices*, N.Y. TIMES (June 13, 2018), <https://www.nytimes.com/2018/06/13/technology/apple-iphone-police.html>.

Apple engineer.¹³⁹ While Apple and other companies have drafted updates to its software that render these decoding devices useless,¹⁴⁰ companies like Cellebrite have found other ways to break the encryption.¹⁴¹ Therefore, it is unclear whether the government would be able to meet the third element of the *New York Telephone* test, the ability of the government to accomplish its goal without the assistance of the third party,¹⁴² and successfully compel a future tech company's service.

III. PROPOSED SOLUTIONS

The security of a nation and the privacy of its citizens must be balanced to ensure a healthy democracy. Government agencies should have access to encrypted data, pursuant to a lawful warrant or subpoena, in order to combat crime and conduct a proper investigation. But forcing technology companies, as the FBI attempted, under the mantle of the AWA, into the service of the government to forcibly decrypt or access a device is not the proper solution. Cooperation between the technology sector and legislature is needed to draft proper legislation that ensures limited, legal access to devices to further a proper investigation.

The AWA is not the proper vehicle for such access. Its vagueness, while proper for its role as a gap-filling measure,¹⁴³ makes it improper for the type of use the government intends: an order that gives the government carte blanche to force companies to comply in whatever way, shape or form with its demands. The lack of determinable limits means that the government could try and extend the use of the AWA beyond decrypting devices into other spheres. The government's patience with companies like Apple is wearing thin,¹⁴⁴ and rightfully so: the companies need to be part of a solution

¹³⁹ *Id.*; Thomas Brewster, *Mysterious \$15,000 'GreyKey' Promises to Unlock iPhone X for the Feds*, FORBES (Mar. 5, 2018, 12:10 PM), <https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#20ddd5f52950>.

¹⁴⁰ Nickas, *supra* note 138.

¹⁴¹ Andy Greenberg, *Cellebrite Says it Can Unlock Any iPhone for Cops*, WIRED (June 14, 2019, 6:05 PM), <https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/>.

¹⁴² *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 175 (1977).

¹⁴³ *See Pa. Bureau Corr. v. U.S. Marshals Servs.*, 474 U.S. 34, 43 (1985).

¹⁴⁴ Laura Feiner, *Senators Threaten to Regulate if Tech Companies Won't Do It Themselves*, CNBC (Dec. 10, 2019, 2:38 PM), <https://www.cnbc.com/2019/12/10/senators-threaten-encryption-regulation-for-tech-companies.html>.

to a problem that is not going away anytime soon. Such compromise is not inconceivable; Apple allegedly backed off of an idea to encrypt iCloud backups after learning from the FBI the potential difficulties it would cause to law enforcement investigations.¹⁴⁵ Key to any viable solution will be cooperation and compromise between the government and the technology industry.

This author does not possess the technological expertise to offer a potential technological solution to the problem. This author does argue, however, that the creation of backdoors, regardless of whether it is for one device or fifty, is not the appropriate answer to this difficult problem. It is expected that the solution will involve a technical aspect; however, backdoors should not be included or considered. What this Paper does suggest is that a practical, legislative response is needed to best address the issue. Reliance on a case that was decided before the technology involved was even conceived is not the appropriate way to tackle changing technology and develop a jurisprudence that can grow as our knowledge of technology grows. Enacting a statute or act with input from the technology industry will allow for the creation of legislation that is most adept at tackling issues, such as accessing encrypted devices, which is equitable and fair.

Such legislation potentially could take the form of an act like the Communication Assistance for Law Enforcement Act (“CALEA”), which requires telecommunication services and providers to maintain a certain level of access for law enforcement to access data when necessary.¹⁴⁶ Any piece of legislation should include a mechanism that allows for prompt judicial review of a decision which allows for access to an encrypted device and use the factors set out in *New York Telephone* as a guide for weighing whether the requested assistance is reasonable and fair and whether the entity’s assistance is really needed.

¹⁴⁵ Joseph Menn, *Exclusive: Apple Dropped Plan for Encrypting Backups After FBI Complained—Sources*, REUTERS (Jan. 21, 2020, 7:07 AM), <https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT>.

¹⁴⁶ *Communications Assistance for Law Enforcement Act*, FCC (Oct. 20, 2020), <https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance>.

IV. CONCLUSION

Technology is ever evolving. From self-driving cars to smartphones, it is an integral part of our lives with an ever-increasing presence. However, as companies seek to increase the security of our devices, the government seeks to have easier access to the devices and data. With increasing frequency, the government has turned to the little known and arcane All Writs Act to try and compel companies such as Apple¹⁴⁷ to unlock seized devices. While law enforcement agencies have every right to have access to the data, pursuant to a valid search warrant, the AWA is the wrong vehicle to facilitate access to the device. Using the three-prong *New York Telephone* test, with the facts from the San Bernardino litigation as an example, it is clear that the government's request fails the test, illustrating how the AWA is the improper vehicle.

To ensure that the government can achieve access to seized devices that are otherwise inaccessible due to encryption or passcodes, the legislature and technology industry need to come together and work on a potential solution. Any solution must be agreeable to both sides and allows the government to have the access it needs while still preserving the technological security of the American people.

The battle between the FBI and Apple is far from over. As recently as January 7, 2020, the FBI is demanding Apple's assistance in unlocking the phone of the suspected terrorist who went on a shooting rampage at a Florida Naval base.¹⁴⁸ Americans as a society value freedom, democracy, and privacy. The debate over "backdoors," end-to-end encryption, and government access to data will not be easy but it must be done (and soon) to create a solution acceptable to both parties before it is too late.

¹⁴⁷ *All Writs Act Orders for Assistance from Tech Companies*, supra note 5.

¹⁴⁸ Devlin Barrett, *FBI Asks Apple for Help Cracking Pensacola Gunman's iPhone*, WASH. POST (Jan. 7, 2020, 3:51 PM), <https://www.washingtonpost.com/national-security/fbi-asks-apple-for-help-cracking-pensacola-gunmans-iphones/2020/01/07/b829ac72-3178-11ea-91fd-82d4e04a3facstory.html>.

