2015

Consequence, Weapons of Mass Destruction, and the Fourth Amendment's "No-Win" Scenario

Scott J. Glick
Maurice A. Deane School of Law at Hofstra University

Consequence, Weapons of Mass Destruction, and the Fourth Amendment's "No-Win" Scenario

SCOTT J. GLICK*

"Today, there is no greater threat to the American people than weapons of mass destruction . . . ." – President Barack Obama (2010)

INTRODUCTION

What is the role that consequence should play in a Fourth Amendment analysis? Should our view of reasonableness be affected by the nature of the consequence that the government seeks to prevent, such as stopping a terrorist from using a weapon of mass destruction (WMD)? While some may consider the use of a WMD by a terrorist to be a plot for an action movie, since the September 11, 2001, attacks, there have been increasing indications that malicious actors or organizations are attempting to obtain a WMD in order to cause massive devastation or catastrophic loss of life.[1] Clearly, this risk did not exist at the time

---

* Senior Counsel, National Security Division, U.S. Department of Justice, and Visiting Assistant Professor of Law, Maurice A. Deane School of Law at Hofstra University. This Article has been reviewed for publication by the Justice Department in accordance with 28 C.F.R. § 17.18. The views expressed in this Article are solely those of the author and do not necessarily reflect the views of the Justice Department. The author wishes to thank Matthew Waxman, Stephen Dycus, Joshua Geltzer, and Jordan Strauss, as well as the faculty of Hofstra Law for their review and comments on an earlier draft of this Article. The author also wishes to thank Erica Newland, J.D. Yale 2015, for her outstanding research and insightful comments.

1. *See* ROLF MOWATT-LARSSEN, HARVARD KENNEDY SCHOOL BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, AL QAEDA WEAPONS OF MASS DESTRUCTION THREAT: HYPE OR REALITY? 5–6 (2012), *available at* http://belfercenter.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf (discussing "Al Qaeda's patient, decade-long effort to steal or construct an improvised nuclear device" and its "perception of the benefits of producing the image of a mushroom cloud rising over a U.S. city, just as the 9/11 attacks have altered the

the Constitution was adopted.[2] Indeed, one expert has warned that at "no time in human history has there been the ability for a cabal of hateful fanatics, unfettered from the constraints of a state, to destroy cities or kill hundreds of thousands in a single cataclysmic act."[3]

Aside from advancements in technology that may enable the government to deploy a comprehensive system of WMD sensors in the future,[4] one of the most effective methods that the government could employ to locate a suspected terrorist who intended to use a WMD in an American city would be to monitor the terrorist's communications. There are two different statutory regimes that regulate the government's ability to obtain the content of communications in the United States—the Foreign Intelligence Surveillance Act of 1978 (FISA)[5] and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[6] To be sure, if the government is able to establish probable cause with respect to a particular telephone or e-mail account that is being used by a terrorist (and is able to meet the other requirements of FISA or Title III), then the government can obtain a lawful wiretap[7] to monitor the content[8] of the communications. Indeed, it is well settled

---

course of history"); Federal Bureau of Investigation, *Weapons of Mass Destruction: Frequently Asked Questions*, http://www.fbi.gov/about-us/investigate/terrorism/wmd/wmd_faqs (noting that there are indicators of increasing WMD threats since the 9/11 attacks); *see also* STEVE BOWMAN, CONG. RESEARCH SERV., RL31332, WEAPONS OF MASS DESTRUCTION: THE TERRORIST THREAT (2002) ("The continuing possibility of terrorist attacks using nuclear, biological, or chemical weapons is an ongoing concern in the national security policy arena in the face of a clear trend among terrorists to inflict greater numbers of casualties.").

2. While cannons pulled by horses or loaded on ships may have posed the greatest threat to colonists, some historians have found circumstantial evidence that British troops sought to use naturally occurring incidents of small pox as biological weapons during the colonial period both prior to and during the American Revolution. *See* Elizabeth A. Fenn, *Biological Warfare in Eighteenth-Century North America: Beyond Jeffery Amherst*, 86 J. AM. HIST. 1522, 1565–70 (2000); Harold B. Gill, Jr., *Colonial Germ Warfare*, COLONIAL WILLIAMSBURG J. (Spring 2004), http://www.history.org/Foundation/journal/Spring04/warfare.cfm.

3. *See Nuclear Terrorism: Assessing the Threat to the Homeland: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs,* 110th Cong. 405 (2008) [hereinafter *Nuclear Terrorism Hearing*] (statement of Gary Anthony Ackerman, Research Director, National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland).

4. *See U.S. Researchers Unveil New WMD Sensors*, GLOBAL SECURITY NEWSWIRE (Apr. 3, 2006), http://www.nti.org/gsn/article/us-researchers-unveil-new-wmd-sensors ("The Argonne National Laboratory in Illinois has developed new sensors for remote detection of WMD materials . . . ."). The application of the Fourth Amendment to the use of such sensors in public or private spaces is beyond the scope of this Article. *Cf.* Kyllo v. United States, 533 U.S. 27, 40 (2001) (discussing the use of a device that "explore[s] details of the home that would previously have been unknowable without physical intrusion").

5. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1811 (2012).

6. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520 (2012).

7. This Article uses the term "wiretap" to generically describe the monitoring, interception, or recording of the contents of telephone or e-mail communications in circumstances in which a person has a reasonable expectation of privacy. However, it should be noted that "electronic surveillance" is a term of art that is specifically defined in FISA. *See* 50 U.S.C. § 1801(f) (2012). Whether specific forms of monitoring, interception, or recording constitute electronic surveillance within the meaning of FISA is beyond the scope of this Article.

8. Other tools in FISA and Title 18 permit the government to obtain noncontent

that where the government has individualized suspicion in regard to a particular communication device and meets the statutory requirements of FISA or Title III, court-authorized wiretaps are constitutional.[9]

However, let us assume that a reliable informant, who has an established track record and inside access to a terrorist group, reports that a highly skilled member of that terrorist group has entered the United States and intends to assemble a WMD in a major metropolitan city on the East Coast sometime within the next thirty to forty-five days. To add additional context, let us further assume that the informant is 80 percent certain that the terrorist is assembling the WMD in a safe house somewhere in Georgetown, a historic neighborhood located approximately two miles from the White House. If the informant does not know the precise location or the specific telephone or e-mail account that the terrorist is using to communicate with other coconspirators, how should a federal court resolve the constitutional tension that would arise if the government sought an order permitting it to target an indeterminate number of communication devices? If the nation was not at war,[10] would a federal court under the circumstances of this hypothetical be faced with what some may call the Fourth Amendment's "no-win" scenario? Would the court face the choice of either issuing an unconstitutional order that allows the government to wiretap every communication device being used in Georgetown (because that is the *only way* to find the terrorist and *prevent* the use of the WMD) or refusing to issue the order because the Fourth Amendment[11] tolerates no other result, which could lead to massive destruction or catastrophic loss of life?

The WMD scenario enables us to explore what may very well be some of the most challenging constitutional questions of our time. First, should consequence—that is, the nature and gravity of harm the government seeks to prevent—ever play an outcome-determinative role in a Fourth Amendment analysis? Equally important: who should decide whether consequence has a role to play? And finally, how can government officials, who are responsible for protecting the nation from terrorists seeking to cause a catastrophic consequence, obtain greater ex ante certainty in regard to the constitutionality of their preventative actions?

---

information, such as dialing, signaling, routing, and addressing information (DRAS) as well as other basic and transactional subscriber information. *E.g.*, 18 U.S.C. §§ 2701–2709 (2012); 18 U.S.C. §§ 3121–3127 (2012); 50 U.S.C. §§ 1841–1846, 1861 (2012). This Article focuses on issues relating to the government's ability to obtain the content of communications.

9. Although the Supreme Court has never directly ruled on the constitutionality of FISA or Title III, lower federal courts have rejected all facial challenges to these statutes. *E.g.*, *In re* Sealed Case, 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002) (holding FISA constitutional); United States v. Bobo, 477 F.2d 974, 982 (4th Cir. 1973) (holding Title III constitutional and citing widespread agreement across the circuits on its constitutionality).

10. Issues relating to the use of wiretaps during a time of war are beyond the scope of this Article. FISA, however, does authorize the "President, through the Attorney General . . . to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress." 50 U.S.C. § 1811 (2012).

11. The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

While the Supreme Court has relaxed Fourth Amendment requirements in the context of searches designed to serve "special needs,"[12] the underlying rationale for upholding these searches is that diminished expectations of privacy exist in certain circumstances and, when weighed against governmental interests that transcend ordinary law enforcement needs, the government's interests outweigh those diminished expectations of privacy.[13] In some special needs cases, the federal courts have therefore concluded that the Fourth Amendment will tolerate suspicionless and even warrantless searches.[14] In the hypothetical, however, we can stipulate that individual expectations of privacy with respect to the content of the wire or electronic communications[15] that would be intercepted would be at their zenith. Moreover, the emergency exceptions carved out by the Supreme Court require an immediacy not necessarily present in our hypothetical.[16] The central and fundamental issue is, therefore, whether consequence matters from a constitutional perspective.

The Supreme Court has yet to face a Fourth Amendment case involving the potential for massive destruction or catastrophic loss of life from the threatened use of a WMD. While the Court stated in dicta more than a decade ago that the "Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an *imminent* terrorist attack,"[17] it has rejected a special crime-scene exception to the Fourth Amendment when a murder has taken place.[18] Additionally, it has recently stated, in a case involving Global Positioning System (GPS)

---

12. Chandler v. Miller, 520 U.S. 305, 313–14 (1997) (stating that particularized exceptions to the individualized suspicion requirement are sometimes warranted when special needs concerns other than crime detection are at issue).

13. *See* Illinois v. McArthur, 531 U.S. 326, 330 (2001) ("When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."); Ric Simmons, *Searching for Terrorists: Why Public Safety is Not a Special Need*, 59 DUKE L.J. 843, 890 (2010) ("For some of these searches, the Supreme Court has stressed that the nature of the intrusion is very slight and that the subject has a reduced expectation of privacy . . . .").

14. *See infra* notes 85–96 and accompanying text.

15. Under Title III a "wire communication" is defined as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce." 18 U.S.C. § 2510(1) (2012). Title III defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include [a wire communication]." 18 U.S.C. § 2510(12) (2012).

16. *See infra* notes 69–84 and accompanying text.

17. City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (emphasis added) (citing Edmond v. Goldsmith, 183 F.3d 659, 662–63 (7th Cir. 1999)).

18. Mincey v. Arizona, 437 U.S. 385, 395 (1978) (rejecting a "murder-scene" exception to the Fourth Amendment's warrant requirement despite the severity of the crime); *see also* Michigan v. Tyler, 436 U.S. 499, 511 (1978) (finding that the seriousness of the crime does not create an exigency justifying a search without a warrant).

monitoring, that there is "no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated."[19] On the other hand, in that same case, five Justices agreed with the proposition that "longer-term GPS monitoring . . . of *most offenses* impinges on expectations of privacy,"[20] and four Justices stated that the Court did not need to consider whether prolonged GPS monitoring in the context of investigations of " *extraordinary offenses* would similarly intrude on a constitutionally protected sphere of privacy."[21] This suggests that a majority of the Court might conclude that consequence should play an important role in a Fourth Amendment calculus. Waiting for such a case to reach the Court,[22] however, is arguably not in the best interests of the nation, particularly if solving the no-win scenario requires policy choices more appropriately made by elected officials than by judges.[23]

The purpose of this Article is to look at consequence, with a particular focus on the threatened use of a WMD, and begin a discussion on a new doctrinal solution to the hypothetical.[24] As background, Part I takes a look at cardinal Fourth

---

19. United States v. Jones, 132 S. Ct. 945, 954 (2012).

20. *Id.* at 964 (Alito, J., concurring, with whom Ginsburg, Breyer, and Kagan, J. joined) (emphasis added); *see id.* at 955 (Sotomayor, J., concurring) ("I agree with Justice ALITO that, at the very least, 'longer term GPS monitoring in investigations of *most offenses* impinges on expectations of privacy.'" (emphasis added)).

21. *Id.* at 964 (Alito, J., concurring) (emphasis added).

22. *See* Richard S. Frase, *What Were They Thinking? Fourth Amendment Unreasonableness in* Atwater v. City of Lago Vista, 71 FORDHAM L. REV. 329, 417 (2002) ("It seems inevitable that the Court will be presented with one or more cases in which the police request additional investigative authority to deal with terrorism or other threats of catastrophic harm."). Recently, the Supreme Court touched on this issue when it considered a Fourth Amendment case involving a driver who had been stopped for expired registration tags. Riley v. California, 134 S. Ct. 2473 (2014). After the driver's car was impounded, an inventory search revealed two handguns under the car hood. *Id.* at 2480. At the scene, and later at the police station, the police conducted a search of his cellular telephone without a warrant, and found text messages and other evidence of gang-related activity. *Id.* Although the Court's decision was limited to the question of "how the search incident to arrest doctrine applies to modern cell phones," *id.* at 2484, Justice Anthony M. Kennedy had the following exchange with California Solicitor General Edward Dumont during oral argument.

> JUSTICE KENNEDY: It seems to me that in order to try to give some answer to [these] concerns that maybe the distinction *ought to be* between serious and nonserious offenses—offenses. I don't think that exists in our jurisprudence. Correct me if I'm wrong.
>
> MR. DUMONT: I think that's correct. The Court has previously declined to draw that line.

Transcript of Oral Argument at 41, Riley v. California, 134 S. Ct. 2473 (2014) (No. 13-132) (emphasis added).

23. *See infra* notes 297–316 and accompanying text.

24. This Article focuses on a subset of a related and broader issue that other scholars have explored—namely, whether "crime-severity" distinctions should affect different Fourth Amendment outcomes. *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 802 (1994); Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 9 (2011); Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment*

Amendment principles and rules, as well as the many exceptions to the warrant, probable cause, and particularity requirements that the Supreme Court has recognized, and analyzes their potential applicability to the hypothetical. Part I also seeks to draw the important distinction between reasonable expectations of privacy, the analytical framework that governs whether certain government activities constitute a search within the meaning of the Fourth Amendment, and the Fourth Amendment's reasonableness requirement, which necessitates a weighing of competing constitutional interests. Most significantly, Part I discusses minimization, a well-established privacy-enhancing mechanism that normally serves as a back-end check on the government's conduct, to determine whether it can serve as a front-end substitute for the Fourth Amendment's particularity requirement.

Part II briefly explores the differences between chemical, biological, radiological, and nuclear WMDs, as well as the different consequences that can reasonably be anticipated from their respective use.[25] Identifying those differences is critical to understanding how the significant definitional issues identified in Part III might affect the implementation of any new doctrinal solution. Part IV then looks at these issues through what I have elsewhere described as the "Fourth Amendment's protective lens,"[26] and proposes that we use a probability consequence matrix as an analytical framework to solve the no-win scenario. Finally, Part V seeks to lay out a path forward so that Congress can consider and enact sensible legislation that will enable us to identify the limited circumstances in which consequence should be considered a factor in a Fourth Amendment calculus, particularly when a terrorist threatens to use a WMD.

I. THE FOURTH AMENDMENT

A. Principles and Rules

The Fourth Amendment is a "compound sentence consisting of two related clauses."[27] The first clause provides that the "right of the people to be secure in

---

"Reasonableness," 98 COLUM. L. REV. 1642, 1660 (1998); Frase, *supra* note 22, at 420; Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. CAL. L. REV. 777, 819–23 (2004); John Kaplan, *The Limits of the Exclusionary Rule*, 26 STAN. L. REV. 1027, 1037 (1974); Wesley MacNeil Oliver, *Toward a Better Categorical Balance of the Costs and Benefits of the Exclusionary Rule*, 9 BUFF. CRIM. L. REV. 201, 241, 246 (2005); Richard A. Posner, *Rethinking the Fourth Amendment*, 1981 SUP. CT. REV. 49, 53, 74 (1981); William A. Schroeder, *Factoring the Seriousness of the Offense into Fourth Amendment Equations—Warrantless Entries into Premises: The Legacy of* Welsh v. Wisconsin, 38 U. KAN. L. REV. 439, 528–29 (1990); Simmons, *supra* note 13, at 895; William J. Stuntz, Commentary, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 875 (2001).

25. Part II is based upon unclassified sources of information that are available to the general public.

26. Scott J. Glick, *Virtual Checkpoints and Cyber-*Terry *Stops: Digital Scans to Protect the Nation's Critical Infrastructure and Key Resources*, 6 J. NAT'L SECURITY L. & POL'Y 97, 125 (2012) (arguing that the Fourth Amendment's "protective lens" strongly supports the existence of a limited "cybersecurity exception").

27. Morgan Cloud, Review, *Searching Through History; Searching for History*, 63 U. CHI. L. REV. 1707, 1721 (1996); *see also* Owen Fiss, *Even in a Time of Terror*, 31 YALE L. &

their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[28] The second, commonly referred to as the "warrant clause,"[29] provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized."[30]

A "search" within the meaning of the Fourth Amendment takes place whenever the government intrudes upon "an expectation of privacy that society is prepared to consider reasonable."[31] This formulation, which flows from Justice John Marshall Harlan's concurring opinion in *Katz v. United States*,[32] breaks down into a "two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?"[33] If the government's conduct violates a person's reasonable expectation of privacy, or involves a trespass or physical intrusion upon a constitutionally protected area, then the courts will consider the government's conduct to be a search.[34] By way of comparison, a "seizure" within the meaning of the Fourth Amendment only takes place when there has been a "meaningful interference with an individual's possessory interests in that property,"[35] or when there has been a "governmental termination of freedom of movement through means intentionally applied."[36] Thus, the threshold question in any Fourth Amendment calculus is whether a search or seizure has occurred.[37] Only after that determination has been made do we turn to the question of whether that search or seizure is reasonable.

Notwithstanding the fact that many scholars have criticized the Supreme Court for its lack of clarity and consistency in its treatment of the Fourth Amendment,[38] a

---

POL'Y REV. 1, 25 (2012) ("The Fourth Amendment has an unusual grammatical structure...[that] consists of two clauses.").

28. U.S. CONST. amend. IV.

29. 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 3.1(a), at 3–4 (5th ed. 2012) (noting that this clause is "customarily referred to as the warrant clause").

30. U.S. CONST. amend. IV.

31. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

32. 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring). *See generally* 1 LAFAVE, *supra* note 29, at 576–93.

33. California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).

34. *See* United States v. Jones, 132 S. Ct. 945, 953 (2012) (holding that placing a GPS tracking device on a vehicle for the purpose of obtaining information constitutes a trespass and therefore a search in a constitutionally protected area, and stating that "[s]ituations involving merely the transmission of electronic signals without trespass . . . remain subject to *Katz* analysis" (emphasis omitted)); *see also* Illinois v. Andreas, 463 U.S. 765, 771 (1983) (stating that "[t]he Fourth Amendment protects legitimate expectations of privacy rather than simply places").

35. *Jacobsen*, 466 U.S. at 113.

36. Brower v. Cnty. of Inyo, 489 U.S. 593, 597 (1989) (emphasis omitted).

37. *See generally* Scott J. Glick, Note, *Reexamining Fourth Amendment Seizures: A New Starting Point*, 9 HOFSTRA L. REV. 211 (1980) (discussing an analytical framework for determining whether a seizure has occurred).

38. *E.g.*, Amar, *supra* note 24, at 757 ("The Fourth Amendment today is an

half century of jurisprudence has yielded a number of fundamental principles and rules. First, as the Supreme Court has repeatedly stated, the Fourth Amendment has a "strong preference for searches conducted pursuant to a warrant."[39] Although the text itself does not delineate when precisely a warrant must be obtained,[40] the Supreme Court has concluded that all warrantless searches are "per se unreasonable" subject only to "established and well-delineated exceptions."[41] Accordingly, unless such an exception applies, the government must obtain a court order from a "neutral and detached" magistrate authorizing the search.[42]

A search warrant cannot be lawfully issued by a court unless it is supported by "Oath or affirmation" that establishes probable cause to believe that a crime has been committed and that evidence of the crime is located in the place to be searched.[43] Moreover, search warrants must "particularly" describe the place to be searched and the items to be seized.[44] Notably, "the Fourth Amendment does not elaborate on the meaning of probable cause."[45] Nonetheless, the Supreme Court has emphasized that the probable cause standard is a "practical, nontechnical conception"[46]—a "fluid concept . . . not readily, or even usefully, reduced to a neat set of legal rules,"[47] that requires courts to take into account competing interests.[48]

The Constitution's text does not define the quantum of proof that would satisfy the probable cause standard.[49] While it is clear that a court cannot authorize a search or seizure based on "mere suspicion"[50] or "affidavits which are purely conclusory,"[51] the Supreme Court has stated that probable cause exists "where the

---

embarrassment."); David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L., 581, 581 (2008) ("The doctrinal incoherence of Fourth Amendment law disturbs many judges and scholars."). The Supreme Court has also been critical of its own jurisprudence. *E.g.*, California v. Acevedo, 500 U.S. 565, 583 (1991) (Scalia, J., concurring in judgment) ("There can be no clarity in this area unless we make up our minds, and unless the principles we express comport with the actions we take."); Coolidge v. New Hampshire, 403 U.S. 443, 483 (1971) (explaining that Fourth Amendment law has not been reduced to "complete order and harmony").

39. Ornelas v. United States, 517 U.S. 690, 699 (1996); Massachusetts v. Upton, 466 U.S. 727, 733 (1984); Illinois v. Gates, 462 U.S. 213, 236 (1983).

40. Kentucky v. King, 131 S.Ct. 1849, 1856 (2011).

41. Katz v. United States, 389 U.S. 347, 357 (1967) (emphasis omitted).

42. Johnson v. United States, 333 U.S. 10, 14 (1948) (inferences should be "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime").

43. U.S. CONST. amend. IV.

44. *See* Berger v. New York, 388 U.S. 41, 56 (1967) (acknowledging that there is an especially great need for particularity when judicial authorization is sought for electronic eavesdropping).

45. Fiss, *supra* note 27, at 20.

46. Illinois v. Gates, 462 U.S. 213, 231 (1983) (quoting Brinegar v. United States, 338 U.S. 160, 176 (1949)).

47. *Id.* at 231.

48. *See Brinegar*, 338 U.S. at 176 (explaining that probable cause is a "practical, nontechnical conception affording the best compromise that has been found for accommodating . . . opposing interests"); *infra* note 66 and accompanying text.

49. *See* U.S. CONST. amend. IV.

50. Wong Sun v. United States, 371 U.S. 471, 479 (1963).

51. United States v. Ventresca, 380 U.S. 102, 108 (1965).

known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found."[52] However, the Supreme Court has also stated that "finely tuned" standards, such as preponderance of the evidence,[53] are more appropriate to formal adversarial proceedings and have "no place" in a magistrate's probable cause determination.[54] Thus, in determining whether probable cause exists, the Supreme Court has directed magistrates and judges to look at all of the circumstances and determine whether there is "a fair probability that contraband or evidence of a crime will be found in a particular place."[55]

The Fourth Amendment's particularity requirement ("no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly* describing the place to be searched, and the persons or things to be seized")[56] serves a slightly different, albeit related, purpose to the probable cause requirement. The particularity requirement serves as a check on the government's ability to obtain a "general" warrant, which was a source of great concern to the Framers.[57] While an academic debate may exist with regard to whether the Framers only opposed general warrants of the home (compared to general warrants of commercial or other highly regulated businesses)[58] taken together, the Fourth Amendment's probable cause and particularly requirements "minimize the risk that

---

52. Ornelas v. United States, 517 U.S. 690, 696 (1996).

53. In order to meet the preponderance of the evidence standard, a party must establish that "on the whole" of the evidence, he "has the stronger evidence, however slight the edge may be." BLACK'S LAW DICTIONARY 1373 (10th ed. 2014); *see* CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, EVIDENCE, 109 (4th ed. 2009) (stating that the fact finder must be "persuaded that the points to be proved are more probably so than not").

54. Illinois v. Gates, 462 U.S. 213, 235 (1983).

55. *Id.* at 238. Moreover, the role of the reviewing court "is simply to ensure that the magistrate had a 'substantial basis for . . . conclud[ing]' that probable cause existed." *Id.* at 238–39 (alteration in original) (citation omitted); *accord* Massachusetts v. Upton, 466 U.S. 727, 732–33 (1984) (stating that the reviewing court should decide "whether the evidence viewed as a whole provided a 'substantial basis' for the Magistrate's finding of probable cause").

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

57. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."); Riley v. California, 134 S. Ct. 2473, 2494 (2014) ("Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era . . . ."); Steinberg, *supra* note 38, at 594 (noting that "the Framers viewed . . . the general warrant as dangerous and subject to abuse"). For a comprehensive history of the Fourth Amendment, see generally WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND MEANING 602–1791 (2009).

58. *See* Berger v. New York, 388 U.S. 41, 58 (1967) ("The use of [general warrants] was a motivating factor behind the Declaration of Independence."). *But see* CUDDIHY, *supra* note 57, at 743 ("Even the states with the strongest constitutional restrictions on general searches had long exposed commercial establishments to warrantless inspection."). *See generally* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 551 (1999) (explaining that the Framers discussions were "almost exclusively about the need to ban house searches under general warrants").

officers executing search warrants will by mistake search a place other than the place intended by the magistrate."[59] In the context of the hypothetical and the need to intercept the terrorist's communications, the particularity requirement ensures that the government is directed to acquire only the communications that the magistrate has authorized. As the Supreme Court has stated, the need for particularity here is "especially great" since wiretapping involves an "intrusion on privacy that is broad in scope."[60] The particularity requirement therefore requires a neutral and detached magistrate to approve the communications that may be searched as well as the communications that may be seized.[61]

Finally, the Fourth Amendment's reasonableness clause ("[t]he right of the people to be secure . . . against *unreasonable* searches and seizures, shall not be violated")[62] serves as an additional check on the government's conduct by preventing the government from exceeding the authorized scope of the warrant, and by ensuring that the police do not act impermissibly in executing the court-approved search or seizure.[63] While some Supreme Court decisions may have raised a question in regard to whether or not the reasonableness clause and the warrant clause were intended to be read in the disjunctive or in the conjunctive,[64] today it is "clearly established that the [reasonableness] clause does provide some additional power."[65] Thus, even when the warrant clause is satisfied, courts are *still* required to assess the degree to which a search or seizure is reasonable; that is, courts are required to assess the degree to which the search or seizure intrudes on an individual's privacy in relation to "the degree to which it is needed for the promotion of legitimate governmental interests."[66]

---

59. 2 LAFAVE, *supra* note 29, § 4.5, at 709; *see also* Groh v. Ramirez, 540 U.S. 551, 561 (2004) (explaining that the particularity requirement also assures the "limits" of the search); 2 LAFAVE, *supra* note 29, § 4.5(b), at 731 ("A search warrant for an apartment house or hotel or other multi-occupancy building will usually be held invalid if it fails to describe the particular subunit to be searched with sufficient definiteness to preclude a search of one or more subunits indiscriminately."); 3 LAFAVE, *supra* note 29, § 7.2(c), at 751 (suggesting that particularity limits the intensity of the search and minimizes the risk that innocent objects will be seized by mistake).

60. *Berger*, 388 U.S. at 56; *see also* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("[R]esponsible officials . . . must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy.").

61. *See Berger*, 338 U.S. at 59 (finding several constitutional defects in New York's wiretapping statute including that it gave "too much to the discretion of the officer executing the order"); 5 LAFAVE, *supra* note 29, § 10.1(c), at 22 (explaining that because particularity limits what a police officer may seize and where he may look, "[t]he police may not look in an envelope for an elephant").

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

63. *See* Wilson v. Layne, 526 U.S. 603, 611 (1999) ("[T]he Fourth Amendment does require that police actions in execution of a warrant be related to the objectives of the authorized intrusion[.]").

64. *See* Cloud, *supra* note 27, at 1722–23; *see also* Amar, *supra* note 24, at 762–81.

65. 2 LAFAVE, *supra* note 29, § 3.1(a), at 4.

66. Samson v. California, 547 U.S. 843, 848 (2006); *see also* United States v. Knights, 534 U.S. 112, 118–19 (2001) ("[T]he reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the

A review of the foregoing principles and rules might lead one to conclude that it is not possible to solve the Fourth Amendment's no-win scenario. Yet, as discussed below, a close examination of decades of Supreme Court jurisprudence, including a number of exceptions that have been approved by the Court, reveals the potential for a new doctrinal solution.

B. Exceptions

Historically, a person's home has been given the greatest degree of protection under the Fourth Amendment.[67] Yet, the Supreme Court has not always required law enforcement officers to obtain a warrant to enter a home and, in certain circumstances, the probable cause and the particularity requirements have also been relaxed, prompting one scholar to opine that Fourth Amendment jurisprudence is a "doctrinal mess."[68] This Part will review exceptions to the Fourth Amendment's warrant, probable cause, and particularity requirements, in order to assess their potential applicability to the hypothetical.

1. The Warrant Requirement

The Supreme Court and the federal courts have identified three related exigent-circumstance exceptions to the warrant requirement: hot pursuit, loss or destruction of evidence, and emergency aid.[69] In *Warden v. Hayden*,[70] the Supreme Court recognized that the hot pursuit of a fleeing felon does not require the police to obtain a warrant prior to entering a home. In *Warden*, the government had been

---

other, the degree to which it is needed for the promotion of legitimate governmental interests.'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))); Richards v. Wisconsin, 520 U.S. 385, 394 (1997) (balancing the "legitimate law enforcement concerns at issue in the execution of search warrants and the individual privacy interests affected by no-knock entries"); Tennessee v. Garner, 471 U.S. 1, 8 (1985) ("We have described 'the balancing of competing interests' as 'the key principle of the Fourth Amendment.'" (quoting Michigan v. Summers, 452 U.S. 692, 700 n.12 (1981))). As Professor LaFave aptly notes, however, this "naturally raises the question of whether this 'compromise' must always be struck in precisely the same way, or whether on the other hand the probable cause requirement may call for a greater or lesser quantum of evidence, depending upon the facts and circumstances of the individual case." 2 LAFAVE, *supra* note 29, §3.2(a), at 30.

67. *E.g.*, United States v. James Daniel Good Real Prop., 510 U.S. 43, 53–54 (1993) (stating that a person's right to "maintain control over his home, and to be free from governmental interference, is a private interest of historic and continuing importance"); United States v. Karo, 468 U.S. 705, 714 (1984) ("[R]esidences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle."); Payton v. New York, 445 U.S. 573, 586 (1980) ("It is a 'basic principal of Fourth Amendment law' that searches and seizures inside a home without a warrant are presumptively unreasonable.").

68. Amar, *supra* note 24, at 759; *id.* at 757 (observing that warrants are required, unless they are not, and that the probable cause requirement has often been ignored).

69. *See* Georgia v. Randolph, 547 U.S. 103, 116 n.6 (2006).

70. 387 U.S. 294 (1967).

informed that an armed robbery had taken place and the suspect had fled into a home "less than five minutes before they reached it."[71] Although the police had a description of the suspect and the weapons he had used during the robbery, the Court held that the Fourth Amendment does not require police officers to obtain a warrant and delay the investigation if doing so would "gravely endanger their lives or the lives or others."[72] The Court further stated that "[s]peed here was essential, and only a thorough search of the house for persons and weapons could have insured that [the suspect] was the only man present and that the police had control of all weapons which could be used against them or to effect an escape."[73]

Stated another way, *Warden* and its progeny stand for the proposition that where probable cause to obtain a warrant exists but the exigency of the particular situation makes it impossible to obtain a warrant, the Fourth Amendment will tolerate a warrantless entry into a home to make an arrest.[74] Notably, however, the Supreme Court has observed that many lower courts have looked at the hot pursuit exception in relation to the crime that has been committed, and the gravity of the offense.[75] That consideration becomes significant as we consider whether consequence, which is directly tied to the gravity of the risk posed by a WMD, should play an outcome-determinative role in a Fourth Amendment analysis.

The Supreme Court has also relaxed the warrant requirement to prevent the loss or destruction of evidence. For example, in *Schmerber v. California*,[76] the defendant was under arrest in a hospital for driving while under the influence of alcohol. The Court concluded that the police could take a blood sample from the defendant without a warrant since there had been a lawful arrest, and delay could lead to a destruction of the evidence.[77] Indeed, when emergency or exceptional circumstances threaten the loss or destruction of evidence, the federal courts have consistently approved warrantless searches.[78] Here too, however, even where the government can establish a potential loss of evidence, the Court has rejected a warrantless entry into a home if the offense the government is pursuing is only a

---

71. *Id.* at 298.

72. *Id.* at 298–99.

73. *Id.* at 299.

74. *See id.* at 298–99; Welsh v. Wisconsin, 466 U.S. 740, 750 (1984); United States v. Santana, 427 U.S. 38, 42–43 (1976).

75. *E.g.*, *Welsh*, 466 U.S. at 752; United States v. Cattouse, 846 F.2d 144, 146 (2d Cir. 1988) (finding that the gravity of the offense is a relevant factor in determining whether exigent circumstances exist); United States v. Martinez-Gonzalez, 686 F.2d 93, 100–01 (2d Cir. 1982) (noting the seriousness of the offense justifying warrantless entry); Dorman v. United States, 435 F.2d 385, 392 (D.C. Cir. 1970) (emphasizing the gravity of the offense).

76. 384 U.S. 757 (1966).

77. *Id.* at 770. One of the underlying rationales for the automobile search exception to the warrant requirement is the potential for the loss of evidence. *See* Chambers v. Maroney, 399 U.S. 42, 48 (1970) (noting that vehicles can be "quickly moved").

78. *E.g.*, Brigham City v. Stuart, 547 U.S. 398, 403 (2006). *Compare* United States v. Jeffers, 342 U.S. 48, 52 (1951) (finding unlawful entry where there was no imminent destruction, removal, or concealment of property) *with* McDonald v. United States, 335 U.S. 451, 455 (1948) (noting that there was no property that was in the process of being destroyed).

minor one,[79] which further suggests that the nature of an offense is important and can play a limiting role as well.

The Supreme Court has also approved warrantless entry into a home to assist a person in need of immediate aid.[80] The Court has stated that "[t]he need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal absent an exigency or emergency."[81] Moreover, the Court has approved the use of a brief "protective sweep" in a home without a warrant, if the sweep was preceded by a lawful arrest of an occupant of the home.[82] The Court has made it clear in the protective sweep cases, however, that the burden is on the government to establish a reasonable basis to believe that the area "harbors an individual posing a danger to those on the arrest scene."[83] Indeed, such a search must be limited in time and location; that is, it must be "no longer than is necessary to dispel the reasonable suspicion of danger" and limited to places where a person, not evidence, might be located.[84]

These cases illustrate that the protection and preservation of life is a factor that could justify what might otherwise be an unacceptable intrusion on privacy. However, they also stand for the proposition that important limiting considerations exist, even when there is danger to life.

2. The Probable Cause Requirement

As discussed earlier, probable cause is at the core of the Fourth Amendment's warrant requirement. Yet, the Supreme Court has relaxed the probable cause requirement in what have become known as the "special needs"[85] or "administrative search"[86] cases, thereby enabling the government to conduct

---

79. *See Welsh*, 466 U.S. at 750; 3 LAFAVE, *supra* note 29, § 6.5(a), at 515 (suggesting that exigent circumstances has a "hollow ring" when there is no emergency and evidence is not in the process of destruction); *see also* MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE, § 260.5 (1973) (stating that a warrantless search of premises may be undertaken upon reasonable cause to believe that premises contain "(1) individuals in imminent danger of death or serious bodily harm; or (2) things imminently likely to burn, explode, or otherwise cause death, serious bodily harm or substantial destruction of property").

80. *E.g.*, Michigan v. Fisher, 130 S. Ct. 546, 549 (2009) (per curiam).

81. Mincey v. Arizona, 437 U.S. 385, 392 (1978) (quoting Wayne v. United States, 318 F.2d 205, 212 (D.C. Cir. 1963)).

82. Maryland v. Buie, 494 U.S. 325, 337 (1990) (approving a warrantless protective sweep of premises following an in-home arrest in order to find others who might pose a danger to officers).

83. *Id.*

84. *Id.* at 334 (approving a "look in closets and other spaces immediately adjoining the place of arrest from which an attack could be immediately launched").

85. *E.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (random drug testing of student athletes); Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665–66 (1989) (drug tests for United States Customs Service employees seeking transfer or promotion to certain positions); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 620–21 (1989) (drug and alcohol tests for railway employees involved in train accidents or found to be in violation of particular safety regulations).

86. *E.g.*, New York v. Burger, 482 U.S. 691, 702–04 (1987) (warrantless administrative

certain kinds of warrantless searches without probable cause or any degree of individualized suspicion.[87] In these cases, which generally developed outside of the terrorism context, the Court upheld suspicionless, and sometimes warrantless, searches that furthered a "special need[], beyond the normal need for law enforcement."[88] The Court looked at the "programmatic purpose"[89] that motivated the government's conduct to ensure that the government was seeking to protect against a "concrete danger"[90] independent of general law enforcement purposes.[91] If the Court found such a programmatic purpose, as in the case of sobriety checkpoints where the animating purpose is to eliminate the "immediate, vehicle-bound threat to life and limb"[92] that results from the presence of intoxicated drivers on the public highways, then it would uphold the search and seizure.[93]

While a compelling governmental need is a prerequisite for the relaxation of the probable cause requirement in these cases, as the Supreme Court has made clear, alone it has not been sufficient. Essential to the Court's analyses has been the consideration of other factors, such as the reasonableness of the search and the level of intrusion on an individual's privacy.[94] For example, in upholding a

---

inspection of premises of "closely regulated" business); Michigan v. Tyler, 436 U.S. 499, 507–09, 511–12 (1978) (administrative inspection of fire-damaged premises to determine cause of blaze); Camara v. Mun. Court of S.F., 387 U.S. 523, 534–39 (1967) (administrative inspection to ensure compliance with city housing code that was not aimed at "the discovery of evidence of crime").

87. Nat'l Treasury Employees Union, 489 U.S. at 665 (emphasizing that "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance"). *See generally* 5 LAFAVE, *supra* note 29, § 10.1.

88. Chandler v. Miller, 520 U.S. 305, 313 (1997).

89. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 45–46 (2000) ("[P]rogrammatic purposes may be relevant to the validity of Fourth Amendment intrusions undertaken pursuant to a general scheme without individualized suspicion.").

90. *Chandler*, 520 U.S. at 318–19.

91. *See* O'Connor v. Ortega, 480 U.S. 709, 720 (1987) (plurality opinion) ("There are some . . . 'exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'" (quoting New Jersey v. T.L.O., 469 U.S. 335, 351 (1985))); *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011–12 (Foreign Int. Surv. Ct. Rev. 2008) (finding a foreign intelligence exception to the Fourth Amendment because national security is of "the highest order of magnitude" and the "programmatic purpose of the surveillances . . . involves some legitimate objective beyond ordinary crime control"); Cassidy v. Chertoff, 471 F.3d 67, 82 (2d Cir. 2006) ("Preventing or deterring large-scale terrorist attacks present problems that are distinct from standard law enforcement needs and indeed go well beyond them."); *cf. Edmond*, 531 U.S. at 43 ("We are particularly reluctant to recognize exceptions to the general rule of individualized suspicion where governmental authorities primarily pursue their general crime control ends.").

92. *Edmond*, 531 U.S. at 43 (discussing Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 451 (1990)).

93. *See Sitz*, 496 U.S. at 451 (1990) ("[A]lcohol-related death and mutilation on the Nation's roads are legion.").

94. *E.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 830–38 (2002) (holding that the school's interest in preventing drug use outweighed limited intrusion and reduced privacy interests); United States v. Knights, 534 U.S. 112, 119–20 (2001) (holding probationers and parolees

drug-testing program for the Vernonia, Oregon, school district—one that was not predicated on probable cause—Justice Antonin Scalia, writing for a majority of the Court, stated that "the ultimate measure of the constitutionality of a governmental search is 'reasonableness,'" particularly in cases where there was "no clear practice, either approving or disapproving the type of search at issue, at the time the constitutional provision was enacted."[95] Whether a particular search meets the reasonableness standard should be "judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[96]

None of the cases in which the Supreme Court relaxed the probable cause requirement to allow the government to meet special or administrative search needs arose in the context of the government seeking to prevent the use of a WMD. On the other hand, the Court opined in the dicta of *Keith*, which concerned electronic surveillance conducted by the government in connection with a plot to bomb a Central Intelligence Agency office in Michigan, that reasonableness was a flexible standard that should be adapted to the government's need.[97] The Court stated in *Keith* that "[d]ifferent standards may be compatible with the Fourth Amendment if they are *reasonable* both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[98] Although *Keith* involved an American political group and not foreign powers and their agents,[99] it was followed by decisions of the Courts of Appeal for the Third, Fourth, Fifth, and Ninth Circuits, each of which found a foreign intelligence exception to the Fourth Amendment's warrant requirement.[100] When that question was presented to the Foreign Intelligence Surveillance Court of Review, the special Article III appellate court established by Congress to review foreign intelligence collection by the executive branch, the FISA Court of Review explicitly stated that while "threat to society is not dispositive in determining whether a search or seizure is reasonable, it *certainly remains a crucial* factor."[101]

Determining that a programmatic[102] need to address foreign national security threats can support a foreign intelligence exception to the Fourth Amendment's

---

have diminished expectations of privacy); United States v. Biswell, 406 U.S. 311, 315–16 (1972) (discussing a business fully aware of the pervasive regulation in their field and thus having a reduced expectation of privacy).

95. Vernonia Sch. Dist. 47J v. Acton, 515 U.S 646, 652 (1995).

96. *Id.* at 652–53 (quoting Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989)); *see also supra* note 66 and accompanying text.

97. United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297 (1972). The case is known as *Keith* because the government filed a writ of mandamus against the Honorable Damon Keith, United States District Court Judge, when he ordered the government to disclose wiretapping information.

98. *Id.* at 322–23 (emphasis added).

99. *Id.* at 321–22.

100. United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973). *But see* Zweibon v. Mitchell, 516 F.2d 594, 613–14 (D.C. Cir. 1975) (en banc).

101. *In re* Sealed Case, 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002) (emphasis added).

102. *E.g.*, *In re* Directives Pursuant to Section 105B of the Foreign Intelligence

warrant requirement, however, does not provide strong precedent for the notion that the gravity of the offense permits the government to target an indeterminate number of communication devices in the United States in response to a specific, intelligence-driven WMD threat. Yet more than sixty years ago (and three years before he issued his seminal concurring opinion in the *Steel Seizure* case)[103], Supreme Court Justice Robert Jackson planted the seeds of the principle that consequence could be a factor in determining whether or not to relax the probable cause requirement. In *Brinegar v. United States*,[104] the defendant was prosecuted for illegally importing liquor into Oklahoma from Missouri, and his conviction was based, in part, on the use of evidence seized from his automobile.[105] Prior to trial, Brinegar moved to suppress the evidence, and the Court held that there was probable cause to search his automobile.[106] In his dissent, Justice Jackson expressed concern that the Fourth Amendment's automobile exception[107] was being taken as "blanket authority to stop and search cars on suspicion"[108]; that is, without probable cause. Justice Jackson then suggested that the gravity of the offense should be considered in certain circumstances.[109] He spoke specifically to the issue of indiscriminate searches performed by police officers:

> [I]f we are to make judicial exceptions to the Fourth Amendment . . . , it seems to me they *should depend* somewhat upon the *gravity of the offense*. If we assume, for example, that a child is kidnapped and the officers throw a roadblock about the neighborhood and search *every outgoing car*, it would be a drastic and undiscriminating use of the search. The officers might be unable to show probable cause for searching any particular car. However, I should candidly strive hard to sustain such an action, executed fairly and in good faith, because it might be reasonable to subject travelers to that indignity if it was the

---

Surveillance Act, 551 F.3d 1004, 1011–12 (Foreign Int. Surv. Ct. Rev. 2008) (stating that the programmatic purpose of FISA collection is a "legitimate objective beyond ordinary crime control"). It should be noted that in 2008, Congress amended FISA and expanded the definition of "foreign power" and agents thereof to include an "entity not substantially composed of United States persons" or "any person other than a United States person" who is "engaged in the international proliferation of weapons of mass destruction." Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 110-261, 1222 Stat. 2436 (codified as amended at 50 U.S.C. §§ 1801(a)(7), (b)(1)(E)) (2008). This 2008 amendment, however, does not solve the issue posed by the hypothetical because, unlike the hypothetical, FISA requires that when the government seeks to target communications devices in the United States, it must target a *specific* communications device or facility. *See* 50 U.S.C. § 1805(a)(2)(B) (2012) (stating probable cause is required with respect to "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used by a foreign power or agent of a foreign power").

103. *See* Youngstown Sheet & Tube Co. v. Sawyer (*Steel Seizure*), 343 U.S. 579, 634–55 (1952) (Jackson, J., concurring).

104. 338 U.S. 160 (1949).

105. *Id.* at 161–62.

106. *Id.* at 177–78.

107. The automobile exception was first articulated by the Supreme Court twenty-four years earlier in *Carroll v. United States*, 267 U.S. 132, 151–53 (1925).

108. 338 U.S. at 183 (Jackson, J., dissenting).

109. *Id.*

> *only way* to save a threatened life and detect a vicious crime. But I should not strain to sustain such a roadblock and universal search to salvage a few bottles of bourbon and catch a bootlegger.[110]

More than three decades later, the Supreme Court referenced gravity of the offense in a number of cases discussing the Fourth Amendment. In *Mincey v. Arizona*,[111] the Court was confronted with a case in which, after arresting the defendant for shooting a police officer, the police had conducted a four-day warrantless search of the defendant's apartment.[112] In *Mincey*, the Court rejected the notion that gravity of the offense was sufficient to justify the warrantless search when it explicitly rejected a murder-scene exception to the warrant requirement.[113] However, in *Welsh v. Wisconsin*,[114] decided six years later, the Court seems to have taken a different view. In *Welsh*, the police had gained entry into a home without a warrant in connection with their investigation of a car accident.[115] Writing for the majority, Justice William Brennan stated that "an *important factor* to be considered when determining whether any exigency exists is the *gravity of the underlying offense* for which the arrest is being made."[116] Six months after *Welsh* was decided, Justice John Paul Stevens observed in another case that "a standard that varies the extent of the permissible intrusion with the *gravity of the suspected offense* is . . . consistent with common-law experience and this Court's precedent"[117] and was almost "too clear for argument."[118] Indeed, later that year, the Court recognized a crime-severity distinction in *Tennessee v. Garner*[119] when it held that the use of deadly force was reasonable in self-defense or when there was "probable cause to believe that [the suspect] has committed a crime involving the infliction or threatened infliction of *serious* physical harm."[120]

Fifteen years later, two cases reached the Supreme Court in which the Court alluded to the issue of whether there should be different Fourth Amendment standards for grave threats. At issue in *City of Indianapolis v. Edmond*[121] was a

---

110. *Id.* (emphasis added). Arguably the seed was planted by Justice Jackson six months earlier. *See* McDonald v. United States, 335 U.S. 451, 459–60 (1948) (Jackson, J., concurring) ("Whether there is reasonable necessity for a search without waiting to obtain a warrant certainly depends somewhat upon *the gravity of the offense* thought to be in progress as well as the hazards of the method of attempting to reach it." (emphasis added)).

111. 437 U.S. 385 (1978).

112. *Id.* at 388–89.

113. *Id.* at 390.

114. 466 U.S. 740 (1984).

115. *Id.* at 742–43.

116. *Id.* at 753 (emphasis added).

117. New Jersey v. T.L.O., 469 U.S. 325, 378–79 (1985) (Stevens, J., concurring in part and dissenting in part) (emphasis added).

118. *Id.* at 380.

119. 471 U.S. 1 (1985).

120. *Id.* at 11 (emphasis added). Jeffrey Bellin has concluded that *Garner* provides "doctrinal support" for the principle that "[a]s a matter of Fourth Amendment reasonableness, crimes involving the threat of serious physical harm warrant more intrusive government responses than crimes that do not." Bellin, *supra* note 24, at 32.

121. 531 U.S. 32 (2000).

drug interdiction checkpoint that had been established by law enforcement authorities. After reviewing a series of decisions that involved suspicionless roadblocks and checkpoints, including the border search and drunk-driving roadblock cases, the Court stated that the "*gravity of the threat alone* cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose."[122] Although combatting illegal narcotics trafficking was a "social harm[] of the first magnitude,"[123] it did not reach the level that warranted a relaxation of the Fourth Amendment's individualized suspicion (probable cause) requirement. Since the primary purpose of the drug interdiction checkpoint was indistinguishable from a "general interest in crime control," the checkpoint ran afoul of the Fourth Amendment.[124] Notably, however, in a statement remarkably reminiscent of Justice Jackson's dissent in *Brinegar*, Justice Sandra Day O'Connor, writing for the majority of the Court, stated that "the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an *imminent terrorist attack* or to catch a dangerous criminal who is likely to flee by way of a particular route."[125]

The second case decided by the Supreme Court in 2000 that alluded to circumstances involving a grave offense was *Florida v. J.L.*,[126] a stop and frisk case. In *J.L.*, the police received an anonymous tip that a "young black male standing at a particular bus stop and wearing a plaid shirt was carrying a gun."[127] When the police responded to the location, they observed three individuals, one of whom was wearing a plaid shirt.[128] Apart from the tip, the police had no reason to suspect illegal conduct by any of the individuals.[129] Nonetheless, the police stopped the individuals, frisked them, and discovered a firearm.[130] The Court held that the tip lacked sufficient indicia of reliability and was not, without more, sufficient to justify a police officer's stop and frisk.[131] The Court noted that the tip "provided no predictive information and therefore left the police without means to test the informant's knowledge or credibility."[132] Although the Court stated that "[f]irearms are dangerous, and *extraordinary dangers sometimes justify* unusual precautions,"[133] it declined to adopt a firearm exception under which a tip alleging an illegal gun would justify a stop and frisk. The majority then went on to state the following in regard to a circumstance where there might be an extraordinary danger, such as a report of a person carrying a bomb: "The facts of this case do not

---

122. *Id.* at 42 (emphasis added).
123. *Id.*
124. *Id.* at 44.
125. *Id.* (emphasis added). *But see* Atwater v. City of Lago Vista, 532 U.S. 318, 347–50 (2001) (rejecting a distinction between minor and other crimes when determining whether warrantless arrests are permissible).
126. 529 U.S. 266 (2000).
127. *Id.* at 268.
128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.* at 271–74.
132. *Id.* at 271.
133. *Id.* at 272 (emphasis added).

require the Court to speculate about the circumstances under which the danger alleged in an anonymous tip *might be so great* as to justify a search even without a showing of reliability."[134]

In the past decade, two Supreme Court decisions have referenced gravity of the offense as a potential factor in a Fourth Amendment calculus. In *Illinois v. Lidster*,[135] the Court addressed the issue of whether brief stops of motorists at highway checkpoints, which were designed to enable the police to obtain information about a recent fatal hit-and-run accident, were presumptively unreasonable. After reviewing its decision in *Edmond*, the Court noted that brief information-seeking highway stops were "less likely to provoke anxiety or to prove intrusive,"[136] and that in judging reasonableness, courts should also "look to 'the *gravity* of the public concerns served by the seizure, [and] the degree to which the seizure advances the public interest.'"[137]

If the seeds of the gravity of the offense principle were planted by Justice Jackson in *Brinegar* and were watered by Justice O'Connor in *Edmond*, then they were surely nourished by the Supreme Court in its recent decision in *United States v. Jones*.[138] *Jones* involved the question of whether the attachment of a GPS tracking device to an individual's vehicle, and the subsequent use of that device to monitor the vehicle's movements on the public street by the government, constituted a search.[139] Writing for the majority, Justice Scalia concluded that the installation of the GPS device constituted a trespass and therefore was a search within the meaning of the Fourth Amendment.[140] Notably, however, Justice Samuel Alito, writing for three other Justices and concurring in the judgment of the Court, stated that "the use of longer term GPS monitoring in investigations of *most offenses* impinges on expectations of privacy, . . . [and the Court] need not consider whether prolonged GPS monitoring in the context of investigations involving *extraordinary offenses* would similarly intrude on a constitutionally protected sphere of privacy."[141]

---

134. *Id.* at 273 (emphasis added).

135. 540 U.S. 419 (2004).

136. *Id.* at 425.

137. *Id.* at 427 (emphasis added) (quoting Brown v. Texas, 443 U.S. 47, 51 (1979)). Notably, in his dissent in *Illinois v. Caballes*, a case involving a narcotics-detection dog who altered as to the presence of marijuana in an automobile, Justice David Souter pointed out that the Court should not

> prejudge a claim of authority to detect explosives and dangerous chemical or biological weapons that might be carried by a terrorist who prompts no individualized suspicion. Suffice it to say here that what is a reasonable search depends in part on demonstrated risk. Unreasonable sniff searches for marijuana are not necessarily unreasonable sniff searches for destructive or deadly material *if suicide bombs are a societal risk.*

543 U.S. 405, 417 n.7 (2005) (Souter, J., dissenting) (emphasis added).

138. 132 S. Ct. 945 (2012).

139. *Id.* at 948.

140. *Id.* at 950 n.3 ("Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, [a Fourth Amendment] search has undoubtedly occurred.").

141. *Id.* at 964 (Alito, J., concurring) (emphasis added) (internal quotation marks omitted).

Justice Alito's concurring opinion prompted Justice Scalia to write that Fourth Amendment distinctions based on the nature of the offense would introduce a "novelty into our jurisprudence" because "[t]here is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated."[142] However, Justice Alito's view was shared by Justices Ruth Bader Ginsburg, Stephen Breyer, and Elena Kagan. Moreover, it was explicitly accepted by Justice Sonia Sotomayor. In her concurring opinion, Justice Sotomayor wrote that she "*agree[d]* with Justice ALITO that, at the very least, longer term GPS monitoring in investigations of *most offenses* impinges on expectations of privacy."[143] Thus, although Justice Scalia delivered the opinion of the Court, the fact that five Justices have recently expressed the view that the Fourth Amendment should treat *most* offenses similarly, as opposed to *all* offenses, suggests that those Justices might agree with the central thesis of this Article—namely, that the Fourth Amendment should treat grave offenses differently, particularly when the government is trying to *prevent* massive destruction or the catastrophic loss of life.

In the state courts, perhaps the most notable decision to express the view that gravity of future harm could justify a warrantless search on less than probable cause was *People v. Sirhan*.[144] After Senator Robert F. Kennedy was assassinated, law enforcement officers in Los Angeles, California, believed that there might be a conspiracy afoot to kill other prominent government leaders, and they concluded that they needed to take "prompt action."[145] In upholding the warrantless search of the room occupied by Sirhan, who was later convicted of assassinating Senator Kennedy, the California Supreme Court took note of the gravity of the offense and the "effect on this nation if several more political assassinations had followed that of Senator Kennedy."[146] The court then upheld the warrantless search, even though there was only a "mere possibility" that there might be evidence.[147]

Prior to *Jones*, the admittedly fleeting references to the role that gravity of the offense should play in a Fourth Amendment calculus prompted Jeffrey Bellin to observe that "[t]he bulk of Fourth Amendment doctrine is transsubstantive, either

---

142. *Id.* at 954. The majority refrained from "rushing forward" to resolve this issue, which it called "thorny" and "vexing." *Id. But cf.* Maryland v. King, 133 S. Ct. 1958, 1980 (2013) (approving the use of DNA testing as a post-arrest booking procedure for "serious" offenses).

143. 132 S. Ct. at 955 (Sotomayor, J., concurring) (emphasis added).

144. 497 P.2d 1121 (Cal. 1972).

145. *Id.* at 1138–40.

146. *Id.* at 1140.

147. *Id.* Other state supreme courts have also discussed how the nature of the offense affects Fourth Amendment questions. *E.g.*, Butler v. State, 829 S.W.2d 412, 414–15 (Ark. 1992) (noting "an important factor to be considered when determining whether any exigency exists is the gravity of the underlying offense for which the arrest is being made."); People v. Miller, 773 P.2d 1053, 1057 (Colo. 1989) (looking to whether "a grave offense is involved, particularly in a crime of violence" when determining whether sufficient exigency exists to justify a warrantless search of a home); Commonwealth v. Roland, 637 A.2d 269, 270 (Pa. 1994) (acknowledging that the gravity of the offense is a factor in determining whether exigent circumstances exist to justify a warrantless search); State v. Smith, 199 P.3d 386, 389 (Wash. 2009) (explaining that circumstances may be exigent if they satisfy a "totality of the situation" test which includes a factor described as "the gravity or violent nature of the offense with which the suspect is to be charged").

by virtue of the Supreme Court's explicit rejection of crime severity as a valid Fourth Amendment consideration, or the Court's pointed omission of that consideration from its analysis."[148] On the other hand, in his multivolume Fourth Amendment treatise, Wayne R. LaFave says that it is "tempting to conclude that the seriousness of the offense should be a factor in the probable cause equation, and that therefore this sub rosa practice of taking the offense into account should be recognized and legitimated."[149] Carol Steiker echoes that sentiment, stating that such an approach may be precisely what the Framers had intended through the use of the term *un*reasonable.[150] Akil Amar has written that it makes "intuitive sense to police officials and citizens alike: serious crimes and serious needs can justify more serious searches and seizures."[151] Amar further says that "[i]t would make little sense to insist on the same amount of probability regardless of the imminence of the harm, the intrusiveness of the search, the reason for the search, and so on."[152]

Ric Simmons believes that suspicionless searches in areas where individuals do not have diminished expectations of privacy could be upheld if the government simply agreed to forgo the use of the fruits of the searches in other prosecutions.[153] While this bright-line rule[154] clearly has merit, and the fact that an aggrieved person[155] could

---

148. Bellin, *supra* note 24, at 17.

149. 2 LAFAVE, *supra* note 29, § 3.2(a), at 38. Gravity of the harm was considered to be an important factor by the drafters of the Model Code of Pre-Arraignment Procedure that was proposed in 1975. *See* 3 LAFAVE, *supra* note 29, § 6.5(d), at 576 (summarizing section 260.5 of the 1975 Model Code of Pre-Arraignment Procedure "to the effect that a warrantless search of premises may be undertaken upon reasonable cause to believe that premises contain . . . things immediately likely to burn, explode, or otherwise cause death, serious bodily harm, or substantial destruction of property").

150. Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 824 (1994) (noting that unreasonable "positively invites constructions that change with changing circumstances"); *see also* Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The Fourth Amendment does not proscribe all [government-initiated] searches and seizures; it merely proscribes those which are unreasonable.").

151. Amar, *supra* note 24, at 802; *see also* Simmons, *supra* note 13, at 895 ("[I]f police have twenty-four hours to find an atomic bomb that they know is hidden in one of a hundred houses, it would be reasonable for them to conduct suspicionless searches of each of those houses."). *Cf.* Bellin, *supra* note 24, at 6 (arguing that judges should "incorporate the severity of the crime being investigated into determinations of constitutional reasonableness . . . [to] grant the government more leeway in investigations of the gravest offenses, while simultaneously enabling concrete limits on investigations of minor crimes"); Gould & Stern, *supra* note 24, at 777, 819–23 (2004) ("[T]raditional [Fourth Amendment] doctrine falls short in an age of threats unprecedented in their potential for harm."); Stuntz, *supra* note 24, at 875 (discussing how "some crimes are worse than others . . . [and] the worst crimes are the most important ones to solve, the ones worth paying the largest price in intrusions on citizens' liberty and privacy").

152. Amar, *supra* note 24, at 784.

153. Simmons, *supra* note 13, at 916.

154. *Id.* at 884–88.

155. FISA defines an "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k) (2012). Title III defines an "aggrieved person" as "a person who was a party to any intercepted wire, oral, or electronic communication or a

bring a civil rights lawsuit pursuant to 42 U.S.C. § 1983 might serve as an ex ante check on the government's conduct,[156] these approaches do not, by themselves, sufficiently protect privacy. Moreover, as discussed in Part III, there are serious definitional issues that need to be resolved by the political branches of government, and failing to resolve those issues could lead, as Owen Fiss fears, to "great abuse,"[157] which could end up proving the adage that "hard cases make bad law."[158]

At the same time, any potential solution to the hypothetical must be workable and address the administrability concerns raised by the Supreme Court.[159] Moreover, the solution must be sufficiently flexible to enable the executive branch to respond to dynamic and potentially unpredictable circumstances.[160] Government officials who are responsible for protecting the nation from terrorists seeking to cause massive destruction or a catastrophic loss of life need greater ex ante certainty that their preventative actions are constitutional.[161] Thus, if there is to be a

---

person against whom the interception was directed." 18 U.S.C. § 2510(11) (2012).

156. *See* Bivens v. Six Unknown Agents of the Fed. Bureau of Narcotics, 403 U.S. 388, 397 (1971) (holding that "petitioner is entitled to recover money damages for any injuries he has suffered as a result of the agents' violation of the [Fourth] Amendment"). However, the Court's statement that "no special factors counseling hesitation" were present, *id.* at 396, has led some lower courts to carve out exceptions related to national security. *See* Meshal v. Higgenbotham, No. 1:09–2178 (EGS), 2014 WL 2648032, at *12 (D.D.C. 2014) ("Under *Lebron [v. Rumsfeld*, 670 F.3d 540 (4th Cir. 2012)], *Doe [v. Rumsfeld*, 683 F.3d 390 (D.C. Cir. 2012)], and *Vance [v. Rumsfeld*, 701 F.3d 193 (7th Cir. 2012)], . . . when a citizen's rights are violated in the context of military affairs, national security, or intelligence gathering *Bivens* is powerless to protect him."). As a result, Steve Vladeck has concluded that there is a "vanishingly small set of challenges to national security policies that will be justiciable." Stephen I. Vladeck, *The New National Security Canon*, 61 AM. U. L. REV. 1295, 1328 (2012).

157. *See* Fiss, *supra* note 27, at 29.

158. Northern Sec. Co. v. United States, 193 U.S. 197, 400 (1904) (Holmes, J., dissenting).

159. *E.g.*, Atwater v. City of Lago Vista, 532 U.S. 318, 347 (2001) (noting that the Fourth Amendment needs "to be applied on the spur (and in the heat) of the moment" and that there is an "essential interest in readily administrable rules"); Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981) (suggesting police need "workable rules"); *see* Bellin, *supra* note 24, at 21 ("[T]he few commentators who squarely address the subject sketch in exceedingly broad strokes, ultimately failing to address the Supreme Court's administrability concern.").

160. *See* Kevin Johnson, *Mueller's Doomsday Scenario: Attack on Aircraft*, USA TODAY, Aug. 23, 2013, at 5A (discussing the substantial challenges faced by the FBI including the "unpredictable nature of attackers acting alone"); *see also* Stew Magnuson, *FBI Anticipates Terrorist Attacks on Soft Targets in the United States*, NAT'L DEF. MAG., May 2011, at 14 ("Soft targets are now a priority for terrorists determined to inflict damage in the United States."); Scott Stewart, *The Persistent Threat to Soft Targets*, STRATFOR GLOBAL INTELLIGENCE (July 26, 2012, 4:04 AM), http://www.stratfor.com/weekly/persistent-threat-soft-targets (discussing the evolving paradigm shift by terrorists from "hard" to "soft" targets).

161. *See* James A. Baker, Constitution Day Address at the Dickinson College Clarke Forum for Contemporary Issues: National Security and the Constitution (Sept. 12, 2013), at 9, *available at* http://clarke.dickinson.edu/wp-content/uploads/Dickinson-Constitution-Day-Talk-12-Sept-2013.pdf ("Our surveillance and privacy laws need an overhaul. For example, it is often still too difficult to figure out what is lawful and what is not. This negatively impacts both intelligence collection and privacy protection. Out of confusion, lawyers can say no when they should say yes, and yes when they should say no.").

solution to the no-win scenario, it must include additional principles and measures beyond the previous discussions. As discussed below, a deep dive into the Fourth Amendment's particularity requirement and minimization principles suggests a constitutional foundation upon which a new doctrinal solution to the hypothetical can be constructed.

3. The Particularity Requirement

As discussed earlier in the context of court-authorized wiretaps, particularity requires the judicial branch to approve the specific communications that the government may lawfully acquire.[162] Yet, the Supreme Court has upheld a wiretap order that permitted the government to acquire virtually *every* communication that was taking place on a lawfully targeted device.[163] How can we square that result with the particularity requirement? The answer lies in how courts apply minimization principles to the government's conduct.

When the government obtains the contents of telephone or e-mail communications, its conduct can be divided into three stages: the acquisition stage, which refers to the stage when the government obtains the communications in the first instance either through a monitoring or a recording device; the retention stage, which refers to the government's ability to keep the communications it has initially obtained; and the dissemination stage, which refers to the government's ability to share the communications.[164] Minimization requires the government to reduce—to minimize—the amount of irrelevant information that it acquires, retains, and disseminates.[165] For example, if the government was to target a suspected spy's telephone, the government could acquire all of the communications that took place on that telephone, including when the spy's wife used the telephone. If the government concludes that the spy's wife is not involved in her husband's clandestine intelligence activities, then the wife's communications (though lawfully acquired) should be destroyed, as well as the spy's communications that are irrelevant to his spying activities.[166] Thus, minimization is typically viewed as a back-end requirement because, even though the executive branch may have taken "great care"[167] when it initially acquired the communications, its conduct would

---

162. *See* Berger v. New York, 388 U.S. 41, 56–57 (1967).

163. *See* Scott v. United States, 436 U.S. 128, 141–43 (1978).

164. *See* 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 9:1 (2d ed. 2012).

165. S. REP. NO. 90-1097, at 69 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2192–93. This minimization requirement has become an integral part of Title III. *See* 18 U.S.C. § 2518(5) (2012). *See generally* 1 KRIS & WILSON, *supra* note 164, § 9:1, at 321–22 ("Minimization governs the implementation of electronic surveillance and physical searches to ensure that they conform to their authorized purpose and scope, and requires the government to 'minimize' the amount of irrelevant information that it acquires, retains, and disseminates.").

166. S. REP. NO. 95-604, at 38 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3939.

167. *See* Katz v. United States, 389 U.S. 347, 354 (1967) (observing that the agents took "great care" to only overhear Katz's conversations in the phone booth).

nonetheless run afoul of the Fourth Amendment if it did not "minimize[] unwarranted intrusions of privacy."[168]

The leading Supreme Court case to address minimization is *Scott v. United States*.[169] In *Scott*, government agents were authorized to intercept virtually *all* of the telephone conversations that were made to or from a particular telephone.[170] Although the supporting affidavits in *Scott* named nine individuals involved in a narcotics conspiracy, the district court authorized the government to intercept the communications of those nine persons as well as "*other* persons [who] may make use of the facilities."[171] After the wiretap ended, twenty-two persons were arrested and before the trial, the defendants moved to suppress the evidence.[172] Among other things, the defendants argued that the government failed to comply with its minimization obligations since the government intercepted virtually all of the communications but only minimized 40 percent of them.[173]

In analyzing the reasonableness of the government's conduct, the Supreme Court emphasized in *Scott* that it was important to consider the circumstances of the wiretap.[174] The Court then noted that there should be no "inflexible rule," and that "when an investigation is focusing on a widespread conspiracy, *more extensive surveillance may be justified* in an attempt to determine the precise scope of the enterprise."[175] For example, the Court noted that in the early stages of surveillance the government may need "to intercept *all calls* to establish categories of nonpertinent calls which will not be intercepted thereafter."[176]

Scott was not the first case in which the Supreme Court observed that minimization should be calibrated to the nature of harm being investigated. The Court had noted in *Keith* that national security surveillance is "often long range and involves the interrelation of various sources and types of information."[177] Thus, since some telephone calls may be ambiguous or involve guarded or coded language, the Court concluded in *Scott* that it would not be *un*reasonable under certain circumstances to intercept "*almost every short conversation* because the determination of relevancy cannot be made before the call is completed."[178] The federal courts of appeals have also observed that, as long as the government makes a "good faith effort to minimize . . . irrelevant information," there is no prohibition

---

168. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) (In executing warrants that authorize "the 'seizure' of telephone conversations . . . responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.").

169. 436 U.S. 128 (1978).

170. *Id.* at 130.

171. *Id.* at 131 (emphasis added).

172. *Id.* at 132.

173. *Id.*

174. *Id.* at 140.

175. *Id.* at 139–40 (emphasis added).

176. *Id.* at 141 (emphasis added).

177. United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 322 (1972).

178. Scott v. United States, 436 U.S. at 141 (emphasis added).

on the retention of "innocuous" communications that "may later turn out to be of great significance."[179]

The legislative branch has also previously concluded that the Fourth Amendment can tolerate the acquisition of irrelevant and even innocent communications in certain circumstances. At the time FISA was enacted in 1978, the House Permanent Select Committee on Intelligence (HPSCI) noted in its report that the executive branch should not be required to make an "instantaneous identification" of communications that may contain valuable foreign intelligence information.[180] Moreover, HPSCI stated in its report that there could be circumstances where the government may retain the communications of "*innocent* persons" to identify other individuals who may be involved in a wide-ranging and clandestine conspiracy that threatens the national security of the United States.[181] Finally, HPSCI stated in its report a view that was shared by the Senate Select Committee on Intelligence (SSCI)—namely, that in certain investigations, there could very well be "technological reasons" that would prevent minimization at the acquisition stage.[182] Thus, as HPSCI and SSCI noted in each of their reports, in some cases, "it may not be *possible or reasonable* to avoid acquiring *all conversations*."[183]

The foregoing discussion shows that both the legislative and the judicial branches have concluded that the Fourth Amendment can tolerate the acquisition of all communications in certain circumstances provided that minimization takes place on the back end. Minimization principles therefore provide "sufficient latitude to meet Fourth Amendment particularity requirements."[184] Observing that these two branches have viewed minimization as a constitutionally acceptable method of balancing competing Fourth Amendment interests suggests the potential for a new

---

179. United States v. Hammoud, 381 F.3d 316, 334 (4th Cir. 2004). Indeed, as the Court of Appeals for the Second Circuit has noted, Fourth Amendment reasonableness requires that the intrusion on privacy be weighed against the "government's surveillance needs." *See In re* Terrorist Bombings, 552 F.3d 157, 175 (2d Cir. 2008) ("Our balancing of these compelling, and competing, interests turns on whether the scope of the intrusion here was justified by the government's surveillance needs."). After examining a number of minimization factors, the Court found that the interception of all communications with an alleged terrorist was reasonable under the Fourth Amendment because even though privacy intrusion may have been "great, the *need* for the government to so intrude was *even greater*." *Id.* at 176 (emphasis added).

180. H.R. REP. NO. 95-1283, pt. 1, at 58 (1978) (advising that it is permissible to retain and to a limited extent disseminate information in "bits and pieces before their full significance becomes apparent"); *see also* 1 KRIS & WILSON, *supra* note 164, § 11:10, at 414 ("[U]nder FISA depending on the case, the recording devices may or may not be left on, and minimization occurs, among other places, in the process of indexing and logging the pertinent communications.").

181. H.R. REP. NO. 95-1283, pt.1, at 58 (approving the acquisition and retention of the communications of a "large number of innocent persons . . . at least until it is determined that they are not involved in the clandestine intelligence activities").

182. *Id.* at 55 ("[I]n many cases, it may not be possible for technical reasons to avoid acquiring all communications."); S. REP. NO. 95-701, at 40 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4009 (noting the technological impossibility of acquiring all situations).

183. H.R. REP. NO. 95-1283, pt. 1, at 56 (emphasis added). *Accord* S. REP. NO. 95-701, at 40.

184. 1 KRIS & WILSON, *supra* note 164, § 11:6, at 408.

doctrinal solution to the no-win scenario—namely, that the Fourth Amendment's particularity requirement could be satisfied in the context of the hypothetical by moving minimization from the back end to the front end. In other words, in certain circumstances, post-interception minimization could satisfy what would normally be a pre-interception particularity requirement.

The question, however, is whether such a "marginal adjustment"[185] should be made every time the government seeks to prevent a potentially grave consequence, or only in a limited and carefully delineated[186] set of catastrophic consequences. Here, our hypothetical looks at the threatened use of a WMD. Part II will therefore provide an overview of four different types of WMDs and the different consequences that can be reasonably anticipated from their respective use.

II. WEAPONS OF MASS DESTRUCTION

In May 2010, President Barack Obama stated in a national security strategy report that there was "no greater threat to the American people than weapons of mass destruction, particularly the danger posed by the pursuit of nuclear weapons by violent extremists and their proliferation to additional states."[187] Although some believe that terrorists may be more focused on the acquisition and use of conventional weapons rather than WMDs,[188] one expert has identified a number of reasons why a violent extremist group may wish to use a WMD, including: (a) the psychological impact that such a weapon would have on the American public; (b) the economic, political, and social instability that would reasonably be expected to follow the use of a WMD; (c) the physical destruction that could be caused to critical infrastructure, loss of life, and contamination to vital areas; (d) the "state-like" prestige that a terrorist group perceives it would receive from the use of a WMD; (e) a "fetishistic predisposition" toward the use of a WMD; (f) defensive aggression if the group perceived its own destruction was imminent; or (g) the group's need to outdo destruction that was caused by another group.[189] Terrorists who are motivated by religious beliefs and seek

185. *See* RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF EMERGENCY 1 (2006) (explaining "the marginal adjustments in [constitutional] rights that practical-minded judges make when the values that underlie the rights—values such as personal liberty and privacy—come into conflict with values of equal importance, such as public safety, suddenly magnified by the onset of a national emergency").

186. *See, e.g.*, Katz v. United States, 389 U.S. 347, 357 (1967).

187. EXEC. OFFICE OF THE PRESIDENT, NATIONAL SECURITY STRATEGY 4 (2010), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf. Former President George W. Bush issued a similar warning in 2002. *See* EXEC. OFFICE OF THE PRESIDENT, NATIONAL SECURITY STRATEGY at v (2002), *available at* www.state.gov/documents/organization/63562.pdf ("The gravest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination.").

188. *See* Rachel Oswald, *Despite WMD Fears, Terrorists Still Focused on Conventional Attacks*, GLOBAL SECURITY NEWSWIRE (Apr. 17, 2013), http://www.nti.org/gsn/article/despite-wmd-fears-terrorists-still-focused-conventional-attacks/.

189. *See Nuclear Terrorism Hearing*, *supra* note 3, at 2–3 (statement of Gary Anthony

"fundamental changes in the existing order" may also be far more willing to engage in "large-scale violence" and attacks involving mass casualties.[190]

Any discussion concerning the threatened use of a WMD, however, needs to take into account that WMDs "differ sharply in character and in their effects."[191] Indeed, one expert cautions that there are "broad differences in the lethality of each type of weapon," and contrary to conventional wisdom, "[t]here is no reason to assume that [the] effect[] of [a] WMD should be measured in terms of mass casualties or mass destruction."[192] In June of 2009, the Department of Defense adopted the following definition of a WMD: "chemical, biological, radiological, and nuclear weapons capable of a high order of destruction or mass casualties."[193] Accordingly, in order to provide a baseline for a discussion about WMDs, Part II focuses on chemical, biological, radiological, and nuclear weapons, as well as the anticipated consequences that could flow from the use of each of these weapons.[194]

A. Chemical Weapons

Chemical weapons are some of the oldest weapons to be considered weapons of mass destruction.[195] For example, toxic fumes were reportedly used as a weapon in India as far back as 2000 BC.[196] It was the scientific revolution of the late nineteenth century, however, that gave chemicals the potential to become major weapons of war.[197]

Chemical weapons may exist as solids, gases, or liquids and their effects can be immediate and deadly. For example, through breathing, ingestion, or skin contact, chemical weapons can adversely affect the nervous system and the blood system,

---

Ackerman, Research Director, National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland).

190. *See* BRUCE HOFFMAN, INSIDE TERRORISM 94–95 (1998).

191. ANTHONY H. CORDESMAN, TERRORISM, ASYMMETRIC WARFARE, AND WEAPONS OF MASS DESTRUCTION: DEFENDING THE U.S. HOMELAND 97 (2002).

192. *Id.*

193. W. SETH CARUS, NATIONAL DEFENSE UNIVERSITY CENTER FOR THE STUDY OF WEAPONS OF MASS DESTRUCTION, DEFINING "WEAPONS OF MASS DESTRUCTION" 1–2 (2012), *available at* http://ndupress.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccationalPaper-8.pdf (citing Joint Publication 3–40, *Combating Weapons of Mass Destruction* (Washington, DC: Joint Chiefs of Staff 2009)).

194. The cybersecurity risks facing the nation have been described in ominous tones by current and former high-ranking government officials. *See* Glick, *supra* note 26, at 101–02 (describing how "a major cyber attack could shut down our Nation's most critical infrastructure: our power grid, telecommunications, [and] financial services." (alteration in original) (citations omitted)); *see also* Bill Gertz, *Inside the Ring: New WMD Threats*, WASH. TIMES, Oct. 11, 2012, at A09 ("A Pentagon-sponsored report warns that the United States faces new threats from mass destruction weapons in the form of cyber, electronic and financial attacks, in addition to more well-known dangers from nuclear, chemical and biological WMD arms."). These risks may very well lead policymakers to conclude that legislative changes are also needed to address cyber weapons.

195. Markus Binder & Michael Moodie, *Jihadists and Chemical Weapons*, *in* JIHADISTS AND WEAPONS OF MASS DESTRUCTION 131, 131 (Gary Ackerman & Jeremy Tamsett eds., 2009).

196. *Id.*

197. *Id.*

which can lead to choking or blisters.[198] Blister agents, such as mustard gas, are "oily liquids that inflict chemical burns on the skin or any other part of the body with which they come into contact, including the lungs if they are inhaled."[199] On the other hand, blood agents, such as cyanide, refer to chemical agents that "achieve their effects by traveling through the blood stream to sites where the agent can interfere with oxygen utilization at the cellular level."[200] Similarly, choking agents, such as chlorine, "attack the airways and cause swelling and edema in the lung tissues."[201] Nerve agents, such as sarin gas, "inhibit the function of vital enzymes in the human body," and experts consider them to be the "most widely feared category of chemical weapon because of the speed and severity of their impact."[202] Finally, incapacitating agents, which also act upon the central nervous system and affect consciousness, memory, problem solving, attention, and comprehension, generally are not lethal, and instead "disable the target personnel for hours if not days after exposure."[203]

The "effects of chemical weapons are normally seen over a smaller area [than their nuclear and biological counterparts], and they have been traditionally viewed as more effective at the tactical or operational level rather than at the strategic level."[204] Moreover, "in contrast to biological weapons, which are . . . slow-acting, the effects of exposure to chemical weapons can become apparent within minutes or at most hours of initial contact."[205] Since "[l]arge amounts of [chemical] agents are required to achieve high lethality,"[206] unless chemical weapons are being used by a nation state,[207] their strategic value for a terrorist group with limited resources may derive more from their potential to cause a psychological impact than from

198. *Id.* at 133 ("Western categorization systems separate military [chemical weapons] agents into several different categories, largely depending on how they work in the body.").

199. *Id.*

200. *Id.*

201. *Id.*

202. *Id.* at 134.

203. *Id.*

204. *Id.* at 132.

205. *Id.*

206. CORDESMAN, *supra* note 191, at 98. The most recent reported use of a chemical weapon is the alleged use of chlorine gas by the Islamic State against Iraqi security forces. *See* Loveday Morris, *Islamic State Militants Allegedly Used Chlorine Gas Against Iraqi Security Forces*, WASH. POST (Oct. 23, 2014), http://www.washingtonpost.com/world/middle_east/islamic-state-militants-allegedly-used-chlorine-gas-against-iraqi-security-forces/2014/10/23/c865c943-1c93-4ac0-a7ed-033218f15cbb_story.html?hpid=z1.

207. Two recently reported uses of chemical weapons by nation-states are the 1988 attack by former Iraqi President Saddam Hussein against the Kurdish town of Halabja and the use of chemical weapons by Syrian President Bashar al-Assad in 2012 and 2013. *See* Press Release, The White House Office of the Press Secretary, U.S. Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013, (August 30, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21; Joby Warrick, *Why Do Chemical Weapons Elicit a Different Response?*, WASH. POST, Sept. 1, 2013, at A12.

their ability to cause mass casualties, as terrorists seek to frighten populations and military units.[208]

Based on the foregoing, it is clear that while the effects that flow from the use of chemical weapons can be assessed fairly quickly, their lethality can vary if the resources and delivery mechanisms that are available are limited. As discussed below, the fact that chemical weapons vary significantly in their effects raises critical issues directly tied to how the reasonableness question in the hypothetical should be resolved.[209]

B. Biological Weapons

From smallpox to bubonic plague, humanity has faced numerous naturally occurring diseases that "evoke images of horror and suffering."[210] As a result of their "ability to cause pervasive mortality, naturally occurring diseases have been used as weapons of war and terror for thousands of years."[211]

Generally speaking, biological weapons are infectious agents that "are produced from pathogenic microorganisms or [other] toxic substances of biological origin . . . [which] are capable of disabling and/or killing people, crops, and livestock."[212] In addition to smallpox, some of the more well-known types of biological weapons include anthrax, salmonella, ebola, and ricin.[213]

In contrast to chemical weapons, which can produce immediate effects, because "most biological weapons consist of living organisms, symptoms will occur only after an incubation period that may last days to weeks."[214] Moreover, the initial symptoms from the use of biological weapons may very well appear as the "common cold or influenza and might be mistaken for a normal outbreak of infectious disease."[215] In the absence of a specific intelligence-driven threat stream or a claim of responsibility, detecting a biological terrorist attack may require reports of illness or death from a large number of persons, which can be particularly difficult to parse during the cold and flu season.[216]

The Centers for Disease Control categorize biological weapons according to lethality, dividing them into three categories. Category A agents include organisms

---

208. Binder & Moodie, *supra* note 195, at 132.

209. *See infra* Parts IV and V.

210. Cheryl Loeb, *Jihadists and Biological and Toxic Weapons*, *in* JIHADISTS AND WEAPONS OF MASS DESTRUCTION, *supra* note 195, at 153, 153.

211. *Id.*; *see also* James W. Martin, George W. Christopher & Edward M. Eitzen, Jr., *History of Biological Weapons: From Poisoned Darts to Intentional Epidemics*, *in* MEDICAL ASPECTS OF BIOLOGICAL WARFARE 1 (Zygmunt F. Dembek ed., 2007), *available at* https://www.hsdl.org/?view&did=19931.

212. Loeb, *supra* note 210, at 154.

213. *Id.* at 154–55.

214. *Id.* at 154. *See* Edward Eitzen, *Use of Biological Weapons*, *in* MEDICAL ASPECTS OF CHEMICAL AND BIOLOGICAL WEAPONS 437, 439 (Frederick R. Sidell, Ernest T. Takafuji & David R. Franz eds., 1997), *available at* http://dead-planet.net/chemical-terrorism/med_cbw/Ch20.pdf ("Very few biological agents are immediately lethal.").

215. Loeb, *supra* note 210, at 154.

216. *Id.*

that pose "a high risk to national security because they can be easily disseminated or transmitted person to person; result in high mortality rates. . . [;] have the potential for major public health impact; might cause public panic and social disruption; and require special action for public health preparedness."[217] Category B agents can lead to moderate illness rates and low death rates.[218] Lastly, Category C agents have a potential for high illness and death rates because they "could be engineered for mass dissemination."[219]

One expert has observed that some biological weapons "offer a means of attack that is potentially cheap, lethal, and hard to detect."[220] The most effective means of distributing a biological weapon is in the form of a dry or wet aerosol, which typically is a "cloud of solid particles suspended in the air."[221] Although other means of delivery may include cluster bombs, artillery shells, rockets, and sophisticated sprayers, the use of large-scale delivery systems is thought to be associated with the military development of biological weapons.[222] Other nontechnical and less expensive delivery mechanisms include human self-infection or the use of animal vectors, improvised crop-dusting airplanes, small backpack sprayers, or purse-sized atomizers.[223]

Some biological weapons can be highly inefficient because they largely depend, in the case of open air delivery mechanisms, on "meteorological and terrain conditions such as wind velocity, temperature, precipitation, and humidity."[224] Indeed, "[o]nly a small number of the hundreds of bacteria and viruses are viable as terrorist weapons; most cannot survive outside of narrow margins of temperature range or are too rare or hard to grow."[225] In addition, "[m]ost wet agents degrade quickly, although spores, dry encapsulated agents, and some toxins are persistent."[226]

Contaminating food and water supplies on a large scale would therefore pose challenges to terrorists because of the quality control processes that exist in the food supply chain. Moreover, one expert notes that terrorists who rely on biological weapons have to contend "with incremental degradation over time due to transporting materials from the point of acquisition or production to the point of use, not to mention ensuring [that] a suitably virulent strain has been properly and effectively weaponized."[227]

The effectiveness of biological weapons is also dependent on factors such as "choice of agent, type of formulation, and the manufacturing process employed."[228]

---

217. *Bioterrorism Agents/Diseases*, CTRS. FOR DISEASE CONTROL & PREVENTION, http://emergency.cdc.gov/agent/agentlist-category.asp.

218. *Id.*

219. *Id.*

220. CORDESMAN, *supra* note 191, at 139.

221. Loeb, *supra* note 210, at 156.

222. *Id.*

223. *Id.*

224. *Id.* at 157.

225. MATT LAWRENCE, WHAT TO DO 'TIL THE CALVARY COMES: A FAMILY GUIDE TO PREPAREDNESS IN 21ST CENTURY AMERICA 114 (2006).

226. CORDESMAN, *supra* note 191, at 99.

227. Loeb, *supra* note 210, at 157.

228. *Id.*

One expert cautions, however, that while many biological weapons would likely result in low mortality rates, some biological weapons could be far more lethal than chemical weapons.[229] The widespread use of certain agents, such as small pox or plague, could lead to widespread morbidity and mortality, as well as the "specter of enforced quarantine."[230] In addition, "the lack of a discreet endpoint . . . [could further] heighten the psychological effects on the targeted population."[231] Thus, biological attacks can cascade into "high-levels of anxiety, widespread fear, and perhaps even paranoia, leading to self-isolation . . . and social disruption to civil society."[232]

Based on the foregoing, it is clear that the effects that flow from the use of biological weapons cannot be assessed as quickly as the effects that flow from the use of chemical weapons, and their lethality can vary significantly depending on a variety of factors. This variation, as discussed below, raises critical issues directly tied to how the Fourth Amendment should resolve the question of what types of searches are reasonable in the face of threatened use of a biological weapon.[233]

C. Radiological Weapons

Radiological weapons, which are a relatively new category of WMDs, are weapons that contain large amounts of ionizing radiation.[234] If ingested or inhaled in sizeable amounts, ionizing radiation can lead to radiation sickness or cancer.[235] Radiological weapons can range from "crude explosive devices to sophisticated dispersal mechanisms."[236] Although radiological weapons can take many forms, one expert cautions that a radiological weapon should "not be confused with a nuclear weapon, and the effects of the two weapons differ greatly."[237] For example, radiological weapons can consist of more conventional explosives, such as dynamite, attached to some type of radioactive material.[238] However, the resulting blast from such a weapon—the so-called dirty bomb—would "do a very poor job at effectively spreading out radioactive material in ways that can do serious harm to health or result in significant radioactive contamination that is hard to clean up."[239]

One expert believes that "for most scenarios involving radiological weapons, . . . few, if any, people near the scene of an attack would succumb to serious and immediate health effects."[240] "To experience these effects, individuals would have to receive relatively high exposures of ionizing radiation[,]"[241] and even then it

---

229. CORDESMAN, *supra* note 191, at 151.
230. Loeb, *supra* note 210, at 160.
231. *Id.*
232. *Id.*
233. *See infra* Parts IV and V.
234. Charles D. Ferguson, *Radiological Weapons and Jihadist Terrorism*, *in* JIHADISTS AND WEAPONS OF MASS DESTRUCTION, *supra* note 195, at 173, 179.
235. *Id.* at 173.
236. *Id.* at 184.
237. *Id.* at 174.
238. CORDESMAN, *supra* note 191, at 194.
239. Ferguson, *supra* note 234, at 184.
240. *Id.* at 173.
241. *Id.*

could take upwards of decades for cancer to develop after exposure. Thus, while the "psychological and social consequences of a radiological attack could linger for years," a radiological weapon "cannot produce a nuclear chain reaction and will not, consequently, result in a massive explosion."[242]

The lethality of radiological weapons can therefore be indeterminate "because of the time required to accumulate a disabling or significant dose of radiation through ingestion, inhalation, or exposure."[243] On the other hand, since radiation destroys human cells, and radiation poisoning can cause untreated victims to dehydrate and bleed to death, some radiological weapons, even in minute quantities, can be deadly.[244]

Based on the foregoing, it is clear that the effects that flow from the use of radiological weapons can vary. As a result, radiological weapons may be more suitable for "terror, political, and area denial purposes, rather than for mass killings."[245] As discussed below, this raises critical issues directly tied to how the Fourth Amendment reasonableness question should be resolved.[246]

D. Nuclear Weapons

More than any other WMD that could be used by a terrorist, a nuclear weapon would "represent a 'game-changing' event far exceeding the impact of 9/11."[247] "Nuclear weapons draw their explosive force from fission, fusion, or a combination of these two methods."[248] While one expert believes that a fusion-based nuclear weapon would be "too sophisticated for fabrication" by terrorists, and while fissionable materials exist only in very minute quantities, purchasing, stealing, or otherwise obtaining highly enriched types of uranium, plutonium, or similar materials would enable terrorists with sophisticated knowledge and expertise to make an improvised nuclear device.[249]

The energy that results from a nuclear weapon is generally grouped into five effects: (1) blast effects, (2) thermal effects, (3) radiation effects, (4) electromagnetic effects, and (5) climate effects.[250] A nuclear weapon could be detonated in the air, at either low or high altitudes, underwater, underground, or on the surface of the planet.[251] Depending upon the size of the weapon (frequently

---

242. *Id.* at 174.

243. CORDESMAN, *supra* note 191, at 194.

244. Ferguson, *supra* note 234, at 185.

245. CORDESMAN, *supra* note 191, at 194.

246. *See infra* Parts IV and V.

247. *Nuclear Terrorism Hearing*, *supra* note 3, at 1 (statement of Gary Anthony Ackerman, Research Director, National Consortium for the Study of Terrorism and Responses to Terrorism).

248. Charles P. Blair, *Jihadists and Nuclear Weapons*, *in* JIHADISTS AND WEAPONS OF MASS DESTRUCTION, *supra* note 195, at 193, 195.

249. *Id.* at 195–203.

250. *See Effects of Nuclear Weapons*, NUCLEAR DARKNESS, GLOBAL CLIMATE CHANGE & NUCLEAR FAMINE: THE DEADLY CONSEQUENCES OF NUCLEAR WAR, http://www.nucleardarkness.org/nuclear/effectsofnuclearweapons/.

251. *See* John Pike, *Nuclear Weapon Effects*, FED'N OF AM. SCIENTISTS (Oct. 21, 1998, 4:35 PM), http://www.fas.org/nuke/intro/nuke/effects.htm. *See generally* SAMUEL GLASSTONE & PHILIP J. DOLAN, THE EFFECTS OF NUCLEAR WEAPONS (3d ed. 1977).

expressed in terms of kilotons and yield), the location of the blast, and the characteristics of the environment, everything in the immediate vicinity of "ground zero"[252]—the point on the Earth's surface closest to the point of a nuclear detonation—would vaporize from the initial blast.[253] A fireball would then immediately rise, expand, and cool, giving the appearance of a mushroom cloud.[254] The blast would also produce a shock wave and "vaporized matter [would] condense [into] a cloud containing solid particles of weapon debris" contaminated by radioactivity, which would disperse over a vast area.[255] A high-altitude nuclear detonation could also produce an electromagnetic pulse, resulting in a sudden burst of electromagnetic radiation that could have catastrophic and devastating effects to critical infrastructures for power, transportation, telecommunications, banking, finance, food, and water.[256]

The detonation of a nuclear WMD would, therefore, lead to short-term as well as long-term physical, health, environmental, social, and psychological effects. Those effects would be felt in varying degrees based on a number of factors, including distance from the point of the blast.[257] Since the detonation of a single nuclear weapon could produce massive destruction and loss of life on an unimaginable scale,[258] it truly qualifies as the most devastating weapon of mass destruction.

---

252. The first use of the term "ground zero" may have been in connection with the Manhattan Project and the bombing of Japan. William Laurence, a reporter embedded with the Manhattan project, reported that "Zero" was "the code name given to the spot chosen for the atomic bomb test." *See* WILLIAM L. LAURENCE, DAWN OVER ZERO: THE STORY OF THE ATOMIC BOMB 4 (1946).

253. *See Effects of Nuclear Weapons, supra* note 250; Alexander Glaser, *Effects of Nuclear Weapons*, PRINCETON U. (Feb. 12, 2007), http://www.princeton.edu/~aglaser/lecture2007_weaponeffects.pdf.

254. *See* Glaser, *supra* note 253.

255. *Id.*

256. *See* FED. ENERGY REGULATORY COMM'N, ELECTROMAGNETIC PULSE: EFFECTS ON THE U.S. POWER GRID i (2010) ("The nation's power grid is vulnerable to the effects of an electromagnetic pulse (EMP), a sudden burst of electromagnetic radiation resulting from a natural or man-made event. EMP events occur with little or no warning and can have catastrophic effects, including causing outages to major portions of the U.S. power grid possibly lasting for months or longer."). *Compare* JOHN S. FOSTER, JR., EARL GJELDE, WILLIAM R. GRAHAM, ROBERT J. HERMANN, HENRY M. KLUEPFEL, RICHARD L. LAWSON, GORDON K. SOPER, LOWELL L. WOOD, JR. & JOAN B. WOODARD, REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE (EMP) ATTACK 1 (2004) ("The electromagnetic fields produced by weapons designed and deployed with the intent to produce EMP have a high likelihood of damaging electrical power systems, electronics, and information systems upon which American society depends. Their effects on dependent systems and infrastructures could be sufficient to qualify as catastrophic to the Nation."), *with* Roscoe Bartlett, *Foreword* to MARK SCHNEIDER, NAT'L INST. FOR PUB. POL'Y, THE EMERGING EMP THREAT TO THE UNITED STATES (2007) ("A high-altitude nuclear-generated electromagnetic pulse (EMP) attack can have devastating consequences on our society by destroying the electronic systems that support our critical infrastructures for power, transportation, telecommunications, banking and finance, and food and water.").

257. *See* Glaser, *supra* note 253.

258. *See supra* notes 250–56 and accompanying text.

III. DEFINITIONAL ISSUES

At this point, it is appropriate to restate the hypothetical and further highlight why it matters that different consequences can reasonably be anticipated from the use of different WMDs. In our hypothetical, a reliable informant has told the government that a highly skilled terrorist, has entered the United States and is assembling a WMD at a safe house sometime within the next thirty to forty-five days. The government does not know the precise location of the terrorist or the specific telephone or e-mail account that is being used by him, but the informant is 80 percent certain that the safe house is located somewhere in Georgetown, fewer than two miles from the White House.[259] Finding and *preventing* the terrorist from using the WMD is clearly the paramount goal for the government.[260]

Noticeably absent from the fact pattern, however, is the specific type of WMD that is being assembled. This point is critical. As discussed in Part II, the use of different types of WMDs can lead to different consequences. This point takes on exceptional importance because a close examination of U.S. law reveals significant definitional issues. Indeed, as the Congressional Research Service has noted, the "term 'WMD' is problematic from an analytic perspective . . . [because it] implies that [these weapons] are similar even though each type differs greatly from the others in its mechanisms and effects,"[261] and because, as discussed below, the definition under U.S. law could include a more *conventional* weapon. For example, in the Violent Crime Control and Law Enforcement Act of 1994,[262] Congress defined a WMD broadly to include chemical, biological, and radiological weapons, as well as "any destructive device as defined in section 921 of this title."[263] Reference to section 921 is particularly challenging from the perspective of the hypothetical because it defines the term "destructive device" to mean:

> any explosive, incendiary, or poison gas—(i) bomb, (ii) grenade, (iii) rocket having a propellant charge of more than four ounces, (iv) missile

---

259. The Federal Emergency Management Administration has studied the truly horrifying effects that would flow from the detonation of a ten kiloton improvised nuclear device at the intersection of 16th and K Streets, NW, Washington, D.C., which is approximately a five-minute walk from Georgetown. *See* B.R. Buddenmeier, J.E. Valentine, K.K. Millage & L.D. Brandt, *Key Response Planning Factors for the Aftermath of Nuclear Terrorism*, FED. AM. SCIENTISTS (Nov. 2011), http://www.fas.org/irp/agency/dhs/fema/ncr.pdf.

260. Although assembling a WMD is also a criminal act, prosecution clearly remains the lowest priority in this scenario. *See In re* Sealed Case, 310 F.3d 717, 727 (Foreign Int. Surv. Ct. Rev. 2002) ("The government's overriding concern is to stop or frustrate the agent's or the foreign power's activity by any means, but if one considers the actual ways in which the government would foil . . . terrorism it becomes apparent that criminal prosecution analytically cannot be placed easily in a separate response category."); *see also*, Scott J. Glick, *FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security*, 1 HARV. NAT'L SEC. J. 87, 110 (2010) (noting the hybrid nature of some national security investigations).

261. *See* JONATHAN MEDALIA, CONG. RESEARCH SERV., R41890, "DIRTY BOMBS": TECHNICAL BACKGROUND, ATTACK PREVENTION AND RESPONSE, ISSUES FOR CONGRESS 3 (2011).

262. Pub. L. No. 103-322, 108 Stat. 1980 (1994).

263. 18 U.S.C. § 2332a(c)(2)(A) (2012).

> having an explosive or incendiary charge of more than one-quarter ounce, (v) mine, or (vi) device similar to any of the devices described in the preceding clauses.[264]

FISA's WMD definition adds further complexity to the discussion. Under FISA, a WMD includes "any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a *mass casualty incident*."[265] On the other hand, the Defense Against Weapons of Mass Destruction Act of 1996 uses a different measurement of consequence.[266] Instead of referencing a "mass casualty incident," this statute defines WMD as "any weapon or device that is intended, or has the capability, to cause *death or serious bodily injury to a significant number of people* through the release, dissemination, or impact of—(A) toxic or poisonous chemicals or their precursors; (B) a disease organism; or (C) radiation or radioactivity."[267]

As the foregoing discussion demonstrates, the failure of the hypothetical to specify the type of WMD is critical. While the media may understand or represent WMDs as a "monolithic menace,"[268] members of the legislative branch, as the elected representatives of the people, have an essential role to play in making "intellectually rigorous distinctions"[269] among different types of WMDs before we can assess whether, and the degree to which, consequence should matter. Once those definitional challenges are resolved, however, the question then turns to whether in a particular case, it would be reasonable to move minimization from the back end to the front end to satisfy the Fourth Amendment's particularity requirement. Part IV therefore explores an analytical framework that may be used in assessing the role of consequence in particular sets of circumstances.

---

264. 18 U.S.C. § 921(a)(4)(A)(i)–(vi) (2012). In addition to these explosive, incendiary, or poison gas devices, section 921 defines a "destructive device" to include the following: "any type of weapon (other than a shotgun or a shotgun shell which the Attorney General finds is generally recognized as particularly suitable for sporting purposes) by whatever name known which will, or which may be readily converted to, expel a projectile by the action of an explosive or other propellant, and which has any barrel with a bore of more than one-half inch in diameter." *Id.* § 921(a)(4)(B).

265. 50 U.S.C. § 1801(p) (Supp. 2014) (emphasis added).

266. 50 U.S.C. § 2302(1) (2012).

267. *Id.* (emphasis added). Dr. Seth Carus, Deputy Director and Distinguished Research Fellow at the National Defense University, has compiled these differences under U.S. law, and he has also pointed out that twenty-two states have laws that contain WMD definitions and that a number of different WMD definitions also appear in international law. *See* Carus, *supra* note 193, Appendix C–D.

268. SUSAN D. MOELLER, CTR. FOR INT'L AND SEC. STUDIES AT MD., MEDIA COVERAGE OF WEAPONS OF MASS DESTRUCTION 3 (2004), *available at* http://www.cissm.umd.edu/papers/files/wmdstudy_full.pdf.

269. Carus, *supra* note 193, at 47. An overly broad statutory definition of a weapon of mass destruction may also affect the "usual constitutional balance of federal and state powers." Bond v. United States, 134 S. Ct. 2077, 2089 (2014) (finding that the federal chemical weapons statute does not apply to the defendant's conduct).

IV. THE FOURTH AMENDMENT'S PROTECTIVE LENS AND THE PROBABILITY CONSEQUENCE MATRIX

A number of scholars have written about the importance of adopting readings of the Constitution that preserve its original values.[270] The underlying values of the Fourth Amendment, which are "basic to a free society,"[271] include the "protect[ion] of personal privacy . . . against unwarranted intrusion by the State."[272] A person who places a private telephone call is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[273] The same can be said of private e-mail communications.[274] Indeed, unless the government's ability to intercept communications is checked, wiretapping devices pose a real and significant threat to liberty.[275]

However, as discussed earlier, it is essential not to confuse the reasonable expectation of privacy test, which enables us to determine whether a search has occurred, with the separate question of whether a search is reasonable. Amar reminds us that, in sorting through Fourth Amendment questions, we cannot abandon common sense and must find constitutional reasonableness.[276] The Supreme Court itself has stated that the Fourth Amendment does not protect against "all intrusions . . . but against intrusions which are not justified in the circumstances, or which are made in an improper manner."[277]

Thus, reasonableness should not be assessed in a vacuum and without consideration of the government's interest. Fourth Amendment reasonableness should be viewed contextually and assessed under particular facts and circumstances. In the context of the threatened use of certain WMDs, it is hard to imagine a governmental interest more compelling than the preservation and protection of society from existential threats, massive destruction, or catastrophic loss of life, which is clearly a constitutional value of the "highest order of magnitude."[278] Indeed, Article IV of the Constitution imposes an affirmative obligation on the federal government to protect the nation.[279]

---

270. *E.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 165, 222 (1999).

271. Wolf v. Colorado, 338 U.S. 25, 27 (1949).

272. Schmerber v. California, 384 U.S. 757, 767 (1966).

273. Katz v. United States, 389 U.S. 347, 352 (1967).

274. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). The Sixth Circuit also observed, however, that in some cases, subscriber agreements might be "sweeping enough to defeat a reasonable expectation of privacy in the content of an email account." *Id.* at 286.

275. Berger v. New York, 388 U.S. 41, 63 (1967).

276. *See* Amar, *supra* note 24, at 802–06.

277. *See* Maryland v. King, 133 S. Ct. 1958, 1969 (2013) (quoting Schmerber v. California, 384 U.S. 757, 768 (1966)).

278. *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008); *see also* Haig v. Agee, 453 U.S. 280, 307 (1981).

279. *See* U.S. CONST., art. IV, § 4 ("The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion . . . ."); *see also* Wayte v. United States, 470 U.S. 598, 611–12 (1985) ("Few interests can be more compelling than a nation's need to ensure its own security. . . . Unless society has the capability and will to defend itself from the aggressions of others,

The Constitution requires consideration of all of these values and leads to a number of key questions when a suspected terrorist threatens to use a WMD: first, how can we reconcile these seemingly competing values—individual privacy and an extraordinarily compelling government interest—so that they are mutually reinforcing and not mutually exclusive; and, second, who gets to decide how we should reconcile them?[280] Layered on top of these questions are additional considerations. As noted earlier, in a crisis involving a specific and credible threat by a terrorist to use a WMD, government officials should have greater ex ante certainty in regard to the constitutionality of their preventative actions.[281] Moreover, any new doctrinal solution must be appropriately flexible to enable those government officials to adapt to what may be dynamic or unpredictable circumstances. Finally, as Bellin has cautioned, solutions must be workable and address the Supreme Court's administrability concerns.[282]

I have previously written about the importance of using the correct lens to analyze Fourth Amendment issues.[283] "The 'lens' method of analysis is based on the premise that one has a better chance of arriving at the correct [analytical] result only if one begins the analysis with the correct lens."[284] Here, the correct lens to apply is the Fourth Amendment's protective lens, which looks to consequence as a constitutionally appropriate factor in assessing whether the government's conduct is reasonable.[285] Notwithstanding our stipulation that expectations of privacy would be at their zenith with respect to the government's acquisition of the content of telephone and e-mail communications, it is simply not acceptable to conclude that the Constitution abides no solution to the hypothetical. Indeed, as Russell Covey has observed, "The gravity of the threat posed by WMD, made or hidden in private residences, suggests that a Fourth Amendment jurisprudence that constructs a

---

constitutional protections of any sort have little meaning."); Youngstown Sheet & Tube Co. v. Sawyer (*Steel Seizure*), 343 U.S. 579, 662 (1952) (Clark, J., concurring) ("In my view . . . the Constitution does grant to the President extensive authority in times of grave and imperative national emergency. In fact, to my thinking, such a grant may well be necessary to the very existence of the Constitution itself."); Terminiello v. Chicago, 337 U.S. 1, 37 (1949) (Jackson, J., dissenting) ("There is danger that, if the Court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact."). *See generally* Charles L. Black, Jr., *Mr. Justice Black, the Supreme Court, and the Bill of Rights*, HARPER'S MAG., Feb. 1961, at 63, 68 (arguing justifications that are put forward for infringing the Bill of Rights should not be ignored when they arise from an "altogether different order of magnitude").

280. *See* Stuntz, *supra* note 24, at 875 ("[S]olutions to hard problems can never be found unless the system grapples with the right questions. That is the central problem with Fourth Amendment law as it stands today: it fails to ask the right questions.").

281. *See* Baker, *supra* note 161, at 9–10.

282. *See* Bellin, *supra* note 24, at 21 ("[T]he few commentators who squarely address the subject sketch in exceedingly broad strokes, ultimately failing to address the Supreme Court's administrability concern.").

283. *See* Glick, *supra* note 26, at 124.

284. *Id.*

285. *See supra* notes 104–52 and accompanying text.

relatively impermeable wall around the home or any other 'constitutionally-protected area' is imprudent and potentially disastrous."[286]

In thinking about a path towards a constitutional solution to the hypothetical, it is important to precisely examine where the tension arises. By any measure, based upon the information provided by a reliable informant, the government's information with respect to the terrorist's conduct is well beyond the minimum threshold set by the Supreme Court with respect to probable cause.[287] However, in addition to not knowing the type of WMD that is being assembled, the other critical piece of information missing from the hypothetical is the identification of the particular communication device that the terrorist is using. If we lived in a world in which there were only cellular telephones and there was only one cell tower[288] that transmitted all cellular telephone calls to and from Georgetown, or a world in which there was only one router[289] through which all of the Internet traffic in Georgetown flowed, then arguably, the constitutional tension in the hypothetical would not exist.[290] Clearly, however, we live in a world in which there are numerous cell towers, Internet routers, and landline telephones, any of which could be carrying the terrorist's communications. The questions can then be restated as follows: using the Fourth Amendment's protective lens, is there any framework

---

286. Russell D. Covey, *Pervasive Surveillance and the Future of the Fourth Amendment*, 80 MISS. L.J. 1289, 1300 (2011); *see also* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 675 n.3 (1989) ("As Judge Friendly explained in a leading case upholding [airport security screening] searches: 'When the risk is the jeopardy to hundreds of human lives and millions of dollars of property inherent in the pirating or blowing up of a large airplane, that danger *alone* meets the test of reasonableness . . . .'" (emphasis in original) (quoting United States v. Edwards, 498 F.2d 496, 500 (2d Cir. 1974))).

287. *See supra* notes 46–55 and accompanying text.

288. Cell towers, sometimes referred to as cell sites, are the physical locations at which the antennas and associated electronic equipment that are used for transmitting wireless telephone communications are placed. *See* HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 265 (Steve Schoen ed., 26th ed. 2011). "Cell sites may be located on stand-alone towers or on top of pre-existing buildings," Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 683 n.10 (2011), and whenever a user places or receives a voice call (or sends or receives a text message), the radio portion of that communication is transmitted between the customer's handset and a nearby tower. *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 6–7 (2013) (statement of Mark Eckenwiler, Senior Counsel, Perkins Coie LLP). *See generally*, Marshall Brain, Jeff Tyson & Julia Layton, *How Cell Phones Work*, HOW STUFF WORKS, (Nov. 14, 2000), http://electronics.howstuffworks.com/cell-phone.htm.

289. *See Frequently Asked Questions*, INTERNET TRAFFIC REPORT, http://www.internettrafficreport.com/faq.htm#router ("Routers are traffic cop computers on [the] Internet . . . [that are] responsible for redirecting data from sender to receiver. When major routers slow down or stop, it has an adverse affect [sic] on Internet data flow in that region."). *See generally* BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 84 (2010) ("The Internet . . . connects different physical networks using a set of conventions that let computers attached to these networks communicate.").

290. *See* H.R. REP. NO. 95-1283, pt. 1, at 55–56 (1978) ("[W]here a switchboard line is tapped . . . it may not be possible or reasonable to avoid acquiring all conversations.").

that could be used to solve the no-win scenario? And what role is played by the *type* of WMD to be deployed?

One potential framework would be to use a probability consequence matrix. For purposes of this discussion, let us assume that there are two variables in this matrix—probability and consequence—and within those variables, at least in the matrix's simplest form, let us further assume that there are two categories: high and low. When there is a high probability of a high consequence WMD being deployed, we should use minimization as a front-end substitute for the Fourth Amendment's particularity requirement. On the other hand, when there is a low or a high probability of only a low consequence WMD being deployed, then perhaps we should not rely on minimization to satisfy the particularity requirement. Such reliance would arguably be, in Fourth Amendment parlance, *un*reasonable. See below.

Table 1. The probability consequence matrix

	Low Probability	High Probability
Low Consequence	No	No
High Consequence	??	Yes

Concluding that minimization on the front end can serve as a substitute for the Fourth Amendment's particularity requirement in a limited and carefully delineated set of circumstances does not completely solve the "no-win" scenario. As illustrated above, the most difficult circumstance to resolve is where there is a low probability of a high consequence attack. One day, technology may provide a solution.[291] Until then, the probability consequence matrix can provide an analytical framework for policymakers to debate the issues. It should be recognized, however, that the range of potential circumstances will likely result in a more complex matrix because probability and consequence should be viewed in the WMD context as a sliding scale.

With respect to high probability/high consequence events, however, additional steps must be taken by both the executive branch and the judicial branch to ensure that individual privacy rights are protected and the government's conduct is appropriately cabined. These steps must include specific minimization procedures. Drawing upon FISA's definition, the procedures should "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning United States persons consistent with the need" to protect against the

291. To the extent that voice-to-text transcription technology for wire communications evolves in the future to a point at which automated processes can accurately screen the content of the communications, the use of such technology, coupled with minimization on the front end, would prevent any human observation of the content of the communications. *Compare Ads in Gmail*, GOOGLE, https://support.google.com/mail/answer/6603?hl=en ("Ad targeting in Gmail is fully automated, and no humans read your email or Google Account information in order to show you advertisements or related information."), *with* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 535 (2005) (arguing that a Fourth Amendment search is best described as the process by which "data is exposed to human observation").

specific WMD threat.[292] Among other things, live monitoring should take place, and as soon as the government determines that it has targeted a communication device that is not being used by the terrorist or one of his co-conspirators, the government should cease to target that device, and all previously acquired communications from that device should be destroyed. Such procedures should also require the government to promptly notify the court if further intelligence or investigative activity allows it to narrow the ongoing surveillance.

Resolving the constitutional tension present in the hypothetical therefore requires the executive branch to submit narrowly tailored and specifically designed minimization procedures to the judicial branch for approval, and requires the judicial branch to closely oversee the executive branch throughout the surveillance period in order to hold the delicate balance between competing constitutional values "steady and true."[293] However, the solution also requires the legislative branch to resolve the definitional issues highlighted by Parts II and III; moreover, other important steps must also be taken. Part V discusses these additional steps.

V. A PATH FORWARD

The Supreme Court has repeatedly emphasized that "the ultimate touchstone of the Fourth Amendment is 'reasonableness'"[294] and "particularized exceptions . . . are sometimes warranted."[295] The hypothetical raises competing constitutional values: the protection of individual privacy on the one hand, and the preservation and protection of society from existential threats, massive destruction, or catastrophic loss of life, on the other hand. The Fourth Amendment should not, however, paralyze the judicial branch and leave the nation "stuck in a zero-sum world,"[296] particularly when the legislative branch can play an important

---

292. 50 U.S.C. § 1801(h) (2012) (definition of minimization procedures); *cf.* 50 U.S.C. § 1801(e)(1)(A)–(B) (2012) (definition of foreign intelligence information).

293. *See In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1016 (Foreign Int. Surv. Ct. Rev. 2008) ("[T]he Constitution is the cornerstone of our freedoms, and the government cannot unilaterally sacrifice constitutional rights on the altar of national security. Thus, in carrying out its national security mission, the government must simultaneously fulfill its constitutional responsibility to provide reasonable protections for the privacy of United States persons. The judiciary's duty is to hold that delicate balance steady and true.").

294. Riley v. California, 134 S. Ct. 2473, 2482 (2014) (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)); Michigan v. Fisher, 130 S. Ct. 546, 548 (2009) (per curiam); Samson v. California, 547 U.S. 843, 855 n.4 (2006); Bd. of Educ. v. Earls, 536 U.S. 822, 828 (2002) ("'[R]easonableness' . . . is the touchstone of the constitutionality of a governmental search."); United States v. Knights, 534 U.S. 112, 118–19 (2001); Illinois v. McArthur, 531 U.S. 326, 330 (2001) (stating that the Fourth Amendment's "central requirement is one of reasonableness") (citation omitted) (internal quotation marks omitted); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995) ("[T]he ultimate measure of the constitutionality of a governmental search is 'reasonableness.'").

295. Chandler v. Miller, 520 U.S. 305, 313 (1997).

296. Ric Simmons, *Ending the Zero-Sum Game: How To Increase the Productivity of the Fourth Amendment*, 36 HARV. J.L. & PUB. POL'Y 549, 575 (2013); *see also* Covey, *supra* note 286, at 1300 ("[T]he proliferation of destructive technologies and the increasing ease of

constitutional role in determining what is reasonable in the context of the hypothetical. Ric Simmons believes that legislative interpretations of the Fourth Amendment's reasonableness clause are arguably "superior to judicial determinations," and "deference to legislators seems even more sensible in the context of antiterrorism searches."[297] At a minimum, as Fiss has stated, the "President and the Congress are coordinate branches of government . . . charged with the duty of giving concrete meaning to the Constitution."[298]

More than fifty years ago in *Keith*, the Supreme Court recognized Congress's constitutional role to consider the policy and practical considerations that are present when the government seeks to use wiretaps to protect the nation from grave threats.[299] Given the different consequences that can be reasonably anticipated from the use of different types of WMDs, it is clear that the legislative branch has a constitutional role to play in determining what is reasonable under the Fourth Amendment in the context of the hypothetical. The legislative branch should resolve the definitional issues highlighted by Parts II and III, and identify the specific showings that the executive branch should be required to make to the judicial branch. In this regard, the legislative branch should also determine the nature and extent of any deference that it believes the judicial branch should give to the executive branch with respect to these showings.[300] Indeed, how the legislative branch would resolve these questions is likely to be quite different from how the judicial branch would resolve them.

The failure of the legislative branch to debate all of the issues in a timely manner would be most unfortunate. Congressional inertia or indifference to these issues may leave the judicial branch without criteria to evaluate whether the

---

manufacturing them will continually increase the hazards of placing off-limits any physical locations to preventative surveillance efforts by the state.").

297. Simmons, *supra* note 13, at 900. In 1978, the House Permanent Select Committee on Intelligence certainly agreed with this assessment as well. *See* H.R. REP. NO. 95-1283, pt. 2, at 21–22 (1978) ("[T]he decision as to the standards governing when and how foreign intelligence electronic surveillance should be conducted is and should be a political decision, in the best sense of the term, because it involves the weighing of important public policy concerns—civil liberties and the national security.").

298. Fiss, *supra* note 27, at 25; *see also* Richard C. Worf, *The Case for Rational Basis Review of General Suspicionless Searches and Seizures*, 23 TOURO L. REV. 93, 131–37 (2007) (arguing that suspicionless searches are constitutional if they have been approved by a legislative body); *id.* at 197 ("Courts should trust the political process to approve the right balance when it comes to searches and seizures of groups of ordinary citizens."). *But see* Stephen Schulhofer, *Pleasant Surprises—and One Disappointment—in the Supreme Court's Cell Phone Decision*, JUST SECURITY (June 27, 2014, 10:45 AM), http://justsecurity.org/12312/pleasant-surprises-disappointment-supreme-courts-cell-phone-decision/ (arguing that Fourth Amendment concerns "cannot be met by porous safeguards that mainstream voters may consider 'reasonable'").

299. United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 322–23 (1972).

300. Although the Supreme Court has suggested that the judicial branch could consider giving "heightened deference to the judgments of the political branches with respect to matters of national security," Zadvydas v. Davis, 533 U.S. 678, 696 (2001), and has noted that courts have been "reluctant to intrude upon the authority of the Executive in . . . national security affairs," Dep't of Navy v. Egan, 484 U.S. 518, 530 (1988), this does not mean that Congress should not debate *the degree to which* there should be deference to the executive branch.

threatened use of a particular type of WMD should qualify for this new doctrinal solution. Indeed, inaction by Congress may very well "put judges into the business of making exceptions to a standard rule that is not easily cabined and is at odds with their obligation to say what the law is."[301]

The role of the judicial branch would, by no means, be a "rubberstamp."[302] The Supreme Court made clear in *Keith* that federal judges have the ability to understand national security matters, as more than three decades of jurisprudence has confirmed.[303] This point is important to emphasize: part of the solution proposed in this Article requires a "neutral and detached"[304] magistrate to determine whether the executive branch has met well-defined standards that have been publicly debated and approved by the legislative branch, and then presented to the President for his approval.[305] However, it is equally important to state that the pathway to the solution should not reflexively rely on the special needs cases, which are based on programmatic purposes that extend beyond the normal needs of law enforcement.[306] Rather, the solution relies on the principle that consequence has a constitutional role to play in Fourth Amendment calculus in certain limited circumstances.[307]

As discussed above, the path forward also requires the executive branch to submit specific minimization procedures to the judicial branch for approval. Approval by the judicial branch of procedures that particularize the specific communications that may be retained by the executive branch would be an effective privacy-enhancing mechanism to ensure that "nothing is left to the discretion of the officer executing the warrant,"[308] a core Fourth Amendment principle. Whether additional restrictions are also appropriate, including restrictions on the government's ability to use the fruits of the wiretap, is another critical question that needs to be answered by policymakers.[309] This is particularly

---

301. Fiss, *supra* note 27, at 29. Fiss would, however, "resist the temptation to allow an exception to the warrant requirement for so-called extraordinary crimes, regardless of how the exception is formulated." *Id.* In addition to being concerned about the difficulty of identifying the criteria needed to implement any exception, Fiss "fear[s] that an exception to the warrant requirement for extraordinary crimes would be susceptible to great abuse." *Id.*

302. *See* ACLU v. Clapper, 959 F. Supp. 2d 724, 733 n.3 (S.D.N.Y. 2013); *see also* Henry Schuster, *Inside America's Secret Court*, CNN (Feb. 14, 2006, 6:41 AM), http://www.cnn.com/2006/US/02/13/schuster.column/ (quoting the Honorable Royce C. Lamberth, former Chief Judge of the FISA court, saying that "the court was not a rubberstamp for the government").

303. *See Keith*, 407 U.S. at 320 ("We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation."); *see also* KRIS & WILSON, *supra* note 164, § 3:6.

304. *See supra* note 42 and accompanying text.

305. *See* U.S. CONST. art. 1, § 7, cl. 2 ("Every Bill which shall have passed the House of Representatives and the Senate, shall, before it become a Law, be presented to the President of the United States; If he approve he shall sign it . . . .").

306. *See supra* notes 85–93 and accompanying text.

307. *See supra* notes 104–52 and accompanying text.

308. *E.g.*, Marron v. United States, 275 U.S. 192, 196 (1927).

309. *See generally* Ricardo J. Bascuas, *Fourth Amendment Lessons from the Highway and the Subway: A Principled Approach to Suspicionless Searches*, 38 RUTGERS L.J. 719,

important because use restrictions with respect to serious criminal activity could very well deprive the government of evidence that could convict a murderer.[310] On the other hand, determining the nature and extent of use restrictions may, in certain circumstances, be critical to a court's conclusion that the government's actions should be considered constitutionally reasonable.

Congressional action that establishes clear definitions and sets meaningful standards would ensure that if the government's actions were subsequently presented to the judicial branch for review, presidential authority would be "at its maximum," rather than in a "zone of twilight" or "at its lowest ebb."[311] Inclusion of the legislative branch should also be viewed as an important constitutional value to be preserved by a nation founded on a system of checks and balances.[312] Finally, the legislative branch must ensure that inflexible constraints are not placed on the executive branch, which would prevent it from responding to the often unpredictable nature of a terrorist threat.[313]

The challenge for the legislative branch is, therefore, to create a flexible process that still maintains an important independent check by the judicial branch.[314] As the Supreme Court has observed in another constitutional context, Congress should engage in a "genuine debate about how best to preserve constitutional values while protecting the Nation from terrorism."[315] Moreover, as Justice Jackson wisely

---

781 (2007) (arguing that suspicionless searches could be justified under certain circumstances if "anything seized unrelated to the danger . . . [is] suppressed"); Covey, *supra* note 286, at 1318 (arguing that we must find ways "to shift the focus of Fourth Amendment law from regulation of the acquisition of information to regulation of its use"); Simmons, *supra* note 13, at 915 (arguing "suspicionless searches could be permitted as long as the government is not permitted to use any fruits of the search in a subsequent prosecution").

310. *Cf.* United States v. Isa, 923 F.2d 1300, 1304 (8th Cir. 1991) (rejecting the suppression of evidence obtained from a FISA wiretap that targeted a suspected foreign agent who had allegedly murdered his daughter).

311. Youngstown Sheet & Tube Co. v. Sawyer (*Steel Seizure*), 343 U.S. 579, 635–38 (1952) (Jackson, J., concurring). *Cf.* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 303–07 (1972) (finding that the 1968 version of Title III was "essentially neutral" and "nebulous," and that Congress "left presidential powers where it found them").

312. *See generally* JOHN ADAMS, THOUGHTS ON GOVERNMENT (1776), *reprinted in* 4 THE WORKS OF JOHN ADAMS, SECOND PRESIDENT OF THE UNITED STATES: WITH A LIFE OF THE AUTHOR, NOTES AND ILLUSTRATIONS 198 (Charles C. Little & James Brown eds., 1851) ("[T]he judicial power ought to be distinct from both the legislative and executive, and independent upon both, . . . as both should be checks upon that."); THE FEDERALIST NO. 9, at 72–73 (Alexander Hamilton) (Clinton Rossiter ed., 1961) ("[Checks and balances] are means, and powerful means, by which the excellencies of republican government may be retained and its imperfections lessened or avoided."); THE FEDERALIST NO. 47, at 303 (James Madison) (Clinton Rossiter ed., 1961) ("When the legislative and executive powers are united in the same person . . . there can be no liberty. . . .") (quoting BARON DE MONTESQUIEU, THE SPIRIT OF THE LAWS 151 (Thomas Nugent trans., Hafner Publishing 1949)).

313. *See supra* note 160 and accompanying text; *see also Keith*, 407 U.S. at 312 ("[U]nless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered.").

314. *Keith*, 407 U.S. at 317.

315. Boumediene v. Bush, 553 U.S. 723, 798 (2008) (Souter, J., concurring) ("The political branches, consistent with their independent *obligations* to interpret and uphold the Constitution, can engage in a genuine debate about how best to preserve constitutional

stated in his concurring opinion in the *Steel Seizure* case, "We may say that power to legislate for emergencies belongs in the hands of Congress, but only Congress itself can prevent power from slipping through its fingers."[316]

CONCLUSION

The prevention of massive destruction or catastrophic loss of life should be viewed as a critical factor in assessing Fourth Amendment reasonableness. In the context of the hypothetical, it is simply unacceptable to conclude that there are no circumstances where a federal court could issue a wiretap order that would enable the government to locate a terrorist and prevent the use of a WMD. As other scholars have noted, "[T]raditional [Fourth Amendment] doctrine falls short in an age of threats unprecedented in their potential for harm."[317] However, the Fourth Amendment's protective lens and the probability consequence matrix can provide a pathway toward a new doctrinal solution. While the matrix will not resolve all of the issues that are raised by the hypothetical, and while subjective judgments may be inherent when assessments of probability and consequence are made, the matrix can provide an analytical framework for assessing the role that consequence should play in a Fourth Amendment calculus.

Fairly well-established minimization principles are an essential element of a new doctrinal solution to the hypothetical. Such a solution, however, will require members of the legislative branch—as the elected representatives of the people—to debate the issues fully and assert their constitutional role in determining what is reasonable when a terrorist threatens to use a WMD. The legislative branch must enact clear definitions and standards "calibrated to the risk"[318] that prevent the executive branch from unnecessarily intruding upon individual privacy.[319] In addition, by requiring the executive branch to submit narrowly tailored minimization procedures, the executive branch's actions will be cabined by the specific exigency which justified the surveillance.[320] Most importantly, the imposition of such procedures will ensure that the executive branch will be acting under the watchful eye of the judicial branch.[321] Taken together, all of these actions will provide government officials with greater ex ante legal certainty in regard to the constitutionality of their preventative actions, as well as the flexibility they may

---

values while protecting the Nation from terrorism." (emphasis added)).

316. *Steel Seizure*, 343 U.S. at 654 (Jackson, J., concurring).

317. Gould & Stern, *supra* note 24, at 777; *see also* Stuntz, *supra* note 24, at 849 ("Different crimes give rise to different government interests, which in turn should lead to different Fourth Amendment standards.").

318. Chandler v. Miller, 520 U.S. 305, 323 (1997) ("[W]here the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable. . . .'").

319. *Keith*, 407 U.S. at 317.

320. Terry v. Ohio, 392 U.S. 1, 25–26 (1968).

321. *See generally* Nixon v. Warner Commc'ns, 435 U.S. 589, 598 (1978) (commenting on the interest of citizens in inspecting judicial records and documents in order to keep a "watchful eye on the workings of public agencies").

need to respond to dynamic and unpredictable circumstances. Thus, government lawyers will say *yes* when they should say *yes*, and *no* when they should say *no*.[322]

Stated another way, and to paraphrase former Supreme Court Justice Potter Stewart's observation about automobile searches, thoughtful and deliberative action by each branch of government is necessary lest the acronym WMD becomes a "talisman in whose presence the Fourth Amendment fades away and disappears."[323] The nation should not have to make the "false choice"[324] between security and liberty. Instead, all three branches should play a role[325] in ensuring the enduring vitality of the Fourth Amendment in this "brave new world"[326] where the terrorist use of a WMD could lead to massive destruction or catastrophic loss of life.

---

322. *See* Baker, *supra* note 161. Judge James E. Baker cautions, however, that the reality of many legal questions related to national security law is that they are not yes or no questions. JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 317 (2007). Thus, if the policy choices discussed in this Article can be "embedded in law," then the law will be a "source of calm and stability" at a time when lawyers are under stress and must apply the law to uncertain or emerging facts. *Id.* at 309, 313; *see also* James E. Baker, *Process, Practice, and Principle: Teaching National Security Law and the Knowledge That Matters Most*, 27 GEO. J. LEGAL ETHICS 163, 178 (2014) ("[I]t is the nature of national security practice to confront novel questions under great pressure where lives are at stake.").

323. Coolidge v. New Hampshire, 403 U.S. 443, 461–62 (1971).

324. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 395 (2004).

325. *See* Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004) (asserting that the constitution "envisions a role for all three branches when individual liberties are at stake").

326. *See* Covey, *supra* note 286, at 1318.