WHETHER THE DEPARTMENT OF JUSTICE SHOULD HAVE THE AUTHORITY TO COMPEL APPLE INC. TO BREACH ITS IPHONE SECURITY MEASURES

*Stephen J. Otte**

I. INTRODUCTION

On December 2, 2015, in San Bernardino California, fourteen people were killed and another twenty-two wounded in what would be one of the worst terrorist attacks since September 11, 2001.[1] In the investigation that followed, the Federal Bureau of Investigation (FBI) recovered twelve pipe bombs, thousands of rounds of ammunition, and three iPhones.[2] Although two of the phones were crushed, the third, an iPhone 5c running on operating system iOS 9 was intact. [3] As the investigation continued, the FBI believed that the perpetrator, Syed Rizwan Farook (Farook), used that phone to communicate with some of the victims of the massacre.[4] However, the FBI did not have the pass code to the phone and, although they could have tried to guess it, the phone would permanently erase all its data after ten incorrect guesses.[5] Furthermore, even though Farook's employer owned the phone and had access to the phone's iCloud account (an account where the phone's data is stored in a separate physical location from the phone), the FBI learned that Farook had not updated his iCloud since October 2015.[6] Thus, the only way for the FBI to retrieve the phone's data would be for them to crack the phone's password to which no one had access, not even the company that created the phone: Apple Inc. (Apple).

Realizing this dilemma, the FBI issued a warrant to search the data stored on the phone.[7] At first, Apple complied with the FBI's demands and provided as much assistance as possible.[8] After these initial efforts failed and it became clear that there was no other apparent way to access the phone, the FBI requested that Apple create software that would bypass

* Associate Member, 2015–2016 *University of Cincinnati Law Review*.

1. Lev Grossman, *Inside Apple CEO Tim Cook's Fight With the FBI*, TIME (Mar. 28, 2016), http://time.com/4262480/tim-cook-apple-fbi-2/.

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. Grossman, *supra* note 1.

8. *Id.*

the phone's security system.[9] Apple refused.[10] In response, the government sought an order for compulsion in the Federal District Court of Central California.[11]

The case was heard by a magistrate judge who ruled that Apple must honor the search warrant and assist the authorities in accessing the encrypted iPhone 5c.[12] As a result, the court granted the FBI's order of compulsion. Furthermore, the court directed Apple to provide reasonable technical assistance to assist law enforcement agents in obtaining access to the data pursuant to the government's authority under the All Writs Act.[13] The order defined "reasonable technical assistance" to include creating custom software that could be loaded on the iPhone to accomplish three goals: (1) bypass or disable the iPhone's "auto-erase" function; (2) enable the FBI to electronically submit passcodes to the device for testing, bypassing the requirement that passcodes be manually entered; and (3) remove any time delays between entering incorrect passcodes.[14]

Apple appealed the magistrate's order;[15] however, in March 2016, the case was dismissed because the FBI found an alternative means to unlock the phone. Although the merits of this case were never heard, the profound legal issues involved are far from resolved. Rather, they are becoming more and more pressing. In particular, law enforcement agencies have increasingly asked the FBI for assistance in searching encrypted devices, including iPhones, tablets, and computers.[16] Based on this data, it is clear that the San Bernardino case will not be a singular incident. As the FBI is faced with more and more encryption cases, it is inevitable that it will continue to rely on the All Writs Act to compel compliance.

As a result of this increased use, courts must determine whether the All Writs Act is an appropriate mechanism to force tech companies to comply with law enforcement efforts. To date, there is little, if any, case law indicating whether law enforcement agencies have a right under the All

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. Order Compelling Apple Inc. to Assist Agents in Search at 1, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016); 28 U.S.C. § 1651 (2012).

14. Order Compelling Apple Inc. to Assist Agents in Search, *supra* note 13, at 2.

15. Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10, 2016 WL 767457 (C.D. Cal. Feb. 25, 2016).

16. Grossman, *supra* note 1, at 5.

Writs Act to require that tech companies produce their client's encrypted data in compliance with a search warrant. Nonetheless, as the number of cases continues to grow, courts will soon be charged with making determinations on this particularly complex issue.

This Comment discusses whether the government should have the authority under the All Writs Act to compel tech companies to create software that bypasses their own built-in

security features. Part II provides a historical background of the All Writs Act and discusses why it is pertinent to tech cases including the most recent controversy involving Apple. Part III argues that the government should not have the authority to compel information technology companies to create software that jeopardizes customer security. Specifically, this section argues that the All Writs Act should not be applied to technology encryption cases because it is unreasonable, violates Fifth and First Amendment liberties, and is inconsistent with the Communication Assistance for Law Enforcement Act. Finally, Part IV provides an analysis of the precedential implications this case may have on future technology search and seizure cases, and suggests solutions to what will be a growing battle between the government's interest to investigate crime and every individual's privacy.

II. BACKGROUND

Law enforcement has long enjoyed its authority to obtain search warrants to almost anything within the bounds of the Fourth Amendment. However, data encryption creates a dilemma for law enforcement because encrypted data is essentially warrant-proof. In theory, it is accessible, but in practice, law enforcement search and seizure of this data is practically impossible without a passcode. Faced with this dilemma, the government has argued that the All Writs Act is the best remedy to access this data because it allows law enforcement to compel data carriers to turn it over.[17]

Not surprisingly, in the most recent San Bernardino iPhone case, both Apple and the government vigorously defended their juxtaposed interpretation of the All Writs Act.[18] Although the merits of the case were not decided, the government will invariably continue to rely on the All Writs Act as it seeks to compel the release of stored encrypted information from electronic devices in the future.

According to its language, the All Writs Act authorizes the federal courts to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[19] In its

17. *Id.*

18. *See* Order Compelling Apple Inc. to Assist Agents in Search, *supra* note 13, at 1.

19. 28 U.S.C. § 1651(a) (2012); *see* Harris v. Nelson, 394 U.S. 286, 299 (1969).

original form, the All Writs Act was part of the Judiciary Act of 1789, which established the federal justice system.[20] Essentially, the All Writs Act was enacted to empower federal judges with the authority to issue court orders—also known as "writs"—to fill gaps within the law or administer justice absent a legal remedy.[21] The First Congress believed that the All Writs Act was sometimes appropriate for federal courts to exercise and protect their newly established jurisdiction.[22]

The All Writs Act has been interpreted to permit the courts to "order a third party to provide nonburdensome technical assistance to law enforcement officers."[23] In *Pennsylvania Bureau of Correction v. U.S. Marshals Services*, the Supreme Court explained, "[T]he All Writs Act is a residual source of authority to issue writs that are otherwise not covered by statute."[24] As such, the All Writs Act does not confer the judiciary with new sweeping power.[25] Rather, the it only allows the courts to issue orders that achieve "the rational ends of the law," and "the ends of justice entrusted to it."[26] In doing so, courts must apply the All Writs Act "flexibly in conformity with these principles."[27] Based on this language, it is clear that the scope of the All Writs Act is limited. Although such writs were once fairly common in Colonial America hundreds of years ago, the courts have restricted their issuance to only extraordinary circumstances where there is no articulable law.[28]

United States v. New York Telephone Co. is the quintessential case that defined the scope of the All Writs Act. Specifically, the Supreme Court established a three-factor test to determine the All Writs Act's appropriate usage.[29] In this case, the Court upheld a lower court order demanding that a phone company assist in implementing a pen register pursuant to a valid search warrant.[30] The Court found that there was "probable cause to believe that the [c]ompany's facilities were being employed to facilitate a criminal enterprise on a continuing basis," and compliance with the warrant was necessary.[31] The Court held that the order was a proper writ under the All Writs Act, because it was consistent with Congress's intent to compel third parties to assist the government in the use of surveillance

20. Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 40–41 (1985).
21. *See id.* at 41.
22. *See* Adams v. United States *ex rel*. McCann, 317 U.S. 269, 273 (1942).
23. Plum Creek Lumber Co. v. Hutton, 608 F. 2d 1283, 1289 (9th Cir. 1979).
24. *Pa. Bureau of Corr.*, 474 U.S. at 43.
25. *See, e.g.*, *Plum Creek Lumber Co.*, 608 F. 2d 1283.
26. United States v. N.Y. Tele. Co., 434 U.S 159, 172–73 (1977) (internal citations omitted).
27. *Id.* at 173.
28. Grossman, *supra* note 1.
29. *N.Y. Tele. Co.*, 434 U.S at 166–74 (1977).
30. *Id.* at 168.
31. *Id.* at 174.

devices.[32] Furthermore, the Court determined that the All Writs Act allowed for supplemental orders to third parties to aid in the execution of a search warrant because

> [t]he power conferred by the [All Writs] 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 implementation of a court order or the proper administration of justice, . . . and encompasses even those who have not taken any affirmative action to hinder justice.[33]

As noted above, the Supreme Court in *New York Telephone Co*. promulgated three factors that have since been used to determine whether the issuance of an All Writs Act order is appropriate.[34] The first factor is whether the issue is "so far removed from the underlying controversy that its assistance could not be permissibly compelled."[35] Next, the court must determine whether an issuance of an All Writs Act order would place undue burden on the affected party.[36] Third, the court must determine that assistance is necessary to achieve the purpose of the warrant.[37] Following *New York Telephone Co.*, it is clear that the All Writs Act should not be used every time the government needs information. Instead, it should only be used in most dire circumstances when the government has exhausted all other resources.[38]

However, this three-part test in *New York Telephone Co.* can be construed ambiguously. As a result, prosecutors and federal agencies alike have relied on it in a variety of circumstances, many of which arguably exceed the scope of the writ.[39] For example, in the San Bernardino Apple iPhone case, the government argued that it met *New York Telephone Co.*'s three requirements to issue the writ, even though the government's requests to Apple were much different than the requests made in *New York Telephone Co.*[40]

Unless the courts begin to define the scope of the All Writs Act as it pertains to these decryption cases, the writs will continue to be employed, sometimes successfully. Below are arguments why the All Writs Act

32. *Id.* at 176.
33. *Id.* at 174.
34. *Id.* at 173-74.
35. *N.Y. Tel. Co.*, 434 U.S at 174.
36. *Id.* at 175.
37. *Id.*
38. *Id.*
39. Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).
40. Order Compelling Apple Inc. to Assist Agents in Search, *supra* note 13, at 1.

should not provide the government with the authority to compel tech companies to develop decryption software against their own will.

III. ARGUMENT

As previously discussed in *New York Telephone Co.*, the district court compelled a telephone company to install a pen register device to detect criminal behavior.[41] In affirming the lower court's decision, the Supreme Court limited the scope of the All Writs Act by creating a three-part test.[42] Specifically, the test precluded future courts from asserting plenary power or "roving commission" in compelling third parties to assist in law enforcement efforts whenever those efforts were deemed to be expedient.[43] Thus, *New York Telephone Co.* and its progeny do not authorize courts to compel decryption of encrypted data. Although this Comment has discussed how the All Writs Act has previously been applied rather broadly, future decryption cases with facts similar to those of the San Bernardino case will most certainly fall beyond the scope of the All Writs Act. Thus, the government should not have the authority to compel information technology companies to create software that jeopardizes customer security. Specifically, the All Writs Act should not be applied to technology encryption cases because (1) it is unreasonable; (2) tech companies are too far removed from the *New York Telephone Co.* standard; (3) decryption software is not required to comply with the warrant; (4) it violates Fifth and First Amendment liberties; and (5) it is inconsistent with the Communication Assistance for Law Enforcement Act.

A. Orders Compelling Companies to Breach Their Own Security Devices Would Be Unduly Burdensome.

According to the holding in *United States v. Hall*, a valid order pursuant to the All Writs Act "must not adversely affect the basic interests of the third party or impose an undue burden."[44] In *New York Telephone Co.*, the company had previously used pen registers for billing purposes as well as to trace harassing phone calls.[45] Hence, the order to use the same pen registers for crime detection was not an undue burden. Thus, when determining the validity of an order pursuant to the All Writs Act, the

41. *N.Y. Tele. Co.*, 434 U.S at 161.
42. *Id.* at 172–73.
43. *Id.* at 181.
44. United States v. Hall, 583 F. Supp. 717, 719 (E.D. Va. 1984).
45. *N.Y. Tel. Co.*, 434 U.S at 174.

courts must assess the reasonableness of an order.[46]

Likewise, in all subsequent "telephone" cases where the courts relied on the All Writs Act, third parties were already equipped with the resources necessary to comply with the demand.[47] In other words, the effected parties could comply with the court order simply by employing preexisting procedures. For example, in *Plum Creek Lumbar Co. v. Hutton*, the Ninth Circuit emphasized that courts may compel third parties "to provide nonburdensome technical assistance."[48] The court also clarified that the All Writs Act does not permit "forcing an employer to rescind a company policy so that [government agencies] can more efficiently conduct an investigation."[49]

Based on this case law, the government's reliance on the All Writs Act in encryption cases will likely violate the requirements of *New York Telephone Co.* because future demands will surely impose an unreasonable "undue burden." This is especially true in instances, like the San Bernardino Apple case, where the government demands that the company produce new software, ultimately eliminating any security measures companies spent millions of dollars creating. Because no such operating system is likely to exist, tech companies can only comply with these orders by creating entirely new operating systems. Thus, they would need to write an entirely new code, instead of disabling an existing one. Engineers would subsequently have to develop a product that the company has no desire to make.

In essence, the government would not be asking tech companies to facilitate their efforts through implementing a program in the course of normal business. Instead, the government would be demanding a fundamental change in the way most companies do business: they would be asking these companies to create and pay for a product that is not even their idea, but the government's inception. This is an unacceptable enlargement of the "no burdensome technical assistance" requirement because it demands unreasonable time and money.

Accordingly, in future tech encryption cases, orders compelling companies to create new software that would eviscerate their own security features should be deemed to fall outside the permissible scope of the All Writs Act because they place an undue burden on these companies; these demands adversely affect the basic interests of the companies. Not only do companies like Apple, Google, or Facebook have a legitimate interest

46. *Id.* at 172.

47. *See In re* Application of the U.S. for an Order, 616 F.2d 1122, 1126 (9th Cir. 1980) (where the company used trap and trace devices that the Government requested)*; see also In re* Application of the U.S, 128 F. Supp. 3d 478 (D.P.R. 2015).

48. Plum Creek Lumber Co. v. Hutton, 608 F. 2d 1283, 1289 (9th Cir. 1979).

49. *Id.* at 1290.

in safeguarding the security of hundreds of millions of customers who depend on data protection systems to ensure their privacy, but these companies also have a legitimate interest in resisting orders to develop software that currently does not exist because new software developments require significant amounts of time and money. Even if the government can demonstrate that compliance with their request is technically feasible, the undue burden or reasonableness standard derived from *New York Telephone Co.* should preclude any All Writs Act order.

B. Tech Companies Are Too Far Removed Under the Standard Set Forth in New York Telephone Co.

In *New York Telephone Co*., the Supreme Court held that the All Writs Act cannot be applied to compel a third party to act if that party is too far removed from the original controversy.[50] Because criminal activity was being facilitated via the telephone company's own services and phone lines, the underlying controversy was not so far removed. Thus, the court upheld the order to install the pen register under the All Writs Act.[51]

For tech companies such as Apple, however, the underlying controversy is simply too far removed. These tech companies have no connection to the data that exists on their devices, and they do not exercise control regarding how their users collect or store their private information. Unlike the New York Telephone Company, tech companies like Apple are unable to readily monitor their client's personal data. Moreover, the difference between installing a pen register and forcing a company to decrypt its users' devices is blatantly obvious. Specifically, a pen register simply records data that is readily available to the company; however, decryption requires specially designed software in order to venture into an individuals' private life, which is an invasive and exacting task. If the underlying controversy truly requires this degree of inquisition, it most certainly should fall beyond the scope of the All Writs Act.

Finally, by forcing companies to enact this extra requirement, the government exceeds the scope of the traditional search warrant because it cannot possibly identify a particular person or property without also requesting a particular form to satisfy the warrant. Requesting such particular form, however, has never been a requirement of satisfying a search warrant. Even in *New York Telephone Co*., the Supreme Court recognized that the order to install a pen register constituted a legitimate seizure within the bounds of Federal Criminal Procedure Rule 41 because

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

51. *Id.*

it did not expand the breadth of a valid search warrant.[52] The Court noted that the pen register was both implicit and necessary for the effectuation of the search warrant.[53] Creating decryption software, however, would exceed the breadth of a valid search warrant because, in order to comply with it, a company would act in ways that are neither implicit nor necessary for warrant's effectuation.

Accordingly, in future decryption cases, courts should reject motions to compel encrypted data because the tech companies are simply too far removed from the underlying case to be forced to comply. Moreover, traditional notions of search and seizure law do not allow the government to specify the particular form of the seized property, which is exactly what the government did with Apple.[54] Instead, the government may only seize property in its original form to satisfy a search warrant. The All Writs Act does not usurp this basic principle by allowing the government to enlarge the requirements of a valid warrant by requiring a third party to alter its form. This principle is true even if the modification request make the property more useful in a criminal investigation.

C. Forcing Companies to Create Decryption Software Is Not Necessary to Achieve the Purpose of the Warrant

In *New York Telephone Co.*, the Supreme Court held that third parties cannot be forced to assist the government unless the government has the authorization to act and the third party's participation is necessary to achieve the purpose of the warrant.[55] The Court determined that a court order pursuant to the All Writs Act is appropriate when "there is no conceivable way" to accomplish surveillance without the company's assistance.[56] The Court also held that the order compelling the phone company's compliance was necessary "to prevent nullification of the court's warrant" and "to put an end to this venture."[57]

Likewise, in the wave of future tech encryption cases, the government will have difficulty demonstrating that it has exhausted all other avenues in order to recover the information. For instance, the government will not likely meet their burden of showing that the All Writs Act is absolutely

52. *Id.* at 169–70. Federal Criminal Procedure Rule 41 concerns the procedure for obtaining a search warrant in a Federal criminal investigation.

53. *Id.*

54. Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971, 991–92 (2012).

55. *N.Y. Tel. Co.*, 434 U.S at 169–70.

56. *Id.* at 175 (noting that FBI had conducted "an exhaustive search" for a way to install a pen register in an undetectable location).

57. *Id.* at 174, 175 n.23; Mich. Bell Tele. Co. v. United States, 565 F.2d 385, 389 (6th Cir. 1977) (holding that telephone company was "the only entity that c[ould] effectuate the order").

necessary to effectuate future cases involving encrypted data because there are government agencies that specialize in digital forensics. Furthermore, since Apple has the digital "keys" to iCloud backups, if the San Bernardino shooter had updated his device, this dilemma would not have even existed because that "key" could have been subpoenaed.

Finally, decrypting data may not be as necessary given the amount of "free" data we release every day. Whether through social networks, surveillance cameras, or even our Fitbits, we spew data all the time. With so much data readily available, it may not be necessary or appropriate for law enforcement to access every last private sphere of our digital lives. Accordingly, the government will be hard pressed to demonstrate that orders pursuant to the All Writs Act are absolutely necessary to achieve the purpose of the warrant. Therefore, the government will most likely fail under the third factor derived from *New York Telephone Co.*

D. The Government's Order Violates the Fifth Amendment

The government's interest in encrypted data cases will undoubtedly implicate fundamental liberty and property interests, which raises Fifth Amendment concerns. Prior case law has already suggested that an order pursuant to the All Writs Act may trigger Fifth Amendment concerns.[58] In *In re Application of U.S. for Order Authorizing Installation of Pen Register or Touch Tone Recorder & Terminating Trap*, the Third Circuit noted that it easily found a deprivation of a property interest because the tracing orders denied applicants the free use of their equipment and of the services of their employees, basic property and contract interests to which they were entitled.[59]

Courts have also held that an affected third party is entitled to a hearing at which they may contest the order.[60] While the hearing fulfills the procedural component of the Fifth Amendment's due process clause, courts have also recognized a substantive limit on the scope of the All Writs Act in regards to the rights of third parties, namely that the assistance required must not be unreasonably burdensome.[61]

Tech companies like Apple have especially acute Fifth Amendment liberty interests at stake in decryption cases. Those interests include protection of their business model and "expectancy of continued patronage," which the courts have recognized as a legitimate property

58. *See In re* Application of the U.S., 128 F. Supp. 3d 478 (D.P.R. 2015).

59. *In re* Application of U.S.A for Order Authorizing Installation of Pen Register, 610 F.2d 1148, 1156 (3rd Cir. 1979).

60. *Id.* at 1157 (concluding that due process requires a hearing on the issue).

61. *See, e.g.*, *N.Y. Tel. Co.*, 434 U.S at 172 (finding the power of federal courts to impose duties on third parties are not without limits—unreasonable burdens may not be imposed.).

interest.[62] Although there is little precedent interpreting the substantive limits on the government's power to compel third parties to assist in in criminal investigations, there is convincing evidence to conclude that the Fifth Amendment forbids the type of assistance the government seeks in the present case: forced assistance of a third party that has not itself been involved in any wrongdoing and that does not possess any control over the desired evidence.

That type of "assistance" is fundamentally inconsistent with the Fifth Amendment, which guarantees freedom from governmental interference absent due process.[63] In the Apple case, for example, this would mean that Apple either acted wrongly or was in possession or control of information to which the government was entitled. As previously discussed, there is nothing to suggest that either of those conditions were met: Apple was not connected to the underlying investigation and the government could not force Apple to comply based on the factors set forth in *New York Telephone Co.*

Although other All Writs cases previously discussed did not address substantive due process concerns, those cases are distinguished from the present types of cases. In non- decryption cases, compelled assistance was deemed permissible because third parties possessed and controlled the very information the government intended to collect. In *New York Telephone Co.*, the Court's own language evinces limits on the types of information and parties the courts can compel to comply with an All Writs order.[64] For instance, when considering whether the New York Telephone Company was too far removed from the underlying controversy, the natural inference is that the Court was concerned with the due process liberty interests of innocent third parties.[65] Furthermore, unlike the New York Telephone Company, which was a "highly regulated public utility with a duty to serve the public," companies like Apple, Google, or Facebook are private companies that ensure privacy and security to its consumers.[66] In other words, most of these companies do not serve a public function; they operate with their client's security and privacy in mind.

Accordingly, in the Apple case and future encryption cases, the facts are distinguished from *New York Telephone Co.* in two critical aspects: (1) most tech companies do not possess or control the information requested; and (2) these companies have a business interest that would be

62. *See, e.g.*, Newark Morning Ledger Co. v. United States, 507 U.S. 546, 555 (1993).

63. *See* U.S. CONST. amend. V.

64. *N.Y. Tele. Co*., 434 U.S at 174.

65. *See id.*

66. *Id.* at 175.

severely harmed if it was forced to comply.[67] Hence, these tech companies most certainly have a legitimate liberty interest that should be protected by the Fifth Amendment.

E. Forcing Apple to Create Software Is Compelled Speech

In order for tech companies like Apple to assist the government in cracking security measures on their own products, they would have to write new software that would remove the security features already in place. However, for most devices to recognize this change in software, they must be cryptographically "signed" by the company. By forcing tech companies to comply with such an order and "sign" the new software, the government would effectively be compelling that company to speak.[68] As several courts have noted, compelled speech is unconstitutional unless it meets the rigorous criteria to overcome strict scrutiny.[69] Although most prior cases involving government efforts to compel speech have involved labeling the ingredients, nutritional information, or health and safety information on products, compelled speech is not limited to cases involving the public welfare.[70] In *Central Hudson Gas and Electric v. Public Service Commissioner of New York*, the Supreme Court distinguished between commercial and noncommercial speech when discussing the parameters of lawfully compelled speech.[71] The Court held that commercial speech was afforded less protection than social, political, or religious speech because it entailed only the commercial interests of the speaker and the audience.[72]

According to the *Central Hudson* test, labeling requirements are constitutional because they serve a very limited purpose: public health.[73] Based on this holding, courts have determined that anything other than commercial speech is afforded the same level of First Amendment protection. In *Riley v. National Federation of the Blind of North Carolina, Inc.*, the Supreme Court held that compelled speech that was noncommercial in nature must be treated as a content-based restriction, which means it was subject to strict scrutiny.[74] The Court further noted that "in the context of protected speech, the difference [between

67. *Id.* ("[I]t can hardly be contended that the Company . . . had a substantial interest in not providing assistance.").

68. *See* Riley v. Nat'l Fed. of the Blind of N.C., Inc., 487 U.S 781, 796–97 (1988).

69. *See, e.g.*, Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 564–65 (1980).

70. *Id.*

71. *Id.* at 561–63.

72. *Id.* at 561.

73. *Id.* at 563–64.

74. Riley v. Nat'l Fed. of the Blind of N.C., Inc., 487 U.S 781, 798 (1988).

compelled speech and compelled silence] is without constitutional significance;" therefore, any compulsion on the government's behalf was highly scrutinized.[75] Finally, the Ninth Circuit has held that encryption software, in its source code form and as employed by those in the field of cryptography, is "expressive for First Amendment purposes, and thus is entitled to [strict scrutiny]."[76] Thus, compelling a tech company to write new code may constitute compelled speech prohibited by the First Amendment.[77]

Here, it is clear that companies in positions analogous to Apple's position in the San Bernardino case deserve First Amendment protection. Forcing tech companies to write a new code should be considered compelled speech, and strict scrutiny must apply because the speech in question is not commercial in nature.[78] Because the government will be unlikely to identify a compelling interest or to show that it narrowly tailored the request in a means that was least restrictive, future orders to compel encrypted data from personal devices should not survive First Amendment considerations.

F. Communication Assistance for Law Enforcement Act Precludes the Government's Demands.

In addition to the previously cited case law suggesting that that All Writs Act is an inappropriate mechanism to assert governmental control over tech companies, statutory law also supports the conclusion that the government does not have authority to compel these companies to create decryption software. Specifically, Congress enacted the Communication Assistance for Law Enforcement Act (CALEA) to address the circumstances when third party private companies must assist law enforcement in electronic surveillance.[79] Within CALEA, Congress decided not to require electronic communication service providers to comply with a decryption order when the company does not retain a copy of the decryption key.[80] Instead, Congress opted to preclude companies like Apple from complying with these types of orders because Congress was keenly aware that the present issue may arise.

---

75. *Id.*

76. Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir. 1999), *reh'g granted, opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

77. *Id.* at 1146.

78. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557 (1980).

79. Barbara J. Van Arsdale, Annotation, *Construction and Application of Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C.A. §§ 1001 to 1010*, 25 A.L.R. Fed. 2d 323 (2016).

80. *Id.*

At the section entitled "Design of features and systems configurations," the statute provides that it

> does not authorize any law enforcement agency or officer—(A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or (B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.[81]

Companies like Apple unquestionably serve as a provider of "electronic communications services" because the services it provides meet this definition.[82] Therefore, CALEA should preclude the government from using the All Writs Act to require companies like Apple to provide assistance with orders to compel decryption. However, even if Apple was not covered by CALEA, the law does not hold covered telecommunication carriers responsible for "decrypting, or *ensuring the government's ability to decrypt*, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[83]

Finally, Congress has never authorized judges to compel third parties to provide decryption services to the FBI.[84] In fact, Congress has explicitly withdrawn this type of authority in other contexts.[85] Additionally, federal courts do not recognize an inherent authority to command non-parties to become de facto agents for the government during ongoing criminal investigations.

Thus, if courts utilize the All Writs Act as a means to expand the CALEA, this would not only represent a stark departure from statute, but this would also violate the separation of powers doctrine.[86] Furthermore, because "Congress may not exercise the judicial power to revise final

81. 47 U.S.C. § 1002(b)(1) (2012).

82. Pursuant to the statute, communications services providers are legally obligated to assist law enforcement in carrying out communications surveillance. *FAQ on the CALEA Expansion by the FCC*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/calea-faq#3 (last visited Sept. 12, 2017).

83. *Id.* § 1002(b)(3) (emphasis added).

84. *Id.*

85. *Id.*

86. Clinton v. Jones, 520 U.S. 681, 699 (1997) (citing Plaut v. Spendthrift Farm, Inc., 514 U.S. 211 (1995)).

judgments," so too should judges avoid judicial activism by construing statutes to meet the demands of society.[87]

V. CONCLUSION

Devices such as our phones, computers, and other tech devices contain unprecedented personal intimacy. Our health, finances, money, conversation analytics, GPS positions, and search histories are all recorded by our personal devices; we truly live in an age of surveillance. For better or worse, these devices allow law enforcement to invade that intimacy like never before. For instance, since October 2015, more than 500 phones have been streamed into the FBI's Computer Analysis Response Team and the agency's Regional Computer Forensic Lab in order to decrypt them.[88] In a separate survey conducted by the Manhattan District Attorney's Office, which consisted of more than a dozen state and local law enforcement agencies, researchers found that more than 1,000 smart phones and other devices have blocked investigators.[89] The question is simply: how or where do we draw the line? According to Tim Cook, CEO of Apple, "if the All Writs Act can be used to force us to do something that would make millions of people vulnerable, then you can begin to ask yourself, [i]f that can happen, what else can happen . . . [m]aybe law enforcement would like the ability to turn on the camera on your Mac."[90]

As the government continues to rely on the All Writs Act to compel encryption, courts must draw that line. Furthermore, that line must take into account the incredible privacy interests at stake. While the law may be considered unclear to some, what is at stake is not. If courts determine that the government may mandate tech companies to create tools for cracking into their customers privately stored data, the security of every personal device may be at risk; every individual who uses these devices may be at risk. Whether it is a cell phone, computer, or tablet, companies like Apple, Google, and Facebook all fear that hackers can and will find ways to break into personal devices, threatening peoples' most intimate and sensitive information.[91] In a world where so much of our personal information is stored on electronic devices, finding the appropriate

87. *Id.; see* Clark v. Martinez, 543 U.S. 371, 391 (2005)*; see also* Alzheimer's Inst. of Am. Inc. v. Elan Corp., No. C-10-00482, 2013 WL 8744216, at *2 (N.D. Cal. Jan. 31, 2013) (finding that Congress alone has authority to update a "technologically antiquated" statute "to address the new and rapidly evolving era of computer and cloud-stored, processed and produced data").

88. Kevin Johnson, *Hundreds of Requests to Unlock Phone Flood FBI*, USA TODAY (Apr. 6, 2016) http://www.usatoday.com/story/news/nation/2016/04/06/iphone-fbi-farook-encryption/82699532/.

89. *Id.*

90. Grossman, *supra* note 1.

91. *See id.*

balance between privacy and national security will become exceedingly challenging and delicate.

However, the courts are not without guidance. When this line of cases arises yet again, courts must be faithful to the narrow scope of the All Writs Act as well as the exceptions provided for under CALEA. They must not expand the All Writs Act to cover territory it was never allowed to cover. This may ultimately require courts to stand firm even when the public pressures the government to take certain measures in preventing terrorism and other atrocious acts. Yet, they must do so because the cost of allowing the government to hijack the security of our personal devices is simply too great.[92]

The implications of precedent permitting the hijacking of personal devices would have profound implications on not only a personal level, but also on a global scale. As more and more of our infrastructure and national security is controlled and monitored electronically, the stability of our world will depend on whether encrypted information that is stored and transmitted electronically is secure. Information that is not secure is likely to be hijacked by the very people we want to keep sensitive information away from: criminals and terrorists. This is not merely speculation. In 2015, hackers uncovered the identity of thirty-two million users from AshleyMadison.com, a site that facilitates adultery.[93] In December 2015, a hacker managed to disable a section of western Ukraine's power grid, leaving 230,000 people without electricity.[94] Finally, millions of Americans health information is hacked, stolen, and sold on the internet each year.[95] Undoubtedly, digital security is important to our personal and national safety. Therefore, the controversy surrounding data encryption cannot be reduced into the simplistic debate of privacy versus national security; it is exceptionally more complicated and must be treated as such by the courts.

As we move forward in the twenty-first century, we are going through two equal yet contradictory crises simultaneously: technology is "going dark" and information necessary for law enforcement is becoming ever more difficult to retrieve. However, if we look at the big picture, it can hardly be said that information is truly going dark. On any given day, we transmit information through a myriad of mechanisms from what we buy and what we search for online, to where we go and how we get there. While encryption may represent a small dark area of our lives, it represents but a mere fraction of the total data that flows out of our daily

92. *See id.*

93. *Id.*

94. *Id.*

95. Nsikan Akpan, *Has Health Care Hacking Beoming an Epidemic?*, PBS NEWSHOUR (Mar. 23, 2016), http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/.

lives. We are losing, and will likely continue to lose, our privacy in all aspects of life. Allowing the courts to force companies to implement software that would decrypt one of the few remaining realms of privacy in our lives would only exacerbate the private-less society we live in.