NOTE

A GLOBAL NETWORK FOR TREASON: THE INTERNET'S IMPERMISSIBLE BROADENING OF THE CLASS OF DEATH-ELIGIBLE DEFENDANTS UNDER § 904 OF THE UNIFORM CODE OF MILITARY JUSTICE

*Alexander J. Hendricks**

The cases of Pfc. Bradley Manning and Edward Snowden have generated controversy and debate across the United States. Both individuals took to the Internet to release classified operational details of the United States government. Supporters of Manning and Snowden label the two as heroes and argue that the decision to release the information was motivated by the need for transparency and accountability. The opposition condemns Snowden and Manning as traitors that deliberately provided the enemies of the United States with information that could be used for injurious purposes. Undoubtedly, the government of the United States is in the latter camp as revealed by its prosecutorial decisions. Though it has been unable to capture Snowden, the United States was able to subject Manning and charge him with a capital offense under § 904 of the Uniform Military Code of Justice, better known as Aiding the Enemy.

Manning was ultimately acquitted of Aiding the Enemy, but the facts of Manning's case and the hypothetical case against Snowden generate a need to reevaluate the validity of § 904's death penalty in the Internet era, where the transmission and exchange of information has reached a level of fluidity that was inconceivable at the enactment of § 904. This Note conducts that evaluation and concludes that executing a defendant under § 904 is "cruel and unusual punishment" and violates the Eighth Amendment. Section 904 violates the Eighth Amendment because the In-

* B.A., Political Science–Berkeley, 2012; Candidate for J.D., Cornell Law School, 2015. I would like to thank the Professors Weyble, who taught me about equally egregious forms of punishment: the death penalty and The Bluebook. I am thankful for my Cornell Journal of Law and Public Policy colleagues, particularly Katherine Hinderlie, Julia Livingston, and Jonathan Fitzsimons, for refining the roughest of drafts into presentable legal scholarship. Finally, I would like to thank my parents, Leif and Diane, and my siblings, Nick, Haley, and Gabi, for their unyielding support and love. May your reward be immortality via footnote.

ternet stripped the genuine narrowing function from the implicit aggravating circumstance of § 904. The Internet rendered the aggravating circumstance functionless by making all those who transact on its networks fulfill the mens rea *standard that is required for death eligibility under § 904. Because the Internet removes the narrowing function from the aggravating circumstance, the jury and prosecutor have unfettered discretion to pick from an impermissibly broad class of death-eligible defendants. This unfettered discretion drastically increases the risk for arbitrary death sentencing in violation of* Furman *and* Gregg*, which jointly held that a death sentence given without a meaningful basis is cruel and unusual punishment. Consequently, § 904 must be modified to heighten the* mens rea *required for death eligibility under § 904 to be a viable capital offense in the Internet era.*

INTRODUCTION

The Uniform Code of Military Justice (UCMJ) contains thirteen non-homicide offenses where execution is an available punishment.[1] One of these offenses, Aiding the Enemy (§ 904), has received notoriety recently because of the court martial of Pfc. Bradley Manning and the attempted extradition of Edward Snowden from Russia. Section 904 details in part that "any person who . . . knowingly . . . gives intelligence to . . . the enemy, either directly or indirectly; shall suffer death or other such punishment as a court-martial or military commission may direct."[2]

Manning and Snowden's cases both involve the knowing, but indirect, distribution of classified material to enemies of the United States. Manning gave classified military documents concerning the Iraq and Afghanistan wars to Julian Assange of the online confidential-document database Wikileaks, while Snowden disclosed to media outlets the operational details of the United States National Security Agency's (NSA) surveillance program.[3] In both cases, the secondary parties[4] circulated the classified information globally.[5]

During the military tribunal of Manning, military prosecutors argued that under § 904 Manning distributed confidential intelligence to sources he knew would publish the information worldwide.[6] Manning

---

1 10 U.S.C. §§ 877–920 (2012).

2 10 U.S.C. § 904 (2012).

3 Julie Tate, *Bradley Manning Declines to Enter Plea at Court-Martial*, WASH. POST, Feb. 23, 2012, http://www.washingtonpost.com/world/national-security/bradley-manning-declines-to-enter-plea-at-court-martial/2012/02/23/gIQAhLF6VR_story.html; Devin Barrett & Danny Yadron, *Contractor Says He Is Source of NSA Leak*, WALL ST. J., June 10, 2013, http://online.wsj.com/news/articles/SB10001424127887323495604578535653583992418.

4 *See infra* Part II.A (explaining the operational definition of "secondary parties").

5 James Ball, *NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts*, THE GUARDIAN, Oct. 24, 2013, http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

6 Eyder Peralta, *What the Manning Verdict Says About Edward Snowden's Future*, NPR: THE TWO-WAY (July 30, 2013, 5:28 PM), http://www.npr.org/blogs/thetwo-way/2013/07/30/207042272/what-the-manning-verdict-says-about-edward-snowdens-future.

thus implicitly knew the classified information would indirectly reach enemies of the United States because of its worldwide accessibility via the Internet.[7] Military prosecutors would likely make a similar argument regarding Snowden's release of confidential information to the *Washington Post*. Although their fact patterns satisfy the elements of § 904, Manning and Snowden's cases exemplify the constitutional defect of § 904 being a capital offense.

This Note argues that Congress employed an implicit statutory-aggravating circumstance in § 904 to limit the military commission's discretion in the eligibility phase of death sentencing.[8] The knowledge that information would reach the enemy, either directly or indirectly, historically narrowed the class of defendants who were eligible for execution under the UCMJ. The development of the Internet, however, divested the circumstance of its narrowing function. The Internet's open-source nature creates a presumption among Internet users that their transmissions are not privacy protected. People who post information to the Internet cannot reasonably assert that they believed their transmissions on the network were accessible exclusively to the transmitter and the recipient. Because Internet users know their online transmissions are globally accessible, they implicitly know that enemies of the United States have access to those transmissions. While an Internet user may not transmit information with the intent that the communications reach enemies, knowledge that an enemy will receive the information is sufficient for a defendant to be eligible for capital punishment under § 904.[9] Therefore, any person who transmits online information that a military commission construes as providing aid to the enemy meets the mental state of knowledge that historically has served as a narrowing circumstance, and that person may be eligible for execution.[10] This death-eligible class that § 904 produces—any Internet user who transmits confidential information—is impermissibly broad and provides for a high risk of arbitrary capital decision making by a military commission. Section 904's implicit aggravating circumstance does not produce a subclass of offenders who are particularly culpable, but instead affords the military commission unfettered discretion in deciding which Internet users are eligible for death. This unfettered discretion is what the Supreme Court in *Furman* explicitly deemed unconstitutional as an arbitrary and capricious exercise

---

[7] *Id.*

[8] 10 U.S.C. § 904 (2012).

[9] *Id.*

[10] Transmission includes not only the original uploading of the information to the Internet, but any reposting of illicit information previously uploaded because that repost heightens the visibility of the formerly confidential information.

of the death penalty.[11] The arbitrary and capricious nature of § 904's eligibility phase violates the Eighth Amendment and makes the statute constitutionally invalid.

This Note will begin with a preliminary section that: (1) addresses the scope and terminology of the Note; (2) provides a justification for reviewing § 904 in light of its legislative history; and (3) discusses the applicability of § 904 of the Uniform Code of Military Justice to civilians. Part I of this Note will provide an historical overview of Eighth Amendment jurisprudence with an emphasis on the function of circumstances that narrow the class of death-eligible defendants. Part II will examine the historical success of "knowledge of enemy receipt of information" as a narrowing circumstance in statutes that predated § 904. Part III will explain why the Internet stripped the "knowledge of enemy receipt" of its narrowing function through the Manning and Snowden cases. Part IV will conclude with prescriptions for amending § 904's implicit circumstance so that it genuinely narrows the class of death-eligible defendants.

PRELIMINARY OBSERVATIONS

A. Scope and Terminology of the Note

This Note isolates one constitutional field and addresses its impact on a capital punishment scheme; however, there are relevant issues that cannot be included within the Note for efficiency purposes. Two significant issues include: (1) the potential constitutional conflict between the First Amendment's protections of speech and a speech-based capital offense; and (2) the complexity of prosecuting a corporate entity for a capital crime. While these issues bear heavily on any valid review of § 904, there is insufficient space and time to give each of these topics the necessary analysis. To dispose of these concerns in an efficient manner, two operating conditions will be in place for this Note: (1) the transmitters are aware that the content is illegal and cannot rely on freedom of speech to exculpate them from liability; and (2) media corporations are persons liable for prosecution for a capital crime.

This Note will refer to Manning, Snowden, and any party who acquires the classified information from its original source as the "primary parties." The primary parties' defining feature is that they acquired the information from the original source and are the first party to break the confidentiality of the information. All other parties who acquire the in-

---

[11] *See* Furman v. Georgia, 408 U.S. 238, 256–57 (1972) (reversing a death sentence penalty and holding that the death sentencing process as applied was cruel and unusual punishment because the jury had unrestricted sentencing discretion that could result in arbitrary sentencing).

formation after the primary parties are "secondary parties." These secondary parties can acquire the information either directly from the primary party or from another secondary party. Examples of secondary parties include the media outlets who receive information and redistribute it on their forums and the Internet users who redistribute the information once the information is on the Internet. The designations of "primary" or "secondary" parties have no bearing on the parties' culpabilities.

B. Justifying Review of § 904 After the 2006 Amendment

Congress authorized § 904 in 1956.[12] Since its enactment, Congress amended the statute only once, in 2006, and in an area unrelated to the aggravating circumstance.[13] The continuity of the implicit aggravating circumstance indicates legislative confidence in § 904's ability to narrow the class of defendants eligible for the death penalty. The recentness of the review suggests there should be deference to Congress, and that the statute should not face the substantive scrutiny this Note purports to conduct.

The Supreme Court recognizes the decisions of legislatures as an "objective indicia that reflect[s] the public attitude toward a given sanction."[14] The Supreme Court has also ruled, however, that the Eighth Amendment's prohibition against cruel and unusual punishments cannot be "fastened to the obsolete."[15] Although legislative decisions on a capital punishment statute assure "obsolete" societal values do not justify the statute, congressional action or inaction does not insulate the statute from constitutional challenges not asserting an "evolving standards of decency" argument.[16] While legislative decisions codify contemporary moral values and communal standards of decency,[17] they are not dispositive for the type of procedural challenge advanced by this Note. This Note advances a procedural challenge based on the diminished functionality of an implicit aggravating circumstance, not an argument for a newfound moral repugnancy to the death penalty. Consequently, the recent legislative affirmation of § 904 does not preempt the type of review advanced by this Note.

---

12 10 U.S.C. § 904 (1956).

13 Military Commissions Act, Pub. L. No. 109-366, 120 Stat. 2600 (2006).

14 Gregg v. Georgia, 428 U.S. 153, 173 (1976).

15 Weems v. United States, 217 U.S. 349, 378 (1910).

16 *See* Trop v. Dulles, 356 U.S. 86, 101 (1958) (establishing the validity of a challenge to a capital punishment scheme due to the evolving standards of decency of a maturing society).

17 *See* McCleskey v. Kemp, 481 U.S. 279, 300 (1987) (explaining how legislative decisions are highly indicative of "contemporary standards").

C. *Application of § 904 of the Uniform Code of Military Justice to Civilians*

A final preliminary challenge to the type of review conducted in this Note is that the UCMJ does not apply to civilians, and consequently the concern about § 904 applying to an impermissibly broad class of defendants is preempted by its limited applicability to military personnel. This argument is supported by the definitional article of the UCMJ, which circumscribes the persons subject to the UCMJ chapter to an enumerated list of military personnel.[18]

Though this argument is valid for the majority of the punitive articles contained within the UCMJ, § 904's applicability is not limited just to "any person subject to this chapter," as in the majority of punitive articles.[19] Instead, § 904 reads "Any person who . . . shall suffer death," a textual deviation from the common pattern of the UCMJ written intentionally to broaden § 904's scope beyond military personnel.[20] Consequently, it cannot be said that the concerns of this Note are invalid because the UCMJ applies only to military personnel, as § 904 is in the unique position of being applicable to civilians, which is reflected in the text of the Note.

I. HISTORIC EIGHTH AMENDMENT AND NARROWING JURISPRUDENCE RELEVANT TO § 904

The Eighth Amendment prohibits the infliction of "cruel and unusual punishments."[21] Through its jurisprudence, the Supreme Court defined when a statutory scheme's implementation of the death penalty is "cruel and unusual" and legitimized statutory mechanisms that can make capital schemes comport with the Eighth Amendment.[22]

In *Furman v. Georgia*, Justice Brennan noted that "cruel and unusual" is "not susceptible to precise definition."[23] Indicative of the difficulty of defining "cruel and unusual punishment" is that no unified opinion emerged from *Furman*.[24] Although the Justices did not decide if the death penalty is per se cruel and unusual, the case established that when a jury's discretion is unfettered, the risk of the arbitrary imposition of the death penalty is too high, making the death penalty cruel and unu-

---

18 10 U.S.C. § 802 (2012).

19 *See, e.g.*, 10 U.S.C. § 881 (2012) ("Any person subject to this chapter"); 10 U.S.C. § 885 (2012) ("Any member of the armed forces").

20 10 U.S.C. § 904 (2012).

21 U.S. CONST. amend. VIII.

22 *See, e.g.*, Furman v. Georgia, 408 U.S. 238 (1972) (per curiam) (finding that the imposition of the death penalty by courts in Georgia and Texas violated the Eighth Amendment).

23 *Id.* at 258 (1972) (Brennan, J., concurring).

24 *See id.* at 240 (noting the multiple concurrences and dissents).

sual.[25] Each Justice provided his own rationale for the Eighth Amendment's prohibition of the arbitrary infliction of the death sentence. Justice Douglas cited the substantial risk of discrimination that accompanies a jury's unfettered discretion in death penalty decisions, concluding that the arbitrary infliction of the death penalty violates the "equal protection [that] is implicit in 'cruel and unusual' punishments."[26] Justice Brennan condemned unfettered jury discretion for its disproportionate punishments, which is "[dis]respect[ful] [to] human dignity when, without reason, [the State] inflicts upon some people a severe punishment that it does not inflict upon others."[27] The other Justices presented comparatively conservative rationales based on the general principles of criminal law (i.e. retribution, deterrence).[28] Even though the Justices' rationales diverged, the Justices reached a consensus that when the sentencing authority has unfettered discretion, the risk of arbitrary sentencing is too high making the death sentence cruel and unusual punishment.[29]

The *July 2 Cases*,[30] led by *Gregg v. Georgia*, channeled the concurrences of the *Furman* opinion to provide guidance to state legislatures attempting to retain their death penalty schemes.[31] The *Gregg* court approved a capital sentencing procedure that required the jury to "find and identify at least one statutory aggravating factor before it may impose a

---

25 *See id.* at 282 (Brennan, J., concurring) ("If a punishment is unusually severe, if there is a strong probability that it is inflicted arbitrarily . . . then the continued infliction of that punishment violates the command of the Clause that the State may not inflict inhuman and uncivilized punishment."). *See also id.* at 294–95 ("[O]ur procedures in death cases, rather than resulting in the selection of 'extreme' cases for this punishment, actually sanction an arbitrary selection. For this Court has held that juries . . . make the decision whether to impose a death sentence wholly unguided by standards governing that decision."); *id.* at 310 (Stewart, J., concurring) ("[T]he Eighth and Fourteenth Amendments cannot tolerate the infliction of a sentence of death under legal systems that permit this unique penalty to be so wantonly and freakishly imposed."); *id.* at 398 (Burger, C.J., dissenting) ("It is concluded that petitioners' sentences must be set aside not because the punishment is impermissibly cruel, but because juries and judges have failed to exercise their sentencing discretion in acceptable fashion.").

26 *Id.* at 249 (Douglas, J., concurring).

27 *Id.* at 274 (Brennan, J., concurring).

28 *See, e.g.*, *id.* at 311–12 (White, J., concurring) ("But when the imposition of the penalty reaches a certain degree of infrequency, it would be very doubtful that any existing need for retribution would be measurably satisfied . . . . Most important, a major goal of the criminal law—to deter others by punishing the convicted criminal—would not be substantially served.").

29 *See supra* note 25.

30 The *July 2 Cases* were a series of Supreme Court decisions, the most prominent being Gregg v. Georgia, 482 U.S. 153 (1976), that reaffirmed the United States' use of the death penalty is not per se cruel and unusual punishment in violation of the Eighth Amendment. The cases provided the state legislatures with guidance as to the capital sentencing procedures that ensure the death penalty is not administered in a cruel and unusual fashion. The Supreme Court identified two main features: (1) sentencing standards that limit the sentencing discretion of the jury; and (2) meaningful appellate review of a death sentence.

31 *See Gregg*, 428 U.S. at 196–97.

penalty of death."[32] In the opinion, the *Gregg* court approved the aggravating factors scheme because it channeled the sentencing authority's discretion thereby "minimiz[ing] the risk of wholly arbitrary and capricious action."[33] The *Gregg* court found that the statutory aggravating factors scheme directed discretion by "narrow[ing] the class of murderers subject to capital punishment."[34] Thus, *Gregg* developed Eighth Amendment jurisprudence in two ways. First, *Gregg* reified the anti-arbitrariness requirement of *Furman*.[35] Second, *Gregg* incorporated aggravating circumstances as a legal mechanism that channels the sentencing authority's discretion by narrowing the class of defendants eligible for the death sentence, thereby making the capital scheme not wholly arbitrary or capricious.[36]

Zant v. Stephens built upon *Gregg* by explicitly clarifying why statutory aggravating circumstances reduce the risk of arbitrary and capricious sentencing.[37] In *Zant*, the Georgia Supreme Court described capital sentencing schemes as a pyramid.[38] The base level of the pyramid contains all defendants who committed homicides.[39] At the apex of the period are the defendants that are culpable enough to warrant a death penalty.[40] To reach the apex, defendants must pass through three thresholds that channel the jury's discretion by requiring the jury to find that the condition associated with each threshold existed in a particular defendant's case.[41] Statutory aggravating circumstances constitute one of these intermediary planes. The statutory aggravating circumstances plane "separates from all murder cases those in which the penalty of death is possible."[42] Statutory aggravating circumstances fulfill a "constitutionally necessary function . . . they circumscribe the class of persons eligible for the death penalty,"[43] adequately channeling the jury's discretion because it cannot impose the death penalty on every defendant

---

32 *Id.* at 206.

33 *Id.* at 189. While the *Gregg* court retained the essential components of the arbitrariness standard established in *Furman*, *Gregg* increased the burden on the defendant to invalidate a death penalty scheme on the grounds of arbitrariness. Instead of having to show that a scheme allows discretion to the extent that decisions are arbitrary, the defendant must now show that the scheme presents a situation of "wholly arbitrary and capricious action." *Id.*

34 *Id.* at 196.

35 *Id.* at 189 (rearticulating the unconstitutionality of an arbitrary decision making process in a capital punishment case).

36 *Id.* at 196–98.

37 Zant v. Stephens, 462 U.S. 862, 874–75 (1982) (dealing with a homicide capital sentencing scheme, and the statutory aggravating circumstances principle stated in the case applies to any capital sentencing scheme).

38 *Id.* at 870.

39 *Id.* at 871.

40 *Id.*

41 *Id.* at 870–71.

42 *Id.* at 871.

43 *Id.* at 878.

charged with a capital crime. Only statutory aggravating circumstances that genuinely narrow the class of persons eligible for the death penalty and reasonably justify the imposition of a more severe sentence on the defendant compared to others found guilty of a similar crime channel the jury's discretion and prevent arbitrary sentencing.[44]

Gregg and *Zant* developed the role of statutory-aggravating-circumstances schemes where the circumstances were distinct from the elements of the underlying crime. *Lowenfield v. Phelps* answered the question of whether the statutory aggravating circumstance can be an element of the underlying capital offense.[45] The *Lowenfield* court held that a death sentence does not violate the Eighth Amendment when the statutory aggravating circumstance that serves as the basis for a defendant's death eligibility is duplicative of an element of an underlying specific-intent offense.[46] Chief Justice Rehnquist wrote that "the use of 'aggravating circumstances' is not an end in itself, but a means of genuinely narrowing the class of death-eligible persons, and thereby channeling the jury's discretion."[47] With a specific-intent offense, the legislature consolidates the guilt and eligibility phases by requiring the jury to find a statutory aggravating circumstance as part of the finding of guilt.[48] The legislature "narrow[s] the definition of capital offenses . . . so that the jury finding of guilt responds to this [narrowing] concern."[49] In essence, the *Lowenfield* court held that in making a guilt determination, the jury is conducting the same statutory aggravating circumstance analysis and reaching the same conclusion as if a separate eligibility phase was conducted.[50]

Thus, Eighth Amendment jurisprudence on narrowing stands as follows: statutory aggravating circumstance can be part of the elements of a specific-intent offense as long as the statutory aggravating circumstance genuinely narrows the class of defendants eligible for the death penalty. Through aggravating circumstances, the jury does not have unfettered discretion. The jury is given a meaningful basis for differentiating death culpable defendants from the non-eligible and the capital punishment scheme is not arbitrary, nor a violation of the Eighth Amendment.

---

44 *Id.* at 877.
45 *See* Lowenfield v. Phelps, 484 U.S. 231, 236 (1988).
46 *Id.* at 246.
47 *Id.* at 244.
48 *Id.* at 246.
49 *Id.*
50 *Id.* at 244–46.

II. THE SUCCESS OF "KNOWLEDGE OF ENEMY RECEIPT" AS AN AGGRAVATING CIRCUMSTANCE BEFORE THE DEVELOPMENT OF THE INTERNET

A. The Legislature Establishes a Reasonable Expectation of Communicational Privacy in Pre-Internet Communication Systems

Prior to the advent of the Internet, the mediums for transmitting information were accompanied by a reasonable right to privacy.[51]

Although the right to privacy is not an explicit protection listed in the Bill of Rights, the United States Supreme Court found the right exists in the "penumbras" of the explicitly listed constitutional rights.[52] Of these explicit constitutional rights, the Fourth Amendment supplies the strongest foundation for a right to communicational privacy. The Fourth Amendment provides that the people of the United States possess a right to be "secure in their persons, house, *papers*, and *effects*, against unreasonable searches and seizures."[53] Individuals are entitled to this protection as long as: (1) society recognizes the expectation of privacy as a reasonable one; and (2) the individual exhibits an actual expectation of privacy.[54]

Society's recognition of privacy in pre-Internet communication technologies is evidenced by Congress's legislation of communications mediums.[55] Congress began recognizing the reasonableness of an expectation of privacy with the Communications Act of 1934.[56] The Communications Act established the Federal Communications Commission (FCC) and conferred to the FCC the power to "regulate interstate and foreign commerce in communication by wire and radio so as to make available . . . communication service[s]."[57] The Supreme Court, in interpreting the Communications Act of 1934, held that the privacy right enshrined in the Act derived from the Fourth Amendment, and that the "Fourth Amendment is a constraint on government action rather than on the actions of private individuals."[58] Consequently, the Act criminalized

---

51 S*ee, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); California v. Ciraolo, 476 U.S. 207, 214 (1986) ("Justice Harlan made it crystal clear that he was resting on the reality that one who enters a telephone booth is entitled to assume that his conversation is not being intercepted."); *Ex Parte* Jackson, 96 U.S. 727 (1887) (holding that regulations made for handling letters in transit cannot overcome the Fourth Amendment right to freedom from unreasonable search and seizure).

52 Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

53 U.S. CONST. amend. IV (emphasis added).

54 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

55 In the same way Congress is a benchmark for society's standards of decency, congressional action is the most visible indicator of what society defines as reasonable.

56 47 U.S.C. §§ 151–155 (1934).

57 47 U.S.C. § 151.

58 United States v. Goldstein, 532 F.2d 1305, 1311 (9th Cir. 1976).

government officials' unauthorized wiretapping while leaving private action unaffected.

It was not until 1968 that Congress broadened the right to privacy to encompass protections from private party interception. In response to the vigilantism of both government and private actors seeking to combat domestic Communism through illegal wiretapping,[59] Congress passed the Omnibus Crime Control and Safe Streets Act of 1968 (Omnibus Act).[60] The Omnibus Act prohibited the unauthorized, nonconsensual interception and publication of "wire, oral, or electronic communications" by government and private parties.[61] The Omnibus Act also established procedures for obtaining warrants to authorize wiretapping by government officials and promulgated regulation for the disclosure and use of authorized intercepted communications.[62]

State statutory law has supplemented the Omnibus Act with the enactment of "eavesdropping statutes" designed to prevent the overhearing, recording, amplifying, or transmission of the communications of others without the consent of at least one of the parties engaged in the communication.[63] Every state has adopted these eavesdropping statutes, with variations amongst the states over the consent requirements for recording a conversation.[64] The majority of states have adopted a single-party consent model, wherein only one of the parties to the communication needs to waive the right to privacy.[65] A typical single-party consent model can be found in the Texas Penal Code, which lists as an affirmative defense to unlawful wiretapping a scenario where "one of the parties to the communication has given prior consent to the interception."[66]

The history of the statutes that precede the Internet, both on the federal and state levels, shows an increased recognition of the reasonableness of the expectation of privacy. In 1934 Congress, as a conduit for society, only recognized an expectation of privacy from the government as reasonable.[67] In 1968, the reasonable expectation of privacy extended to freedom from private party interception with the Omnibus Act.[68]

---

59 *See Katz*, 389 U.S. 347 (exemplifying the police overreach that resulted in the Omnibus Act); Berger v. New York, 388 U.S. 41 (1967).

60 18 U.S.C. §§ 2510–2522 (1968).

61 18 U.S.C. §§ 2511–2515.

62 18 U.S.C. §§ 2516–2519.

63 Travis Triano, *Who Watches the Watchmen? Big Brother's Use of Wiretap Statutes to Place Civilians in Timeout*, 34 CARDOZO L. REV. 389, 416 (2012).

64 *See*, *e.g.*, Cal. Penal. Code § 631(a) (All-party consent); N.Y. Penal Law § 250.00 (One-party consent).

65 Caycee Hampton, *Bilateral Consent Wiretap Statutes: Inviting Police Intimidation*, 49 CRIM. L. BULL. 504, 511 (2013).

66 4 TEX. PENAL CODE §16.02(c)(3)(A).

67 *See* 47 U.S.C. § 605 (1940).

68 *See* Pub. L. No. 90-351, 82 Stat. 213 (codified as amended at 18 U.S.C. §§ 2511–2515 (2012)); United States v. Goldstein, 532 F.2d 1305, 1311 (9th Cir. 1976).

Consequently, until the development of the Internet, the controlling principle was that society recognizes a right to privacy in communications where both parties maintain the privacy agreement and each individual actually believes their communications are protected. This right, derived from the Fourth Amendment protections from unreasonable search and seizure, protected parties from unauthorized third-party interception and access to the privileged communications.

B. The Reasonable Right to Communicational Privacy Enables Aggravating Circumstances to Genuinely Narrow Offenders to Produce a Death-Eligible Class

The reasonable expectation of privacy in pre-Internet technologies established relational parameters in transmissions, bounding transmitters to a tacit communicational privacy agreement.[69] The bounding of the communication transaction limited death eligibility to a discrete and easily identifiable class of defendants that either actively violated the privacy agreement or transacted directly with enemies of the United States.

The tacit privacy agreement made the illegal distribution of information an active offense rather than a passive consequence of transmission. Parties engaging in transmission through pre-Internet communications systems reasonably believed that the content of their transmissions would remain confidential.[70] This reasonable belief bars liability in the event a third party uses the information for injurious purposes because the transmitting party would not possess the mental state required by the information crimes statutes.[71] In transmitting, the parties were not by default operating with the knowledge that enemies of the United States would have access to the communication.[72] The prosecution could not rely on a theory of passive and indirect information sharing to prove the defendant had a culpable mental state. Consequently, mere transmitters and users of technology without injurious purposes were immune from death eligibility. Only two discrete classes of individuals are death eligible: (1) transmitters who acted contrary to the privacy agreement and deliberately disseminated the information to third parties that intended to use the information to harm the United States;

---

69 *See* Matt Greenberg, Case Note, *Law Enforcement Officers with Clean Hands May Not Make Investigative Use of a Wiretap that Was Illegally Acquired by a Third Party:* Berry v. Funk, *14 F.3d 1003 (D.C. Cir. 1998)*, 68 U. CIN. L. REV. 463, 492 (2000).

70 *See* Katz v. United States 389 U.S. 347, 352 (1967) (Harlan, J., concurring) ("One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

71 *See* Hampton, *supra* note 65, at 3.

72 This assumes that the party did not transmit the information firsthand to a party who the transmitting party has reason to believe would use the information in a manner injurious to the United States.

and (2) individuals who transmit information directly to enemies of the United States. The former death-eligible class is comprised of transmitters who actively consented to disclosure of information to these injurious third parties or were third parties who violated the privacy agreement by intercepting privacy-protected communications. Third party or primary party, this first class of individuals willfully broke a tacit privacy agreement to share information with enemies of the United States. Parties who deliberately chose to directly engage in information transactions with enemies compose the latter class. With both classes of death-eligible defendants, the defendant needed to actively distribute the information to known enemies of the United States.

Thus, the right to privacy inherent to pre-Internet technologies produced discrete and identifiable classes of death-eligible defendants by making the worst offenders easily identifiable because of either their active violation of a tacit privacy agreement or their direct transacting with enemies of the United States.

C. An Example of the Reasonable Expectation of Communicational Privacy's Effect on Narrowing Circumstances: The Espionage Act of 1917 and the Rosenberg Trial

Congress enacted the Espionage Act of 1917 with the same rationale it would use to ratify § 904 as part of the UCMJ.[73] The Espionage Act's purpose was to "punish acts of interference with the foreign relations, and the foreign commerce of the United States, to punish espionage," and to hold individuals who commit acts injurious to the United States criminally liable.[74] The Espionage Act's capital punishment section, "Gathering or Delivering Defense Information to Aid Foreign Government," prohibits the wartime transmission of information to foreign governments that the transmitter has reason to believe will use the information to injure the United States.[75] This section employs a statutory aggravating factor similar to § 904's implicit aggravating factor; the person transmitting the information must have "intent or reason to believe that it is used to the injury of the United States."[76] It was under the "Gathering or Delivering Defense Information to Aid Foreign Govern-

---

[73] 18 U.S.C. §§ 792–799 (2012). Congress ratified § 904 before the Internet, but in the period between the ratification of the statute and the creation of the Internet there were no prosecutions under the statute. To observe how capital prosecutions for non-homicide related crimes functioned prior to the Internet, it is necessary to use prosecutions under a historical corollary of § 904. Accordingly, the Espionage Act of 1917 and prosecutions under the Act will be the substitute for § 904 in the period preceding the Internet.

[74] Espionage Act of 1917, Pub. L. No. 24, 40 Stat. 217 (1917).

[75] 18 U.S.C. § 794 (2012).

[76] *Id.*

ment" section, subject to the implicit statutory aggravating factor, that the United States prosecuted and executed Julius and Ethel Rosenberg.

The United States government alleged that the Rosenbergs transmitted confidential information about the atomic bomb to the Soviet Union.[77] The primary witness was Ethel Rosenberg's brother, David Greenglass.[78] Greenglass was an army employee at Los Alamos laboratory in New Mexico when the Rosenbergs recruited him to aid in their espionage activities.[79] The Rosenbergs controlled the actions of Greenglass, acting in a principal and agent relationship. During his time at Los Alamos, Greenglass utilized his position as a sergeant with the United States Army to engage nuclear scientists about the details of the Manhattan Project.[80] At trial, Greenglass testified that he provided Ethel with schematics of the atomic bombs from the Los Alamos nuclear plant.[81] Ethel then transcribed the notes containing U.S. nuclear secrets and provided them to her husband Julius, who maintained direct contact with agents from the Ministry for State Security of the Soviet Union.[82] In addition to his role as a courier, Julius Rosenberg acted as a recruiter for the Soviets in the United States by funding college students with Soviet money to establish contacts in the American intelligence network and among the universities of the United States.[83]

The Rosenberg case is helpful because it is illustrative of both classes of defendants eligible for the death sentence when a reasonable right to privacy existed in communication systems.

The communications between Greenglass and those nuclear scientists, which took place primarily through telephone conversations and written company memos, retained a reasonable right to privacy on behalf of the scientists.[84] The scientists were insulated from liability because society recognized the right to privacy that adhered to the communications between themselves and Greenglass, and the scientists exhibited an actual belief that their transmissions were privacy protected. The scientists distributed details of the nuclear program to Greenglass in a profes-

---

77 United States v. Rosenberg, 195 F.2d 583, 588 (2d Cir. 1952).

78 The Associated Press, *David Greenglass, Spy Who Sent Sister Ethel Rosenberg to Electric Chair, Dies*, THE GUARDIAN, Oct. 14, 2014, http://www.theguardian.com/world/2014/oct/15/david-greenglass-spy-who-sent-sister-ethel-rosenberg-to-electric-chair-dies.

79 Note, *The Rosenberg Case: Some Reflections on Federal Criminal Law*, 54 COLUM. L. REV. 219, 220 (1954).

80 Paul Valentine, *David Greenglass, Central Figure in Cold War Atomic Spy Case, Dies at 92*, WASH. POST, Oct. 14, 2014, http://www.washingtonpost.com/national/david-greenglass-central-figure-in-cold-war-atomic-spy-case-dies-at-92/2014/10/14/6339be3e-5094-11e4-8c24-487e92bc997b_story.html.

81 *Rosenberg*, 195 F.2d at 589.

82 *Id.*

83 *Id.*

84 Valentine, *supra* note 80.

sional context under the presumption that he had authorization and legitimate purposes, and that the information would not be accessible by third parties with injurious designs.[85] No interpretation of the communication transactions had the scientists actively violating the privacy agreement, nor giving consent to distribute the information to a third party. The scientists had no "reason to believe that [the information] would be used to injure the United States."[86] Thus, a reasonable expectation of communicational privacy exculpated the scientists through a categorical undermining of the *mens rea* requirement of the Espionage Act's capital punishment section. This result is consistent with the aims of the Eighth Amendment's prohibition of arbitrary and capricious imposition of the death penalty, as the nuclear scientists in the Rosenberg trial were the least culpable of all the actors.[87] Neither by design, nor by negligence did the nuclear scientists involve themselves in the conspiracy to provide aid to the Soviet Union, making it cruel and unusual to impose any legal punishment on them, least of all capital punishment.

In contrast to the scientists, Greenglass entered into his relationship with the scientists with the intention of violating the privacy agreement.[88] He was the first class of death-eligible offender: a transmitter who acted contrary to the privacy agreement and deliberately disseminated the information to third parties that intended to use the information to harm the United States. Greenglass entered into a tacit privacy agreement with the scientists then willfully broke the agreement to transmit the information with the Rosenbergs for compensation. Greenglass knew the money was coming from the Soviet Union and that the information he was sharing would undermine the United States' strength during the Cold War. Greenglass affirmatively waived the right to a bound transaction by sharing with the Rosenbergs the schematics of the nuclear weapons and the content of the conversations conducted between himself and the nuclear scientists. It is the action of sharing with the Rosenbergs, and not partaking in the original conversations with the scientists, which implicates Greenglass as the active violator of the reasonable expectation of privacy. Unlike the scientists, Greenglass could not appeal to the right to privacy to undermine his *mens rea* because it was his decisions to waive the right. Consequently, Greenglass was death eligible as an active violator of the tacit privacy agreement he entered into. Greenglass's eligibility is not an arbitrary result, but instead is consistent with his culpability. Unlike the nuclear scientists, Greenglass was an active participant in espionage that injured the United States. In the relationship

---

85 *Id.*

86 18 U.S.C. § 794 (2012).

87 U.S. CONST. amend. VIII.

88 Valentine, *supra* note 80.

between Greenglass and the scientists, the narrowing function produced a result that was neither arbitrary, nor capricious.

The Rosenbergs were eligible for the death penalty as the second class of offenders: individuals who transmit directly to enemies of the United States. The Rosenbergs did not break a tacit privacy agreement like Greenglass. Instead, the Rosenbergs passed along state secrets to Soviet agents they knew to be enemies of the United States. The Soviet Union's status as an enemy to the United States was uncontroversial; therefore, unlike Greenglass's dealings with the nuclear scientists, it was the original conversation with the Soviet agents and not the breaking of any privacy agreement that made the Rosenbergs death eligible. The existence of a reasonable right to communicational privacy did not affect the Rosenbergs' death eligibility It did, however, affect the prosecutor's decision to seek execution for the Rosenbergs and not for Greenglass, thereby channeling prosecutorial discretion and ensuring that the prosecutor's decision of when to seek the death penalty was not arbitrary or capricious.

In corroboration with a Soviet handler named Anatoliy Yatskov, the Rosenbergs recruited Greenglass and his wife into the Soviet spy network and used Greenglass's authority to access nuclear secrets.[89] Although the prosecution was able to implicate Greenglass as the information leak, it could only establish minimal contacts between Greenglass and agents of the Soviet Union.[90] This was because the active violation of the privacy agreement between Greenglass and the nuclear scientists only implicated Greenglass as a participant in the conspiracy, but did not establish his role. It was the reasonable expectation of privacy that adhered to the transmissions between the Rosenbergs and the Soviet agents that assigned roles and associated culpabilities to the Rosenbergs and Greenglass. The Rosenbergs did not violate a privacy agreement to make them death eligible, but instead transacted with people they knew to be enemies of the United States. Ironically, throughout the conspiracy the Rosenbergs maintained the privacy agreement guaranteed by a reasonable right to privacy. The information chain between the Soviet agents and Greenglass went one direction: from Greenglass, to the Rosenbergs, and then to the Soviet agents. The lack of reverse communication made the roles clear: Greenglass's was an "agent" of the Rosenbergs, who acted as "principals" responsible for procuring and transmitting the nuclear information to the Soviet Union. The prosecution's assignment of culpability was consistent with these roles. The prosecution, based on the information chain that stemmed from the breaches, concluded that the Rosenbergs were the most culpable offend-

89 *See* United States. v. Rosenberg, 195 F.2d 583, 588–89 (2d Cir. 1952).
90 *Id.* at 527.

ers while Greenglass was merely a cog in that network that did not warrant capital punishment. As the principals, the prosecution charged the Rosenbergs with the capital offense while the prosecution pled out Greenglass.[91] Thus, the reasonable expectation of communicational privacy produced privacy agreements, which allowed for the meaningful differentiation of death-eligible defendants, thereby ameliorating any concerns of arbitrariness in the Rosenberg case.

D. Conclusion from the Pre-Internet Era of Communications Technology

Both federal and state legislatures established a reasonable expectation of privacy for pre-Internet communications technologies. This reasonable expectation of privacy enables aggravating factors to genuinely narrow the class of defendants to a non-arbitrary death-eligible group by binding transmitters to a tacit privacy agreement that must be actively violated for culpability to adhere. Those active violators of the privacy agreement are the worst offenders who knowingly shared information with an enemy of the United States. There is a meaningful basis for distinguishing death-eligible defendants, meaning that the death penalty under these schemes was not cruel and unusual punishment.

III. THE IMPACT OF NO REASONABLE EXPECTATION OF PRIVACY FOR INTERNET USERS ON THE "KNOWLEDGE OF ENEMY RECEIPT" CIRCUMSTANCE IN § 904

A. Jurisprudence Asserting No Reasonable Expectation of Communicational Privacy for Internet Transmissions

Although the legislature was central in establishing a reasonable expectation of privacy in pre-Internet communications systems, the judiciary has been the institution to issue a policy dealing with a reasonable expectation of communicational privacy over the Internet through its recent jurisprudence.

Courts have consistently held that unlike prior information-transmitting technologies, the Internet does not retain the same reasonable expectation of privacy particularly when those transmissions occur through web site postings.[92] The Southern District of New York most recently codified this principle in the *Meregildo* case.[93] In *Meregildo*, the defendant was a gang member who not only posted evidence of his thefts and assaults on his Facebook page, but also maintained a running account of

---

[91] *Id.* at 588.
[92] *See, e.g.*, United States v. Meregildo, 883 F. Supp. 2d 523 (S.D.N.Y. 2012).
[93] *Id.*

crimes he committed and future crimes he intended to commit.[94] When the police discovered the evidence on the defendant's Facebook page and found through his posting history that he had detailed the alleged crimes with specificity, they obtained a warrant and arrested the defendant.[95] The prosecution charged the defendant with racketeering, assault, and grand larceny with probable cause entirely predicated on the information from the Facebook page.[96] The defendant argued that the invasion of his social networking page to secure a warrant for arrest violated the defendant's Fourth Amendment right to freedom from unreasonable search and seizure. The defendant posited that he had a reasonable expectation of privacy for the content on his Facebook page because the accessibility of the content on his personal page was restricted exclusively to his Facebook friends, associates who the defendant had consented to sharing his content with.[97] The defendant concluded that only he could waive his privacy right by consenting to a search of the information on his Facebook page by the police, and that he had never consented to the search that produced the evidence against him.[98]

The court disposed of the defendant's claim in two ways. First, operating under the presumption that a privacy right could exist for Internet communications, the court held that the power to waive the reasonable expectation did not vest solely with the Facebook user.[99] According to the court, a cooperating witness who is a "friend" could consent to a waiver of the right to privacy on behalf of the Facebook poster without violating the Fourth Amendment.[100] The friend can consent to the waiver of the right to privacy because the friend, upon delivery of information through the Internet, has discretion to utilize the delivered information in any way he conceives.[101] The friend possesses this discretion with the material of the Facebook user because the Facebook user has consented to an online relationship in which the recipient has freedom of informational use through the acceptance of the friend request that vests informational power in the online friend.[102]

The *Meregildo* court then dealt with the expectation of privacy and its relation to social networking, web site postings, and Internet transmission. The court reasoned that a reasonable expectation of privacy adheres to content stored on a home computer, but when the content is

94 *Id.* at 525–26.
95 *Id.*
96 *Id.* at 524.
97 *Id.* at 525.
98 *Id.* at 526.
99 *Id.*
100 *Id.*
101 *Id.*
102 *Id.*

transmitted the reasonableness of the expectation of privacy might extinguish, particularly in the context of a social networking website.[103] The *Meregildo* court reached this conclusion on social networking for reasons similar to those elucidated in a case that preceded *Meregildo* by two years, *Romano v. Steelcase, Inc.*[104] *Romano* held that the very nature and purpose of social networking sites, public Internet webpages, and blogs were to share personal postings with others.[105] According to *Romano*, users of these technologies engage them because of the "knowledge" that the information becomes publicly available through transmissions and that if this were not true, social networking would cease to exist.[106] The effect of *Romano* is that parties transmitting information over the Internet do not carry a right to privacy that can insulate a defendant from search and seizure or undermine the *mens rea* requirements of capital punishment statutes for information crimes. The reasonable expectation of privacy of pre-Internet technologies is not translatable to the Internet because the Internet is an open-source medium created with the purpose of complete global connectivity.[107] As the *Meregildo* court reasoned, while an Internet user may honestly believe that their profiles and the information on those profiles are private to the Facebook user and his Facebook friends, this is not a reasonable expectation because the Internet has expanded the circle of "friends" that can access transmitted information to viewers including "someone . . . never expected to see them."[108] The default standard for hosting and transmitting information over the Internet is that the user "[surrenders] his expectation of privacy . . . by [sharing] those posts with his 'friends' at his peril."[109] The "peril" the *Meregildo* court is referencing is the dissemination of the user's information to parties that the original user could not have foreseen.

In conclusion, *Meregildo* and *Romano* collectively embody the principle that because Internet websites are transmission forums premised on information connectivity, it is not reasonable for an Internet user to attempt to limit their liability by asserting that a privacy right exists.[110] Users engage websites with the purpose of mass distribution of their personal information. Consequently, the default condition for Internet users

---

103 *Id.* at 525–26.

104 Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010).

105 *See id.* at 656–57.

106 *Id.*

107 *Id.* ("'Users would logically lack a legitimate expectation of privacy in materials intended for publication or public posting.'" (quoting United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004))).

108 *Meregildo*, 883 F. Supp. 2d at 526.

109 *Id.*

110 *See id.*; *Romano*, 907 N.Y.S. 2d at 656.

must be that a reasonable expectation of privacy does not exist when they transmit and host information on a website.

B. The Impact of the Loss of a Reasonable Expectation of Communicational Privacy on § 904: Undermining "Knowledge of Enemy Receipt"

The reasonable expectation of privacy in transmissions prior to the Internet enabled the "knowledge of enemy receipt" circumstance to perform its narrowing function to prevent arbitrary death sentencing by establishing tacit privacy agreements between transmitting parties that needed to be actively violated in order for a defendant to be death eligible. The need for a defendant to actively violate a privacy agreement provided a meaningful basis for differentiating the most culpable defendants from those who did not deserve to be death eligible; therefore, death penalties administered for information crimes prior to the Internet were not cruel and unusual and did not violate the Eighth Amendment.

Section 904 has an implicit aggravating circumstance—knowledge of enemy receipt of the information—which is similar to the implicit circumstance of the Espionage Act. To comport with the Eighth Amendment, this implicit statutory aggravating circumstance must genuinely narrow the class of death-eligible defendants to a discrete and identifiable group of offenders who are sufficiently culpable to warrant execution. Yet because of the judicial precedent that has determined there is no reasonable expectation of communicational privacy over the Internet, the circumstance does not genuinely narrow offenders eligible for death, but leaves the sentencing authority to exercise unfettered discretion in determining which defendants should receive the death sentence.

Romano held that a right to privacy did not adhere to Internet transmissions because the purpose of a website and the Internet writ large is to allow users to disseminate their information on a global scale.[111] The case established that the default mental state for users of the Internet is not the same as pre-Internet technologies.[112] Internet users cannot reasonably expect their information transmissions to be private, but instead operate with the knowledge that the Internet inherently makes their transmissions accessible to unintended third parties, including enemies of the United States. This bears on § 904 because the implicit aggravating circumstance of knowledge of receipt by an enemy is satisfied by all Internet transmitters, who according to *Romano* are knowledgeable about the potential accessibility of their transmissions by unforeseen parties worldwide, including enemies of the United States.[113] No longer must

---

111 *Romano*, 907 N.Y.S. 2d at 656.
112 *Id.* at 657.
113 *Id.*

there be an active violation of a privacy agreement for a defendant to be death eligible. Instead, death eligibility under § 904 is a passive consequence of transmitting information over the Internet. Consequently, § 904's statutory aggravating circumstance does not provide a meaningful basis for establishing a discrete and identifiable death-eligible class, but instead affords the sentencing authority unfettered discretion to decide who should be death eligible from an impermissibly broad class of all Internet users who transmit information that can be construed as beneficial to an enemy of the United States. "Knowledge of enemy receipt" does not genuinely narrow the class of defendants eligible for death, but instead produces the unconstitutionally high risk of arbitrary decision that *Furman* held to be a violation of the Eighth Amendment.

C. Exemplifying the Constitutional Infirmities of § 904 Through Edward Snowden

Both Manning's and Snowden's cases implicate the constitutional infirmities of § 904 by designating both individuals death eligible without a substantive distinction between them and the other actors who partook in the release of classified information to enemies of the United States.

The theories of death eligibility for both Manning and Snowden under § 904 would be that the two released information to media outlets that posted the information directly to the Internet with the knowledge that the information would indirectly reach Al Qaeda.[114] The prosecution would rely on the lack of a right to privacy to prove the *mens rea* of the statutory aggravating circumstance, arguing that by giving the information to entities with global distribution networks on the Internet, Snowden and Manning possessed the requisite knowledge that enemies would receive the confidential information.[115] The requisite *mens rea* and the classified nature of the information established, the prosecution would conclude that Snowden and Manning are death eligible.[116] With Snowden and Manning, the purported narrowing would occur through showing that the defendants knew enemies of the United States would receive the information. This line of argument is problematic, however, because the same prosecutorial logic would hold the media outlets and the Internet users death eligible as well.

Isolating the Snowden case, Edward Snowden, the primary party, transmitted the operational details of the NSA to the *Washington Post*, the secondary party. Prior to his contact with the *Washington Post*, Snowden had not disclosed the confidential information on the Internet

---

114 Peralta, *supra* note 6.
115 10 U.S.C. § 904 (2012).
116 Peralta, *supra* note 6.

or to any other media outlet.[117] Snowden had stolen the NSA operational manual, but his resources limited the impact of disclosure.[118] Only Snowden knew the contents of the operational manual of the NSA, and he had little circulatory power until he joined with the *Washington Post*. Snowden gave the classified information to the *Washington Post*.[119] With knowledge that Snowden acquired the information without proper authorization, and with a network that extends across the globe, the newspaper published the information both in print and online.[120] Through publication on the Internet, the *Washington Post* knew that the information would reach enemies of the United States and would materially benefit those enemies.[121] Thus, the newspaper qualifies as death eligible under § 904 as it fulfills the statutory aggravating circumstance implicit to the statute; however, the newspaper is not subject to prosecution.[122] This is problematic because it is a viable argument that the *Washington Post* is "worst of the worst" in this information conspiracy.

There are three reasons why the *Washington Post* is arguably the most culpable actor in the Snowden scenario: legitimation, distribution, and profit. Without the *Washington Post*, the impact of Snowden's disclosure as an individual would have relied upon his own credibility. When the *Washington Post* offered to publish the confidential information, it immediately validated Snowden's information and provided him with the global network to heighten drastically the visibility of the unauthorized disclosure. Furthermore, unlike Snowden, the *Washington Post* profited from the worldwide circulation of the classified information. The *Washington Post*'s very purpose for publishing the documents was to promote global readership of the classified documents and garner subscriptions. Despite these facts, the *Washington Post* was not subject to prosecution even though a straightforward application of the elements of § 904 would place the newspaper into the death-eligible class.[123]

Although the Internet users who repost the information could not be condemned as the worst offenders in the information conspiracy, they too are death eligible under the statutory aggravating circumstance of § 904. To reiterate, the statutory aggravating circumstance implicit to

---

117 *See* Barton Gellman, *Code Name 'Verax'*, WASH. POST, June 9, 2013, http://www.washingtonpost.com/world/national-security/code-name-verax-snowden-in-exchanges-with-post-reporter-made-clear-he-knew-risks/2013/06/09/c9a25b54-d14c-11e2-9f1a-1a7cdee20287_story.html.

118 *Id.*

119 *Id.*

120 *Id.*

121 *See* Peralta, *supra* note 6.

122 10 U.S.C. § 904 (2012).

123 Yochai Benkler, *Bradley Manning 'Aiding the Enemy' Charge Is a Threat to Journalism*, THE GUARDIAN, July 19, 2013, http://www.theguardian.com/commentisfree/2013/jul/19/bradley-manning-trial-aiding-the-enemy-charge.

§ 904 is the knowledge of enemy receipt. The secondary party of Internet users is death eligible under this circumstance because the party takes the confidential information that benefits enemies of the United States and, without authorization, increases the Internet visibility of the documents. By replicating the information on the Internet, the average user, because of the default presumption established by *Romano*, possesses the requisite *mens rea* of knowledge that the information will have a global reach to enemies of the United States because it is by default not privacy protected according to judicial precedent.[124] Consequently, an average Internet user who replicates the information on the Internet could be liable for capital prosecution under the current iteration of § 904, and yet the prosecutor has again exercised his discretion without a statutorily defined meaningful basis for not prosecuting these secondary parties.[125]

Through the Snowden case, it is clear § 904's implicit aggravating circumstance of knowledge of enemy receipt is not producing a narrow class of death-eligible defendants who are classified as such because of their culpability, but is instead providing a basis for prosecutors and jurors alike to arbitrarily decide which defendants are suitable for execution. In practice, the narrowing that occurs in § 904 is the product of practical constraints and prosecutorial discretion rather than through the implicit aggravating circumstance as required by *Furman*. As Snowden's case reveals, the lack of an implicit aggravating circumstance that genuinely narrows the class of defendants gives the sentencing authority unfettered discretion that leads to arbitrary decision making which allows the worst offender to escape liability. The purpose of aggravating circumstances is to genuinely narrow the class of death-eligible defendants for creating a death-eligible class of offender and under the implicit aggravating circumstance of § 904, this function is not being performed.

As a final note, there are those who would counter the argument advanced by this Note that the current § 904 gives the prosecutor and jury unfettered discretion, resulting in arbitrary prosecutorial decisions and death sentencing that does not penalize the most culpable offenders. The counterargument would be that § 904 results in the most culpable offender being death eligible in all scenarios because it is a *military* prosecutor who exercises discretion. This counterargument would posit that Congress was aware of the broad discretion afforded to the military tribunal and military officers in determining a class of death-eligible defendants when § 904 was ratified. Congress still ratified §904 and provided this unfettered discretion exclusively to the military because of the belief that military prosecutors are the only individuals positioned to

---

124 Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 656 (N.Y. Sup. Ct. 2010).

125 10 U.S.C. § 904.

prosecute in the interests of national security because of their access to classified military intel. When applied to the Snowden case, this counterargument would conclude that the military prosecutor determined that Edward Snowden represented a more substantial threat to national security than did the *Washington Post* on the basis of classified military intel and that the judgment should be given deference as it comes from the expertise of a military officer who understands the exigencies of security.

There are areas where the exigencies of war call for deference to military decision making. Where the potential injustice outweighs the need for deference, however, the Supreme Court has reviewed the case with the same scrutiny as in civilian courts. Illustrative of this is *United States v. Tempia*, a case implicating *Miranda* rights. In *Tempia*, an officer (Tempia) was accused of misconduct while off base and demanded counsel during his interrogation by military officers.[126] Tempia was told that the Staff Judge Advocate would be unable to assist in the case, so Tempia confessed.[127] Tempia's defense counsel later sought to have his confession excluded under the rationale that Tempia was not afforded proper counsel.[128] Though it was a case dealing with military misconduct, the military commission recognized that *Miranda* rights were still afforded to Tempia because the court-martial system of justice operates in a dual capacity, to ensure "justice would be done to both the individual accused and to the military establishment of which the accused was a part."[129] The administration of the death penalty is an area where the potential injustice is of a magnitude that outweighs potential security concerns which would justify deference. This judgment about the death penalty is reflected in the court-martial's appellate review system. 28 U.S.C. § 1259 empowers the Supreme Court with the discretion to review cases under the UCMJ on direct appeal where the United States Court of Appeals of Armed Forces has conducted a mandatory review,[130] and the United States Court of Appeals of Armed Forces is mandated to review all death penalty cases under the UCMJ.[131] Thus, even though national security requires military deference in certain issue areas, the Supreme Court has extended civilian constitutional standards to military action in cases where the potential injustice in not extending the protection outweighs the need for deference.

---

126 State v. Tempia, 16 C.M.A. 629, 632 (1967).

127 James F. Falco, United States v. Tempia*: The Questionable Application of* Miranda *to the Military*, 13 VILL. L. REV. 170, 172 (1967).

128 *Id.*

129 *Id.* at 183.

130 28 U.S.C. § 1259 (2012).

131 10 U.S.C. § 867 (2012).

IV. POLICY PRESCRIPTIONS AND CONCLUSION

Section 904 in its current incarnation is constitutionally infirm. The aggravating circumstance implicit to the statute does not provide a meaningful basis for distinguishing death-eligible defendants from those who should not be eligible for capital sanction. This is because the "knowledge of enemy receipt" requirement that the statute relies on to circumscribe the defendant class has become an accepted principle for parties that transmit information over the Internet.[132] The Internet did not retain the right to privacy that adhered to pre-Internet communications technology, which resulted in the judiciary determining that users of the Internet presumptively operate with the knowledge that the information they post and transmit through the Internet is accessible by unforeseen parties worldwide, parties including enemies of the United States. Consequently, any Internet user who hosts or transmits information perceived to be detrimental to the United States is eligible for capital sanction under the statute. This class is impermissibly large and does not channel the jury's discretion sufficiently, thereby making § 904 inconsistent with the Eighth Amendment's prohibition of "cruel and unusual punishment."[133]

For the statute to comport with the Eighth Amendment, Congress must amend the *mens rea* requirement of § 904 and increase the burden to purposeful sharing of information to enemies of the United States. Additionally, the courts should presume that the purpose for information disclosure was to reach an enemy combatant and then allow the defendant to rebut that presumption with the defendant's burden of proof contingent upon whether the defendant was a primary or secondary party. As a secondary party, most Internet users could exculpate themselves with ease. Users could assert that although they knew that the posted information might reach an enemy, their connection to the enemy combatants who received the information was so tenuous that it is highly implausible the user purposefully put the information online to give to an enemy third party. Furthermore, the media outlets could also exculpate themselves from liability by asserting that the purposes for disseminating the confidential information were business motivated and not related to undermining United States national security. The primary parties, including Manning and Snowden, would face a higher burden to show that their purpose was not to disseminate the information to enemies of the United States. These primary parties would need to show that purposeful distribution to enemy combatants was not even an incidental motivator to their unauthorized disclosure of confidential information.

---

132 10 U.S.C. § 904 (2012).

133 U.S. CONST. amend. VIII.

Regardless, in order to withstand Eighth Amendment scrutiny, Congress must amend § 904's implicit statutory aggravating circumstance so that it genuinely narrows the class of offenders eligible for the death sentence. This amendment must reflect the advent of the Internet and the default mental state its users maintain: knowledge. Unless Congress updates § 904 to reflect the unreasonableness of an expectation of privacy, § 904 will be found to have an impermissibly high risk of arbitrary sentencing that makes the punishment "cruel and unusual" in violation of the Eighth Amendment.[134]

134 *Id.*