Notre Dame Journal of Law, Ethics & Public Policy

Volume 19
Issue 1 *Symposium on Security & Liberty*

Article 20

February 2014

The Fourth Amendment and Remote Searches: Balancing the Protection of the People with the Remote Investigation of Internet Crimes

Jeremy A. Moseley

NOTES

THE FOURTH AMENDMENT AND REMOTE SEARCHES: BALANCING THE PROTECTION OF "THE PEOPLE" WITH THE REMOTE INVESTIGATION OF INTERNET CRIMES

JEREMY A. MOSELEY*

Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. . . . The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[1]

—Justice Louis D. Brandeis

INTRODUCTION

The preceding quote by Justice Brandeis adds caution to the choice that the United States continually faces—greater protection by the government or greater freedom from government intrusion. When confronted with this choice in the context of the Internet, courts face another dilemma: To what extent do government agents' actions over the Internet implicate the Fourth Amendment? Professor Allan Stein provides the following context to this choice: "Sovereignty is not just exercise of power, but commitment to a particular legal order."[2] Indeed, one of the most considered questions with regard to Internet jurisdiction is what country, if any, has the authority to regulate the Internet.[3] A system that transcends jurisdictional lines raises

* J.D. Candidate, University of Notre Dame Law School, 2005; Thomas J. White Scholar, 2003–2005; B.A., Pensacola Christian College, 2002.

1. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting) (criticizing the majority's holding that wire taps were not a "search or seizure" requiring a warrant). *See infra* notes 20–45 and accompanying text.

2. Allan R. Stein, *Frontiers of Jurisdiction: From Isolation to Connectedness*, 2001 U. CHI. LEGAL F. 373, 399 (discussing the problems of jurisdiction related to the investigation of international crimes).

3. Michael J. Madison, *The Narratives of Cyberspace Law (or, Learning from Casablanca)*, 27 COLUM.-VLA J.L. & ARTS 249, 258 (2004).

serious questions about national sovereignty.[4] As this quote suggests, the United States has more to consider than whether other nations will find an exercise of power to be legitimate. Just as important is what will "the people" say? The United States' commitment to a particular legal order, a democracy within a republic, provides numerous questions with which the government must grapple before an exercise of power over the Internet can be considered legitimate. Relevant to the following discussion are the questions of whether the Fourth Amendment protects against government searches over the Internet ("remote searches") and whether the location of the criminal affects the Fourth Amendment's application to remote searches.

Remote searches present a unique combination of Fourth Amendment jurisprudence and questions of jurisdiction. A remote search involves accessing information from a remote location.[5] For example, a government agent in Virginia could hack into a website located on a server in Kansas, or even Russia, or the agent could retrace the movements of an Internet user based on the Internet Protocol address in an attempt to determine the user's identity. When the agent finds the information for which he is looking, he may download the data to his own computer. In this instance, locating and downloading the data implicates the Fourth Amendment's scope of a "search and seizure" without the government agent ever physically entering a constitutionally protected area. Further, the fact that the search is remote can raise jurisdictional questions, especially because the agent may not know the location of the end user he is seeking.

Due to the remoteness of the search, jurisdictional lines are easily blurred on the Internet. This blurring provides a unique dilemma for the United States government. Because of the protections of the Fourth Amendment provided to the people, federal agents may have more latitude in pursuing crimes in other countries than they have within the United States. At first glance, if the government follows an international treaty when pursuing international criminals, the Fourth Amendment is not implicated. Trouble arises, however, when the criminal is inside the United States. For, while the exercise of power is more legiti-

4. Allan R. Stein, *Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision*, 98 NW. U. L. REV. 411, 412 (2004).

5. Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 404 (2003).

mate, the scope of that power is now constrained by the Fourth Amendment.[6]

As criminals find new ways to use technology to threaten America's safety, the initial public reaction seems to be a heightened fear of these more deviant criminals—as though the idea of Internet crimes evokes an unprecedented evil that can destroy our freedoms if not ended immediately.[7] This fear leads many to conclude that the government must have a greater ability to stop criminals, even if this includes invasive procedures. However, as Justice Brandeis warned, this fear should not compel Americans to allow the government unfettered power to fight this new area of crime. For even with new technology, Chief Postal Inspector Lee Heath asserted that many of these crimes are simply "old wine in a new bottle."[8]

In analyzing remote searches, this Note will discuss in Section I how the Fourth Amendment has developed in relation to new technology. Section II will address the ways in which the scope of the Fourth Amendment is limited by jurisdictional questions. Finally, this Note will synthesize in Section III the development of technology and jurisdictional questions by explaining how courts should provide the necessary Fourth Amendment protection from remote searches without limiting the application of their decisions to today's technology.

I. DEVELOPMENT OF THE FOURTH AMENDMENT

As with any technological development, the temptation exists to allow law enforcement to employ the latest technology, without contemplating the repercussions.[9] Yet this development does not occur in a vacuum,[10] as well it should not. In fact, the protection given by the Fourth Amendment in the context of the

6. Viktor Mayer-Schonberger, *The Shape of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L L. 605, 613 (2003).

7. Victoria Smith Ekstrand, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 COMM. L. & POL'Y 405, 415 (2003).

8. *Technology: Feds Nab 125 in Global Cybercrime Sweep*, CNN, Nov. 21, 2003, *at* http://www.cnn.com/2003/TECH/internet/11/21/crackdown.cybercrime.reut/index.html (on file with the Notre Dame Journal of Law, Ethics & Public Policy).

9. Oscar H. Gandy, Jr., *Exploring Identity and Identification in Cyberspace*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1085, 1103–07 (2000) (arguing, in the commercial context, that because consumers demand the latest technology and convenience without considering the accompanying loss of privacy the government must regulate these invasions of privacy).

10. For example, the substantial connections requirement in immigration law has affected Fourth Amendment jurisprudence relating to remote searches and has left open the possibility that only United States citizens can

Internet can greatly affect both the direction of future technological developments[11] and the ability for these rules to govern future developments effectively.[12]

Thus arises the problem that courts endlessly struggle with when considering technological advancements: how to apply a ruling based on past technology to current and future technological advancements. For example, if a court applied a bright line rule to the Internet as it was in 1993, the rule pronounced by the court would now be ineffective because of how the Internet has developed. Similarly, any rule articulated today could be useless in a matter of years. Yet cases take years to decide, while technology changes in a matter of months. The ways in which courts have previously handled new technology demonstrate the dilemma courts face with remote searches—adequately addressing today's technology with a protection guaranteed two hundred years ago. The Fourth Amendment provides:

> The right of the people to be secure in their person, 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 person or things to be seized.[13]

A. *Early History and Development of the Fourth Amendment*

Traditionally, courts followed the textual meaning of the Fourth Amendment and considered the protection of the home to be the main purpose of the Fourth Amendment.[14] By requiring both probable cause and a warrant before government officials can search an individual's house, the Fourth Amendment restricted the government from conducting arbitrary searches. Because this only prohibits "unreasonable" searches, courts must balance the protection of privacy with the "promotion of legiti-

---

receive any protection from the Fourth Amendment. *See infra* note 92 and accompanying text.

11. For a discussion of the role government regulation should play in the development of the Internet, see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

12. *See generally* Edward Lee, *Rules and Standards for Cyberspace*, 77 NOTRE DAME L. REV. 1275 (2002) (addressing the inconsistency of courts in applying either a narrow ruling to Internet cases or a broad ruling and proposing a framework for courts to determine which approach is best, particularly with regard to copyright law).

13. U.S. CONST. amend. IV.

14. Weeks v. United States, 232 U.S. 383, 390 (1914).

mate governmental interests."[15] Based on the maxim that a man's house is his castle, courts considered this protection a high priority.[16] Because of its basis in this "castle doctrine," courts strongly protected intrusion into the home but were more reluctant to extend this protection beyond the home.[17] Yet, even early cases recognized that the essence of the Fourth Amendment was protection of people, not places. In *Boyd v. United States*, Justice Bradley explained:

> It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . it is the invasion of this sacred right which underlies and constitutes the essence of [the] judgment.[18]

Even with this seemingly clear articulation of the purpose of the Fourth Amendment, courts were still reluctant to protect areas outside of the home. Therefore, as technology changed the methods for investigation, courts grappled with whether these new methods even implicated the Fourth Amendment. Not surprisingly, the last three decades, which have seen tremendous advances in technology, have seen this provision litigated more than any other clause in the Bill of Rights.[19]

B. *Change in Thinking with Improvements in Technology*

The traditional view of the Fourth Amendment first encountered the problem of new technology in *Olmstead v. United States*.[20] Police employed new technology to tap phone lines at the defendants' office building and their homes.[21] Police, however, did not trespass on any of the defendants' property. In fact, the taps were placed on the phone lines in the street near the defendants' residences. The Supreme Court applied the traditional meaning of the Fourth Amendment and concluded that

---

15. Chavez v. Martinez, 538 U.S. 760, 775 (2003) (holding coercive interrogation tactics were constitutional when balanced against the governmental interest in securing the witness's testimony while undergoing medical treatment).

16. THOMAS M. COOLEY, CONSTITUTIONAL LIMITATIONS: A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 365–66 (1883).

17. *See infra* notes 20–45 and accompanying text.

18. Boyd v. United States, 116 U.S. 616, 630 (1886).

19. *See generally* W. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (2d ed. 1987).

20. Olmstead v. United States, 277 U.S. 438 (1928).

21. *Id.* at 456–57.

the practical scope of the Fourth Amendment was "persons, houses, papers, and effects."[22] Applying "searches and seizures" to things heard or seen by the police did not fit under the Fourth Amendment's protection and should thus be left to the Legislature to protect.[23] While one may appreciate the Court's willingness to defer to Congress, this traditional interpretation fails to account for the implications of allowing technology to trample "personal security" and "personal liberty."[24] Justice Brandeis, in his dissent, exposed the flaw in the majority's reasoning:

> In the application of a constitution, therefore, our contemplation cannot be only of what has been but of what may be. Under any other rule a constitution would indeed be as easy of application as it would be deficient in efficacy and power. Its general principles would have little value and be converted by precedent into impotent and lifeless formulas. Rights declared in words might be lost in reality.[25]

As Justice Brandeis warned, a declaration of rights is only as effective as its application. Thus, following a bright-line rule of what the Fourth Amendment protects ("persons, houses, papers, and effects")[26] can lead to the loss of any meaningful protection. Justice Brandeis further noted that the government may some day be able to reproduce papers in court without ever removing them from secret drawers.[27] Yet, such advancement in technology should not affect the protection guaranteed to citizens. Brandeis's comments, in some respects, foreshadow remote searches. Had the ruling in *Olmstead* not been overturned later by the Supreme Court, the Fourth Amendment would now be an "impotent and lifeless formula."[28]

Fortunately, the next time the Supreme Court applied the Fourth Amendment to new technology, the Court focused on whether allowing the government's use of the technology was reasonable. The Court again considered whether the Fourth Amendment applied to federal agents listening to phone conversations in *Katz v. United States*.[29] Agents attached a listening device to the phone booth that Katz was using and listened to his

22. *Id.* at 466.
23. *Id.* at 468.
24. Boyd v. United States, 116 U.S. 616, 630 (1886).
25. *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).
26. *Id.*
27. *Id.* at 474.
28. *Id.* at 473.
29. Katz v. United States, 389 U.S. 347 (1967).

end of the conversation.[30] The lower courts followed the traditional approach and found no violation of the Fourth Amendment, because the agents did not physically enter Katz's property.[31] The Supreme Court reversed.

In looking to the purpose of the Fourth Amendment, the majority noted, "[T]he Fourth Amendment protects people, not simply areas . . . ."[32] Though cases decided between *Olmstead* and *Katz* had eroded the traditional approach to the Fourth Amendment,[33] the *Katz* Court finally overruled *Olmstead*.[34] In so doing, the Court held, "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[35] Because Katz intended to exclude others from hearing his conversation when he entered the telephone booth, he did not relinquish his right to private conversation simply because the conversation took place in a phone booth instead of in his house. The Court determined that advances in technology meant that the presence or absence of physical intrusion into a given enclosure could no longer be the deciding factor in Fourth Amendment analysis.

Justice Harlan wrote a concurring opinion to articulate a twofold requirement for extending Fourth Amendment protection: (1) the person must have a subjective expectation of privacy; and (2) the expectation must be one that society is prepared to recognize as "reasonable."[36] This delineation of the scope of the Fourth Amendment has been quoted often by subsequent courts to reiterate the principles embodied in the Fourth Amendment.[37] In fact, this two-part test now constitutes the

30. *Id.* at 348.

31. Katz v. United States, 369 F.2d 130, 134 (9th Cir. 1966), *vacated by* 389 U.S. 347 (1967).

32. *Katz*, 389 U.S. at 353.

33. *See, e.g.*, Warden v. Hayden, 387 U.S. 294 (1967) (holding that officers did not need a warrant to enter the house minutes after a fleeing suspect entered the house); Silverman v. United States, 365 U.S. 505 (1961) (finding that placing a listening device in the defendant's home without obtaining a warrant violated the Fourth Amendment).

34. *Katz*, 389 U.S. at 359.

35. *Id.*

36. *Id.* at 361 (Harlan, J., concurring).

37. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 452 (1989) (O'Connor, J., concurring) (holding that an officer's observation of the interior of a greenhouse from a helicopter was not a violation of the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 207 (1986) (finding that the aerial observation of a fenced-in backyard was not an unreasonable search); Rakas v. Illinois, 439 U.S. 128, 148–50 (1978) (holding that a passenger could not challenge the warrantless search of a car because he had no legitimate expectation of privacy in another's car).

required analysis for all Fourth Amendment considerations for searches and seizures.

More recently, however, the Supreme Court wavered in its protection of the purpose of the Fourth Amendment by adopting a bright-line rule in *Kyllo v. United States*.[38] The question before the Court in *Kyllo* was whether using a thermal-imaging device to detect concentrations of heat within a house constituted a "search."[39] Specifically, police suspected Kyllo of growing marijuana in his home.[40] To verify their suspicions, police used a thermal-imaging device to detect high concentrations of heat emanating from the house.[41] The high level of heat emissions along one wall led police to believe that Kyllo was using halide lamps to grow marijuana. Based on the information gathered from the thermal-imaging device, police obtained a search warrant and found Kyllo growing marijuana in his home.[42] Although a visual observation had never been considered a search, the Court noted that the thermal-imaging device provided police with information that otherwise would not have been obtained without entering the house.[43] Because Kyllo had a subjective expectation of privacy, protection turned on whether this expectation was reasonable. The Court explained its holding: "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use."[44] The heat emanations provided information that police could not have obtained without either using technology or entering the house.

Although the Court sought to narrow the rule by adding a caveat—technology not in general public use—the caveat limited the application of this rule to present technology rather than basing it solely on the purpose of the Fourth Amendment. While, in this case, the Court found that new technology was still subject to the Fourth Amendment, the long-term effect could still be to limit the effectiveness of this protection as technology becomes more available. This reaction by the Court is evidence of the difficulty courts face in applying principles of law to new technology

38. Kyllo v. United States, 533 U.S. 27 (2001).
39. *Id.* at 29.
40. *Id.* at 28.
41. *Id.*
42. *Id.* at 30.
43. *Kyllo*, 533 U.S. at 32–33.
44. *Id.* at 34 (internal citation omitted).

without unintentionally limiting their application to current technology. In his dissent, Justice Stevens explained: "Instead of concentrating on the rather mundane issue that is actually presented by the case before it, the Court has endeavored to craft an all-encompassing rule for the future."[45] Yet, in focusing on a rule for the future, the Court limited the usefulness of the rule by making it dependent upon whether the technology is in widespread public use—a consideration which should not be dispositive of Fourth Amendment protection.

For example, authorities can easily track one's movements on the Internet. With remote searches, they can determine whether illegal content is saved on a computer or whether the content of the computer suggests other illegal activity. Even many hackers can intercept and read email messages because of the decryption software that is available. This technology is not yet widespread. Yet the availability of such software, for hackers or federal agents, should not determine whether one has an expectation of privacy in computer content or email communications. Whether these searches or seizures are reasonable should be based on what the Fourth Amendment protects, not on what technology is available.

C. *What It Means Now For Technology*

Overall, courts have followed the principle of the Fourth Amendment rather than a bright-line rule for Fourth Amendment analysis.[46] Rather than limiting their reasoning to present technology by establishing rules that may become obsolete as technology changes, courts, such as the Eighth Circuit in *United States v. Bach*,[47] have followed the Supreme Court's reasoning in *Katz*. In so doing, they have kept the flexibility in the Fourth Amendment that is crucial to its ability to protect "the people."

In *Bach*, the court considered whether the seizure of emails from Yahoo!'s servers constituted an unreasonable seizure under the Fourth Amendment.[48] Based on information given to the police by a concerned mother, police investigated users who had met with the mother's minor child by tracing the screen name that was used in Internet chat rooms. The police then obtained a warrant for all emails connected to that Yahoo! screen name.

45. *Id.* at 51 (Stevens, J., dissenting).

46. Michael Scaperlanda, *The Domestic Fourth Amendment Rights of Aliens: To What Extent Do They Survive* United States v. Verdugo-Urquidez?, 56 Mo. L. Rev 213, 216 (1991).

47. United States v. Bach, 310 F.3d 1063 (8th Cir. 2002).

48. *Id.* at 1065.

Because the servers were located in California and the investigation was in Minnesota, police faxed the warrant to Yahoo! and asked for a copy of all of the emails from that screen name.[49] The question before the court was whether it was reasonable to allow a civilian (Yahoo!) to gather the information required under the warrant without an officer being present.[50] The Eighth Circuit held that the seizure was reasonable under the Fourth Amendment based on the following factors: (1) physical presence of an officer would not have helped the search and may have even hindered it; (2) "the technical expertise of Yahoo!'s technicians far outweighs that of the officers; (3) the items 'seized' were located on Yahoo!'s property;" (4) officers had obtained a warrant authorizing the search; and (5) "the officers complied with the provisions of the Electronic Communications Privacy Act."[51]

While starting with the same two principles that Justice Brandeis had established years before, the court used the preceding factors to reach its conclusion. In so doing, the Eighth Circuit avoided limiting the application of its decision to current technology. Additionally, the court quoted a prior Eighth Circuit opinion stating that the reasonableness standard of the Fourth Amendment "is flexible and should not be read to mandate rigid rules that ignore countervailing law enforcement interests."[52] This understanding of the Fourth Amendment is especially crucial when analyzing the intersection of remote searches and the jurisdictional issues of applying the Fourth Amendment.

II. THE CURRENT LAW OF CROSS-BORDER AND REMOTE SEARCHES

Just as technology has changed how courts determine what constitutes a "search and seizure," the location of the government action can also affect whether the Constitution applies. An examination of how Fourth Amendment jurisprudence is applied to cross-border searches is necessary to understand how the Fourth Amendment will apply to remote searches. The most troubling areas of this application are with regard to United States citizens abroad and to noncitizens without substantial connections to the United States. Because courts apply the Fourth

49. *Id.*

50. *Id.* at 1066.

51. *Id.* at 1067.

52. *Id.* at 1067 (quoting United States v. Murphy, 69 F.3d 237, 243 (8th Cir. 1995)).

Amendment to United States citizens and to noncitizens differently, these categories will be addressed separately.

A. *United States Citizens Abroad*

Fourth Amendment protection extends to the actions of United States officials against United States citizens on foreign soil.[53] Based on the theory that the government derives its powers from "the people," the government's actions against the people are constrained by the Constitution, regardless of whether these actions are in the United States or on foreign soil.[54] While every court starts with this premise, changes in the approach to this problem indicate that these statements are now merely lip service to the Constitution, rather than a meaningful constraint on the government.

Even if United States officials follow the law of the foreign country in which the "search and seizure" takes place, they must still follow the Fourth Amendment if they are searching the home of a United States citizen.[55] The Circuit Court for the District of Columbia considered this question in *Powell v. Zuckert.* Powell's house was searched by United States and Japanese officials, pursuant to a general Japanese search warrant. Based on evidence found in his house, Powell was discharged from the military.[56] The government agreed that the search would have violated the Fourth Amendment but argued that the Fourth Amendment did not apply.[57] The court considered whether the Fourth Amendment applied to the actions taken by the United States officials in a different country.[58] The government claimed that a treaty requiring cooperation between Japanese and United States officials in investigations allowed the United States officials to be present during the search of Powell's home by the Japanese.[59] The court determined, however, that United States officials did not merely observe the search; rather, they carried it out.[60] More importantly, the court quoted *Reid v. Covert*[61] which

53. *See* Reid v. Covert, 354 U.S. 1, 16 (1957).

54. *See* Randall K. Miller, *The Limits of U.S. International Law Enforcement After* Verdugo-Urquidez*: Resurrecting* Rochin, 58 U. PITT. L. REV. 867 (1997) (discussing the theory of "connecting" individuals to the United States to determine who is entitled to Fourth Amendment protection).

55. *See* Powell v. Zuckert, 366 F.2d 634 (D.C. Cir. 1966) (holding that a treaty cannot authorize the United States to search the foreign home of a United States citizen without probable cause).

56. *Id.* at 639.

57. *Id.* at 640.

58. *Id.*

59. *Id.* at 638.

60. *Id.* at 640.

stated: "No agreement with a foreign nation can confer power on the Congress, or on any other branch of Government, which is free from the restraints of the Constitution."[62] Thus, any action by United States officials against United States citizens is constrained by the Constitution, regardless of the location.

In *United States v. Peterson*,[63] the Ninth Circuit considered what was required to make a search that was the product of a joint investigation between United States and foreign officials reasonable.[64] Philippine and Thai authorities tapped the phone line of a United States citizen and gathered information regarding a shipment of illegal drugs into the United States.[65] The government agreed that the actions of the officials resulted from a joint investigation, and thus, the Fourth Amendment applied.[66] To determine whether the search was reasonable, the court first looked to the foreign law under which the wire taps were obtained.[67] Under Philippine law, the local officials did not meet the requirements for obtaining a wire tap. Because of this, the search did not comply with Philippine law and, therefore, was not reasonable under the Fourth Amendment.[68]

Failure to follow foreign law, however, did not end the court's inquiry. The court noted that while Philippine law governed the search itself, United States law governed whether evidence illegally obtained should be excluded.[69] The focus of this inquiry was whether excluding the evidence would deter federal officers from unlawful conduct.[70] Following a good faith exception to the exclusionary rule, the court reasoned that the United States officials reasonably believed that their conduct was legal because they believed that Philippine officials had complied with Philippine law in obtaining the wire taps.[71] Thus, the conduct that violated the Fourth Amendment was committed by foreign officials. Because the United States officials believed the action

61. Reid v. Covert, 354 U.S. 1 (1957) (finding that a treaty's authorization of power by the United States over a United States citizen is still constrained by the Constitution).

62. *Powell*, 366 F.2d at 640 (quoting *Reid*, 354 U.S. at 16).

63. United States v. Peterson, 812 F.2d 486 (1987).

64. *Id.* at 487.

65. *Id.* at 488.

66. *Id.* at 490.

67. *Id.* at 490–92.

68. *Id.* at 491.

69. *Id.*

70. *Id.*

71. *Id.* at 492.

was legal, the violation could not be imputed to them under the good faith exception to the exclusionary rule.[72]

A federal district court again allowed a good faith exception for Fourth Amendment violations in *United States v. Juda.*[73] In *Juda,* the defendant planned to smuggle illegal drugs into the United States.[74] Australian officials installed a tracking device in the defendant's boat, at the request of United States officials, to track the boat's voyage to North America.[75] The Australian agents assured the United States officials that no warrant was needed under Australian law to install a tracking device on the boat.[76] The court pointed out that, although a warrant from a United States court would not have legal effect, it would provide evidence of probable cause and would detail the scope of the search.[77] The court noted, however, that procuring a warrant for a search outside the United States is still a controversial issue that many courts consider beyond their jurisdiction.[78] Thus, the legal compliance required in such situations is compliance with foreign law.[79] Because of the Australian officials' assurance that their actions were in compliance with Australian law, the court found, as in *Peterson,* that the search fell under a good faith exception to the warrant requirement.[80] In both cases, whether the Fourth Amendment could provide any protection turned on whether United States officials were conducting the unreasonable search or seizure. As long as the United States officials did not conduct the unreasonable search or seizure, they had to prove only that they reasonably believed that the foreign officials were following foreign law, regardless of how minimal that standard of foreign law may be.

Most recently, the Ninth Circuit considered how to apply the Fourth Amendment to United States officials' actions overseas in *United States v. Barona.*[81] The defendants conspired to smuggle cocaine into the United States.[82] While they were in Denmark,

72. *Id.*
73. 797 F. Supp. 774 (N.D. Cal. 1992).
74. *Id.* at 780.
75. *Id.* at 776.
76. *Id.* at 782.
77. *Id.*
78. Such an action may be viewed as seeking to project United States law on other countries; whereas, the goal is simply to limit the actions of United States officials, regardless of the location. *Id.*; *see also* FED. R. CRIM. PRO. 41(a) advisory committee notes.
79. *Juda,* 797 F. Supp. at 782.
80. *Id.* at 783.
81. 56 F.3d 1087 (9th Cir. 1995).
82. *Id.* at 1089.

Danish authorities tapped a public telephone near the hotel in which they stayed.[83] The court found that the investigation was a joint venture between United States and Danish officials.[84] Because of the joint investigation, the court considered whether the search was reasonable by examining whether Danish law was followed.[85] The court ended its discussion of the reasonableness of the search by concluding that Danish law was followed; therefore, the search was reasonable under the Fourth Amendment.[86]

Judge Reinhardt's dissent, however, points out that Danish law does not require probable cause to obtain a wire tap.[87] Even though the investigation was a joint venture, United States officials were allowed to meet a lower standard than what is required for obtaining a warrant in the United States. By looking solely to foreign law to establish that the search was reasonable under the Fourth Amendment, the court removed the probable cause requirement of the Fourth Amendment, leaving it "without any real force."[88] Judge Reinhardt cautioned that foreign law has gone from being a factor in previous cases to being determinative for finding that a search was reasonable.[89] In fact, because of the good faith exception discussed in *Peterson* and *Juda*, United States officials need only a good faith belief that foreign officials complied with foreign law.[90] This leaves a standard for the Fourth Amendment that is lower than even foreign law requirements.

Yet this was not the intent of the *Peterson* court. The *Barona* court's focus on foreign law mischaracterizes *Peterson*. In *Peterson*, the court noted that the Philippine law for obtaining a warrant contained the same probable cause requirement.[91] Therefore, United States officials could reasonably believe that their actions were legal, because they believed that Philippine officials had followed their own law that required probable cause. In *Barona*, however, the foreign law did not include a probable cause requirement. Thus, federal agents could not reasonably believe that a United States court would consider their actions legal. Instead of noting this distinction, the *Barona* court allowed the Fourth Amendment protection to be eroded further by allowing

83. *Id.* at 1090.
84. *Id.*
85. *Id.* at 1095.
86. *Id.* at 1096.
87. *See id.* at 1099 (Reinhardt, J., dissenting).
88. *Id.*
89. *Id.*
90. *Id.* at 1090.
91. United States v. Peterson, 812 F.2d 486, 491 (1987).

foreign law, even without a probable cause requirement, to become the standard. Allowing United States officials to follow the lower standards set by foreign governments becomes even more troubling in light of remote searches, which will be discussed in Section III.

B. *Noncitizens Without Substantial Connections to the United States*

The concept of "substantial connections" is grounded in principles of immigration law.[92] With respect to the Fourth Amendment, however, courts have not yet developed what constitutes a substantial connection to the United States.[93] As the following discussion indicates, it is not clear whether a noncitizen can have substantial connections to the United States.[94] While the Fourth Amendment constrains United States officials acting against United States citizens, even when the United States citizen is not in the United States, courts have found no Fourth Amendment protection from United States officials for noncitizens, either in foreign countries or in the United States.

In *United States v. Verdugo*,[95] the Supreme Court considered whether the Fourth Amendment applies to United States officials acting outside the United States against noncitizens.[96] Verdugo was arrested in Mexico by Mexican officials and brought to the United States. After his arrest, the Drug Enforcement Agency ("DEA") and Mexican officials searched Verdugo's home in Mex-

92. *See* Fletcher N. Baldwin, Jr., *The Rule of Law, Terrorism, and Countermeasures Including the USA PATRIOT Act of 2001*, 16 FLA. J. INT'L L. 43, 85 (2003). Based on a theory that grants plenary power over immigration to Congress, courts enter the realm of immigration law only when absolutely necessary. *See* Chae Chan Ping v. United States, 130 U.S. 581 (1889) (holding that the authority over immigration is an exercise of sovereignty vested in the executive branch). Courts feel much more comfortable to point out the separation of powers and the connection of immigration to foreign affairs, thus leaving most decisions completely within the discretion of the executive branch. STEPHEN H. LEGOMSKY, IMMIGRATION AND REFUGEE LAW AND POLICY 121 (3d. ed. 2002). One may have difficulty finding another area of law in which courts so willingly limit judicial review. *See* Ryan Goodman & Derek Jinks, *Toward an Institutional Theory of Sovereignty*, 55 STAN. L. REV. 1749, 1787 (2003); *see also* Sarah H. Cleveland, *Powers Inherent in Sovereignty: Indians, Alien, Territories, and the Nineteenth Century Origins of Plenary Power Over Foreign Affairs*, 81 TEX. L. REV. 1, 80 (2002).

93. Miller, *supra* note 54, at 882.

94. Arguably, a noncitizen with substantial connections to the United States should receive the protection of the Fourth Amendment; however, all courts that have considered this question have found that a substantial connection did not exist. *See infra* notes 111–114 and accompanying text.

95. 494 U.S. 259 (1990).

96. *Id.* at 261.

ico.[97] Verdugo sought to have the evidence obtained from the search suppressed, because the DEA did not have a warrant to search his house.[98] The District Court and the Ninth Circuit Court of Appeals agreed that the evidence should be suppressed.[99] The Ninth Circuit viewed the Constitution as the only source of power for the government, making the Fourth Amendment an absolute restriction on the government's power.[100] Under this theory, it was of no consequence whether the power was used in the United States or aboard, or whether the defendant was a United States citizen or a noncitizen. In any circumstance, federal agents were limited by the Fourth Amendment. Based on this reasoning, a grant of power given to foreign governments by an international treaty would not aid the ability of the United States to pursue criminals beyond its borders. Because the Fourth Amendment follows U.S agents to foreign lands, they still need a warrant to search a house in a foreign country.

The United States Supreme Court disagreed.[101] In reversing the trial and appellate courts, the Supreme Court looked to the unique phrasing of the Fourth Amendment.[102] While the Fifth and Sixth Amendments refer to the "accused" and to a "person," the Fourth Amendment applies to "the people."[103] The Court considered this phrasing to be a term of art that applied only to those with the power to form the government: those who had socially contracted to be subject to its powers.[104] While the protections of the Fifth and Sixth Amendments applied to everyone in American courts, the Fourth Amendment applied only to United States citizens, regardless of location. Until the *Verdugo* court emphasized the wording "the people," the Fourth Amendment was assumed to also cover noncitizens within the United States.[105] Now, the question of whether noncitizens within the United States receive any protection from the Fourth Amendment remains unanswered.

The Court also focused on the unique purpose of the Fourth Amendment.[106] While the Fifth and Sixth Amendments

97. *Id.* at 262.
98. *Id.* at 263.
99. *See* United States v. Verdugo-Urquidez, 856 F.2d 1214 (9th Cir. 1988).
100. *Id.* at 1217.
101. *Verdugo*, 494 U.S. at 264.
102. *Id.*
103. *Id.* at 265.
104. *Id.*
105. Daniel J. Capra, *Prisoners of Their Own Jurisprudence: Fourth and Fifth Amendment Cases in the Supreme Court*, 36 VILL. L. REV. 1267, 1322 (1991).
106. *Verdugo*, 494 U.S. at 264.

protect a person at trial, the Fourth Amendment protects the home or private property of the person. A Fourth Amendment violation is fully accomplished at the time of an unreasonable governmental intrusion, regardless of whether the evidence seized is sought for use in a criminal trial.[107] By this distinction, one can see that the Fourth Amendment's function is to protect "the people" from their government. Hence, those who did not provide the power to the government do not receive this protection from the government.[108] Just as the foreign affairs doctrine allows the executive branch virtually unlimited power to interact with other countries, denying Fourth Amendment protection to noncitizens allows the government to interact with the international community the same as any other foreign government would interact. Thus, treaties affecting the ability of the United States to conduct searches in foreign countries are not hindered by the Fourth Amendment.

In determining who constitutes "the people" protected by the Fourth Amendment, the Court looked at whether a noncitizen had substantial connections to the United States.[109] Because Verdugo's only connection to the United States was that he was brought here and detained for trial, the Court did not consider this a substantial connection. The Court suggested that a substantial connection could only arise from a voluntary and lawful presence within the United States.[110] The Court, however, did not articulate any standard for determining what type of presence is voluntary or lawful for purposes of Fourth Amendment protection.[111] The Court concluded that Verdugo's presence in the United States was not voluntary; thus Verdugo was not a part of "the people" receiving protection under the Fourth Amendment.

The Court's emphasis on a term of art and the need for substantial connections to the United States has left open whether anyone who is not a United States citizen can be considered one of "the people."[112] If not, then whether the Fourth Amendment would protect a noncitizen living in the United States remains

107. *Id.*

108. Michael J. Wishnie, *Immigrants and the Right to Petition*, 78 N.Y.U. L. REV. 667, 675 (2003) (arguing that immigrants are dissuaded from contacting law enforcement because of the lack of constitutional protection).

109. *Verdugo*, 494 U.S. at 271.

110. *Id.* at 271–72.

111. *The Supreme Court, 1989 Term—Leading Cases*, 104 HARV. L. REV. 129, 276–77, 281 (1990).

112. *Cf.* Victor C. Romero, *The Domestic Fourth Amendment Rights of Undocumented Immigrants: On* Guitterez *and the Tort Law/Immigration Law Parallel*, 35 HARV. C.R.-C.L. L. REV. 57, 74 (2000) (discussing a district court's application of

unsettled. The Ninth Circuit discussed this problem in *Barona*.[113] Some of the defendants that were claiming United States officials had violated the Fourth Amendment were resident aliens. The court pointed out that, based on *Verdugo*, resident aliens may not have sufficient substantial connections to afford them Fourth Amendment protection.[114] The court noted, "[w]e could hold, therefore, that [the defendants] have failed to demonstrate that, at the time of the extraterritorial search, they were 'People of the United States' entitled to receive the 'full panoply of rights guaranteed by our Constitution.'"[115] Because the court found that the Fourth Amendment was not violated, it did not decide whether permanent aliens received Fourth Amendment protection.

Additionally, in *United States v. Gorshkov*,[116] a federal district court's interpretation of voluntary and lawful presence emphasized that these terms are not as self-defining as they first appear. Gorshkov hacked into business computers from his computer in Russia. After much investigation, the FBI set up a "sting" computer company in Seattle. Gorshkov and another hacker flew to Seattle to demonstrate their computer hacking ability to this company. Gorshkov accessed his computer in Russia on the laptop provided to him by these undercover FBI agents for his demonstration. The FBI had installed a "sniffer" program on the laptop to record all key strokes made by Gorshkov. After they arrested Gorshkov, the FBI used the information from the laptop to download files contained on Gorshkov's computer in Russia. The FBI "seized" the evidence from the Russian computer without obtaining a search warrant because of fear that a partner of Gorhskov's in Russia would delete the evidence before the agents obtained a search warrant.

The court considered whether the Fourth Amendment applies to this "seizure," as well as whether the "seizure" was reasonable under the Fourth Amendment. Based on *Verdugo*, the court determined that the Fourth Amendment did not apply to Gorshkov. Although his entry into the United States was voluntary, the court determined that one entry into the United States "for a criminal purpose is hardly the sort of voluntary association

---

Verdugo's "indeterminate test" in *United States v. Guitterez*, No. CR 96-40075 SBA, 1997 U.S. Dist. LEXIS 16446 (N.D. Cal. Oct. 14, 1997)).

113. United States v. Barona, 56 F.3d 1087, 1094 (9th Cir. 1995).

114. *Id.* at 1093–94.

115. *Id.* at 1094.

116. United States v. Gorshkov, No. CR00-55-C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

with this country that should qualify Defendant as part of our national community for purposes of the Fourth Amendment."[117]

The treatment of substantial connections in *Gorshkov* emphasizes the loophole that the *Verdugo* court opened in applying the Fourth Amendment. If a lawful entry into the United States is required, *Verdugo* would provide illegal immigrants with no protection against unlawful searches.[118] Yet the problem with allowing this limit on protection is that, while searching the house of an illegal immigrant, federal officials could easily violate the rights of one who has a substantial connection to the United States.[119] Allowing a lower standard for anyone residing in the United States could lead to more violations of the rights of United States citizens.

Because of the problems in determining how the Fourth Amendment applies to (1) new technology and to (2) citizens and noncitizens not necessarily in the United States, applying the Fourth Amendment to remote searches becomes even more difficult. Yet, if courts do not adequately address the complications raised by remote searches, they may leave the Fourth Amendment a hollow shell of protection that provides no shield for citizens against unreasonable government actions. Due to the high probability that federal officials will not know who is affected by a remote search, courts must be extremely careful to limit the government's ability to conduct remote searches that are not subject to the Fourth Amendment. For example, an official may know that a particular computer is used by a noncitizen suspect. But if the computer is also used by a citizen, the search would violate the Fourth Amendment. For this reason, courts should apply the protection of the Fourth Amendment to remote searches regardless of the technology that is employed by the government or the criminal.

III. APPLYING THE FOURTH AMENDMENT TO REMOTE SEARCHES

Remote searches present a unique combination of Fourth Amendment jurisprudence and questions of jurisdiction. Whether a remote search will constitute a "search or seizure" depends upon the approach applied to technology. The ways in which government action can be limited are also affected by whether the investigation involves a foreign power or foreign jurisdiction.

117. *Id.* at *3.
118. *See* Scaperlanda, *supra* note 46, at 241.
119. *Id.* at 242.

A. *Foreign Affairs*

The first question raised is who has the jurisdiction to investigate international Internet crimes. Because many articles have discussed the jurisdictional problem in depth,[120] only a summary of these debates is necessary to provide the correct foundation for international remote searches. Much debate has centered on whether the nation affected most by the crime should be allowed to seek enforcement of its laws beyond its borders.[121] Some argue that the country in which the criminal is residing should control any investigation within its own borders.[122] These problems are magnified by the fact that most evidence of Internet crimes can disappear rapidly. The country that has been injured by a crime has started an investigation unsure where the evidence may lead. Once the investigation leads to another country, the investigating country may have to get approval from that country to continue the investigation.

Understandably, most countries are leery of allowing foreign governments to conduct searches within their own country, especially considering that different nations have different laws with which they must comply during an investigation. Yet this takes significant time during which crucial evidence may disappear.[123]

The second consideration is what laws or regulations should apply to the investigation.[124] As discussed earlier, constitutional limitations do not extend to the government's actions against non United States citizens in other countries. Additionally, the

120. *See, e.g.*, Patricia L. Bellia, *Bits Across Borders*, 2001 U. CHI. LEGAL F. 35 (examining the principles of international law involved with the discussion of Internet jurisdiction and arguing that any agreement with the United States should comport with the Fourth Amendment); Jack Goldsmith, *Against Cyberanarchy*, 65 U CHI. L. REV. 1199 (1998) (maintaining that Internet transactions should be governed the same as any other transaction); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996) (arguing that a separate international jurisdiction is needed to govern the Internet).

121. Bellia, *supra* note 120, at 79–80.

122. Stein, *supra* note 2, at 403–04.

123. Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425, 427–28 (2003). To alleviate this problem, the United States met with numerous European countries to propose a treaty that would allow foreign investigation of Internet crimes in those counties which agree to the treaty. *Id.* at 429. This pooling of jurisdiction could greatly increase law enforcement's ability to capture Internet criminals.

124. The treaty would alleviate some of these problems because it contains provisions that are similar to the Constitution. *Id.* at 435. While discussion of this issue may be more theoretical, this treaty has not yet been ratified and later developments with conflicting jurisdictions may not necessarily start from this baseline. *Id.* at 426.

actions of foreign officials are not restricted by the Fourth Amendment. Based on the current interpretation of the phrase "the people," foreign officials could conduct an investigation in the United States free from constitutional restraint as well.[125] The United States' commitment to a particular legal order should eliminate this problem. For even if courts have left open the possibility that foreign searches on United States soil need not comply with the Fourth Amendment, policy considerations should prevent the United States from entering into any such agreement.[126]

The cases addressing cross border searches reveal the willingness of courts to find no Fourth Amendment protection, especially when a search involves foreign officials. The problem that arises is that if federal agents do not follow the Fourth Amendment while conducting searches in other countries, the United States may not be able to expect the foreign government to follow the Fourth Amendment while in the United States.[127] Legally, they may not have to.[128] The treaties into which the United States enters could become more prevalent as technology continues to add to the problem of jurisdiction. While well-meaning law enforcement officials may constitute a dangerous encroachment upon constitutional protections, well-meaning foreign officials are an even greater threat.

The solution is to require a higher standard of all government actors. To keep constitutional protections from suffering at the hands of foreign governments, United States officials should be willing at least to follow foreign law in other countries. Instead, they currently just have to show that they *believed* the foreign government followed foreign law, not that it did follow the law. Alternatively, United States officials should follow the Fourth Amendment, regardless of the location or the subject of the search. Otherwise, the United States may set a standard for international investigations that falls short of how it is required to act toward its own citizens. Such a situation could potentially create even more problems for international investigations of

125. *Cf.* D.C. Kennedy, *In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty*, 9 RICH. J.L. & TECH. 1, 24 (2002) (discussing the expanded investigative powers foreign states would enjoy under the Council of Europe's proposed cybercrime treaty).

126. Peter J. Spiro, *Treaties, International Law, and Constitutional Rights*, 55 STAN. L. REV. 1999, 2005–06 (2003) (examining the historical manner in which constitutional rights have given way to foreign treaties).

127. Justin F. Kollar, *USA PATRIOT Act, Fourth Amendment, and Paranoia: Can They Read This While I'm Typing It?*, 3 J. HIGH TECH. L. 67, 72–73 (2004).

128. *Id.* at 74.

Internet crimes if other governments seek to investigate crimes in the United States under these lower standards.

B. *Domestic Policy*

Jurisdictional questions do not pose the same problem in domestic cases as they do in the international context. State officials may still struggle with this problem, but this is not an issue for federal agents. The issue of substantial connections to the United States, however, looms even larger in the domestic arena.[129] Federal officials often have no idea for whom they are searching on the Internet or whose computer they are remotely searching. Additionally, they may not know how many people use the computer, or whether any of them have substantial connections to the United States.[130] The best solution is to require government officials to meet the same standard for all domestic investigations, regardless of whether the subject of the search is a United States citizen.[131] A federal agent should not be allowed to remotely search a computer without a warrant simply because he believes that the person may not have substantial connections to the United States. Even if a court may allow the evidence if it turned out that no United States citizens had been unreasonably searched, the potential for abuse against United States citizens is strong.[132] Additionally, a Fourth Amendment violation is not dependent upon whether the evidence is excluded from trial; the violation occurs at the time of the search. Thus, the government's authority to conduct remote searches must be limited to avoid violating the Fourth Amendment rights of a United States citizen. Even though Internet crimes are harder to trace at this time, Fourth Amendment protection should not suffer because of this. Allowing current technology to limit the protection of the Fourth Amendment by creating exceptions for remote searches could eliminate Fourth Amendment protection from future technology.

In applying the Fourth Amendment to remote searches, courts must retain flexibility in the Fourth Amendment, rather than following a bright-line rule. For example, the *Gorshkov* court, in addressing whether the search was reasonable under the Fourth Amendment, pointed out that the FBI had probable

129. Miller, *supra* note 54, at 875.

130. *Id.* at 886 (discussing the differences between the Fourth Amendment protection provided to legal and illegal aliens).

131. Brett M. Frischmann, *The Prospect of Reconciling Internet and Cyberspace*, 35 LOY. U. CHI. L.J. 205, 213 (2003).

132. *Id.* at 215.

cause to believe that the evidence would be destroyed before a warrant or assistance from Russian authorities could be obtained. These exigent circumstances allowed for more latitude in seizing data before obtaining a warrant. Additionally, the agents did not examine the information they had downloaded until after the warrant was obtained.[133] Therefore, the agents acted reasonably to ensure Gorshkov's privacy until the judge issued a warrant. Because the evidence could disappear if agents did not act quickly, the seizure was reasonable.[134] The court's consideration of these exigent circumstances reflects a flexible approach to protecting the purpose of the Fourth Amendment.

By focusing this portion of the opinion on the fact that the evidence could disappear quickly, the court left open the possibility that later technology could change this dilemma, thereby eliminating the need for quick retrieval of the data. For example, future technology could reduce the ability of criminals to permanently remove information, or it may one day be easier to track people over the Internet. If the court had determined that the Fourth Amendment could never be applied in these circumstances, the government would have unfettered authority to search over the Internet. This would be similar to the loss of protection following the *Olmstead* decision in which the Fourth Amendment was strictly limited to the home.

Unfortunately, the *Gorshkov* court also determined that the Fourth Amendment still did not apply to the seizure because copying the data did not interfere with the defendant's possessory interest in the data.[135] His control over his copy of the data remained unaffected; thus, his rights had not been violated.[136] This section of the opinion fails to consider the advances in technology. In fact, Justice Brandeis, many years ago, discussed the possibility that one day police may be able to produce secret documents without ever opening drawers.[137] Copying data over the Internet certainly leaves the owner with unfettered access to the original; however, the Fourth Amendment still protects people, not places. Focusing on the owner's ability to control the original data ignores the right to privacy that is violated by the agent copying the data. The court's perception in the first issue and its failure to address even present technology in the second ques-

133. United States v. Gorshkov, No. CR00-55-C, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001).

134. *Id.*

135. *Id.* at *3.

136. *Id.*

137. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

tion underscores the difficulty in applying the Fourth Amendment to technology without creating a rule that will limit its application in the future.

CONCLUSION

Our unique system of government is based upon the proposition that government should be limited to the powers that are granted to it by the people of this nation.[138] In fact, the Bill of Rights embodies this proposition by ensuring that the federal government understands what actions are beyond its power, of which one action is unreasonable searches and seizures. While new methods and new technology place the analysis of the Fourth Amendment in different contexts, these new contexts should not affect the protection provided to the people by the Fourth Amendment.

Flexibility, rather than a bright-line rule, is the key to the vitality of the Fourth Amendment. To adequately protect "the people," regardless of the technology implemented, courts must continue to focus on the principle of protecting "the people." A narrow focus on a past court's application of the Fourth Amendment while losing sight of the principles it sought to protect leaves the Fourth Amendment impotent. While more intrusive investigations may make the United States seem safer for a time, allowing the fear of technology-savvy criminals to overrun personal liberty could emasculate the Fourth Amendment. With changes in technology, the scope of the Fourth Amendment's protection must change, as well, to maintain the proper balance between the power of the police and the protection of the people. As the United States Supreme Court cautioned, "It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties . . . which makes the defense of the Nation worthwhile."[139]

138. John Harrison, *Forms of Originalism and the Study of History*, 26 HARV. J.L. & PUB. POL'Y 83, 86 (2003).

139. United States v. Robel, 389 U.S. 258, 264 (1967) (holding that a statute which made it unlawful to be a member of a Communist organization and be employed by a defense facility was unconstitutional as a violation of the freedom of association).