COMMENT

VERDUGO IN CYBERSPACE: BOUNDARIES OF FOURTH AMENDMENT RIGHTS FOR FOREIGN NATIONALS IN CYBERCRIME CASES

Stewart M. Young[*]

Cite as: Stewart M. Young, Verdugo *in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases*, 10 MICH. TELECOMM. TECH. L. REV. 139 (2003), *available at* http://www.mttlr.org/volten/young.pdf

[*] J.D. Candidate, Stanford Law School, 2004; M.A., Waseda University, 2002; B.A., Princeton University, 2000. I would like to thank Professor Mariano-Florentino Cuéllar for his insightful thoughts and suggestions, Catherine Kiefer of MTTLR for her excellent comments and editing, as well as Ashley Warner for her editing prowess. This Comment is dedicated to my family, and I would especially like to thank my father, Mike Young, for all of the editorial comments, suggestions, and support.

This Comment examines the current legal framework governing Fourth Amendment rights for foreign nationals accused of committing crimes within the United States. Over the past three years, federal courts have tried several cases charging foreign nationals with committing crimes through the use of the Internet; these cases demonstrate a lack of clarity in the standard for warrant requirements regarding these searches. Utilizing these cases, this Comment creates a hypothetical case that presents the issues of Fourth Amendment rights for foreign nationals and seeks to determine how such a question should be answered. It advocates the clear application of United States v. Verdugo-Urquidez to remote cross-border searches conducted by law enforcement officials against foreign nationals. It concludes by introducing several suggestions to clarify the standard implemented by Verdugo for non-remote cross-border searches. In addition, this Comment adds a critical view to the rights that should be accorded foreign nationals when accused of committing crimes through the Internet.

INTRODUCTION

To remark on the extraordinary growth of the Internet over the past decade is to belabor the breathtakingly obvious. Nor does highlighting the equally obvious concomitant growth in Internet crime win anyone points for originality. Still, Internet crime, like its low-tech brothers,

requires investigation. This creates a much less obvious and highly difficult problem, a problem that results from the complex intersection among high-tech criminal activity, high-tech investigative tools, and the United States Constitution.

Unlike most conventional international criminals, cybercriminals never have to enter the jurisdiction of the victim-state to commit their crimes. A person can lounge in the comfort of his own home in Vladivostok, Russia, and commit a crime in Newark, New Jersey, all without braving the rush hour traffic or the occasional blackouts of the East Coast of the United States, indeed, without ever stepping foot in the United States. Of course, as it turns out, police in Newark can also investigate much of this activity without ever needing to brave a Russian winter. Officials can hack into the cybercriminal's computer just as easily as the criminal hacks that of his victims. There is an important difference, however, between the two hackers. Unlike the criminal, the police are still constrained by the Fourth Amendment[1] when applying investigative technologies. Precisely how the Fourth Amendment constrains these investigations is far from obvious and, in this day of increasing technological sophistication on the part of both the police and criminals, it is important to begin to address this issue.[2]

This Comment will examine the application of the protections of the Fourth Amendment to individuals who commit Internet-related crime while residing outside of the jurisdiction of the United States. The principle case addressing this issue is *United States v. Verdugo-Urquidez*.[3] *Verdugo* spawned a particular jurisprudence regarding the Fourth Amendment rights of foreign nationals, but the application of this jurisprudence to searches of a foreign national's computer or servers outside of U.S. territory is not entirely clear.[4] Indeed, even its relevance to cases

1. The Fourth Amendment states that "[t]he 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.

2. This Comment will refer to the terms "Internet", "cyberspace", and the "World Wide Web" interchangeably throughout. Essentially, all three terms have become synonymous, although there are subtle differences among the three terms. However, since most of the academic legal literature on the subject does not make reference to the subtle distinctions between each term, this Comment will use the same practices as other legal journals.

3. 494 U.S. 259 (1990) (holding that U.S. officials did not have to meet Fourth Amendment requirements when conducting a search in a foreign country even if the searched party lacked voluntary connection to the United States). I will refer to this case as "Verdugo" throughout this Comment.

4. For instance, numerous questions abound about what legally constitutes a remote-cross border search within the boundaries of the United States. *See* Patricia L. Bellia, *Chasing*

involving cybercrimes committed by foreign nationals is debatable. *Verdugo*'s facts and holding are easily distinguishable from those cases where evidence is secured by a remote cross-border search.[5]

In Part I, I will propose a hypothetical dealing with cross-border searches against foreign nationals accused of committing Internet-based crimes with effects in the United States. To focus the problem more acutely, this hypothetical is constructed by drawing from two recent cases where foreign nationals were accused of just such criminal activity: *United States v. Ivanov*[6] and *United States v. Zezev*.[7] Part II will discuss *Verdugo*, focusing on the main factors involved in the decision. In Part III, I will apply *Verdugo* to the hypothetical suggested in Part I to determine what Fourth Amendment protections should be provided to the defendant. This section will also discuss the limitations inherent in applying the *Verdugo* holding to our hypothetical case. Finally, Part IV advocates using *Verdugo* to analyze these types of remote-cross border search cases; it also offers clarifying factors for applying the Fourth Amendment to these searches—factors that are attentive to both the unique characteristics of the search and the important values embodied in the Fourth Amendment. This proposed standard derives from the reasoning of *Verdugo* and is consistent with that case's underlying premises; yet it avoids the risks that arise from an expansive interpretation of the *Verdugo* holding. This Comment concludes by encouraging the adoption of the proposed standard in order to better facilitate the detraction of cybercrime while properly protecting the civil rights of those accused.

I. THE RELEVANT PROBLEM AND CREATING THE HYPOTHETICAL

To be perfectly accurate, the development of the Internet and the resulting opportunities for crime have not created a new problem as much

Bits Across Borders, 2001 U. CHI. LEGAL F. 35, 82 n. 152 ("Precisely what the Fourth Amendment requires when the United States conducts a cross-border search of data physically located abroad is a complicated question.").

5. *Id*. ("Verdugo left open the question whether the Fourth Amendment constrains a foreign search by U.S. officials of an individual who has a substantial connection to the United States . . . .").

6. 175 F. Supp. 2d 367 (D. Conn. 2001) (convicting Ivanov of hacking into the Online Information Bureau (an e-commerce business) and extorting money from OIB in exchange for not corrupting its server or business).

7. This case was not reported in Lexis or Westlaw. It was reported on the Department of Justice's Cybercrime website and by the New York Times. *See* Press Release, U.S. Dep't. of Justice, U.S. Convicts Kazakhstan Hacker of Breaking Into Bloomberg L.P.'s Computers and Attempting Extortion (Feb. 26, 2003), *at* http://www.cybercrime.gov/zezevConvict.htm [hereinafter U.S. Convicts Kazakhstan Hacker]; Michael Cooper, *Bloomberg Tells Trial Jury of his Part in Taped Sting*, N.Y. TIMES, Feb. 12, 2003, at B4.

as they have modified and made more difficult an old problem. The Internet permits someone to sit abroad at his computer and commit a crime within U.S. jurisdiction, while never entering the physical boundaries of the United States. This phenomenon is not new, of course. Telephones, telegrams, and facsimile machines have long facilitated transnational communication, speeding not only commerce, but also crime. And foreign companies have long been able to violate our antitrust laws without ever sending even the lowest level employee to the United States.[8]

Logistical complications, however, have generally made it difficult to gather evidence of these traditional crimes when executed abroad.[9] In order to search the London gentlemen's club where a conspiracy is hatched, for example, law enforcement officials would have to travel to England, get past the doorman, and rifle through the club's files or tap its phones. Unless the Federal Bureau of Investigation ("FBI") could tap all the phones in Miami, law enforcement personnel would need to fly to Colombia and tap a drug lord's phone directly. And Federal Trade Commission ("FTC") officials, or their Department of Justice counterparts, would have to eat sushi for a week in Tokyo while searching the business records of a Tokyo company that allegedly violates U.S. antitrust laws. In other words, the U.S. government would have to physically invade an individual's privacy in a foreign country or least travel to that foreign country in order to conduct the search.

In the case of Internet crime, however, U.S. law enforcement officials need not physically enter the territory of another country while they gather evidence against a foreign suspect.[10] They, like their criminal adversaries, can do much of the work from their own computer terminals in the United States. The use of computer technology, therefore, creates a new wrinkle in Fourth Amendment jurisprudence regarding the rights of foreign nationals during law enforcement searches.

---

8. *See* U.S. Dep't. of Justice, Statement Accompanying Release of Revised Merger Guidelines (June 14, 1984), *reprinted in* ELEANOR M. FOX & LAWRENCE A. SULLIVAN, ANTITRUST 925 Appendix B (1989) ("[T]he Guidelines' standards relating to the definition of markets and calculation of market shares will apply equally to foreign and domestic firms.").

9. For instance, the U.S. government had placed FBI offices abroad in a number of countries, with 45 Legal Attache offices and four Legat sub-offices. Although allowing for more interaction with law enforcement abroad, these offices are still generally very small. *See* http://www.fbi.gov/contact/legat/legat.htm (last visited Nov. 13, 2003) (describing the FBI's Legal Attache Program). Additionally, most local police departments and the Securities and Exchange Commission have virtually no logistical presence outside of the United States.

10. Bellia, *supra* note 4, at 77 ("[D]oes the fact that searching officials never enter the target state's territory [when performing a remote cross-border search] convert the affront to sovereignty from an intentional performance of sovereign functions on another state's territory into mere interference with the goals of a regulatory scheme . . . . ").

The purpose of the Fourth Amendment is to uphold a person's reasonable expectation of privacy from governmental searches and other intrusions. It originally dealt only with physical searches by law enforcement,[11] but logic quickly compelled its expansion to protect against any intrusion that violated one's sense of privacy and personal security.[12]

Of course, it was not generally thought that these protections extended beyond the borders of the United States.[13] Foreign nationals living in foreign countries were entitled to privacy to the extent "reasonable" in that country, not in ours. For instance, individual countries have different laws recognizing rights of financial privacy from government intrusion.[14] As such, a citizen may only claim a right to privacy to the extent that one is provided under the laws of that citizen's country. It would not be reasonable for a citizen to claim a heightened right of privacy against government intrusion if their respective countries did not provide for that right. But with foreign nationals committing computer crime against the U.S. government and its citizens in large numbers, and with the U.S. government now able to conduct remote cross-border searches,[15] the application of Fourth Amendment rights is not as straightforward or simple as it used to be.

Over the past three years, the U.S. government prosecuted several cases specifically dealing with foreign nationals committing Internet-related crimes in the United States.[16] In each of these cases U.S. law

11. *See* Olmstead v. United States, 277 U.S. 438, 464 (1928) ("The Amendment itself shows that the search is to be of material things—the person, the house, his papers or his effects.").

12. *See* Katz v. United States, 389 U.S. 347 (1967).

13. "Nowhere is the Fourth Amendment more effective than within the territorial boundaries of the United States . . . it is a well-established principle that the Constitution is of greatest import within the United States." Victor C. Romero, *Whatever Happened to the Fourth Amendment?: Undocumented Immigrants' Rights After INS v. Lopezmendoza and United States v. Verdugo-Urquidez*, 65 S. CAL. L. REV. 999, 1017 (citing In re Ross, 140 U.S. 453, 464 (1898) (stating that the guarantees of the Constitution "apply only to citizens and others *within* the United States") (emphasis added)).

14. Richard Priess, *Privacy of Financial Information and Civil Rights Issues: The Implications for Investigating and Prosecuting International Economic Crime*, 14 DICK. J. INT'L L. 525, 528–529 (1996).

15. The government in both United States v. Ivanov and United States v. Gorshkov utilized remote cross-border searches to gather evidence against the suspects. *See* Press Release, U.S. Dep't. of Justice, Russian Computer Hacker Sentenced to Three Years in Prison (Oct. 4, 2002) [hereinafter Russian Computer Hacker Sentenced], *available at* http://www.usdoj.gov/criminal/cybercrime/gorshkovSent.htm ("A few days after the two men [Ivanov and Gorshkov] were arrested, the FBI obtained access via the Internet to two of the men's computers in Russia. The FBI copied voluminous data from the accounts . . . and examined the data . . . .") (last visited Nov. 13, 2003).

16. *See, e.g.*, Press Release, U.S. Dep't. of Justice, Russian Computer Hacker Convicted by Jury (Oct. 10, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/

enforcement personnel physically present in the United States searched, via the Internet, the alleged criminal's computer or server. In the *Gorshkov* and *Ivanov* cases, the courts allowed the evidence gathered from the search to be presented during trial.[17] Drawing from these cases, one can construct a hypothetical case that is both realistic and calculated to introduce the serious Fourth Amendment problems that these cases are likely to present.

A. *Introduction to the Internet and Cybercrime*

From its rather modest inception as a device to enhance the exchange of scientific information, the Internet has become, without exaggeration, the "Information Superhighway," linking millions, perhaps billions of computers together across the World Wide Web.[18] With these links, however, came the opportunity for criminals to gain appreciably wider access to potential victims and, equally important, their financial information and other resources. Dependency on computers and the networks built around those computers "is growing exponentially," and the "dependency amounts to significant vulnerability . . . [because] computer networks underlie key societal functions as diverse as finance, military command and control, medical treatment, and transportation."[19]

---

gorshkovconvict.htm (reporting on the conviction in United States v. Gorshkov) (last visited Nov. 13, 2003); Press Release, U.S. Dep't. of Justice, Russian Man Sentenced for Hacking Into Computers in the United States (July 25, 2003), *available at* http://www.usdoj.gov/criminal/cybercrime/ivanovSent.htm (reporting on the sentencing in United State v. Ivanov) (last visited Nov. 13, 2003); Press Release, U.S. Dep't. of Justice, Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion (July 1, 2003), *available at* http://www.usdoj.gov/criminal/cybercrime/zezevSent.htm (reporting on the sentencing in United States v. Zezev) (last visited Nov. 13, 2003).

17. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 *1, *6 (W.D. Wash. May 23, 2001) (denying the motion by Gorshkov to suppress the computer data seized by federal agents from two computers located in Russia); United States v. Ivanov, 175 F. Supp. 2d 367, 370 (D. Conn. 2001) ("The defendant and the government agree that when Ivanov allegedly engaged in the conduct charged in the superseding indictment he was physically present in Russia and using a computer there at all relevant times.").

18. The Internet started as a conglomerate of computers networked together in the 1960s under the auspices of the Advanced Research Projects Agency ("ARPA"), a Department of Defense Agency and the predecessor of DARPA ("Defense Advanced Research Projects Agency"). Lawrence E. Evans, Jr., *Internet Overview*, 63 TEX. B.J. 227, 234 (2000). The first linkages of computers consisted of machines at Stanford, UCLA, UCSB and the University of Utah. The development of the World Wide Web occurred when scientist Timothy Berners-Lee developed the system in order to facilitate communication and information sharing between scientists working for the European Laboratory for Particle Physics. Rob A. Reilly, *Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward*, 6 RICH. J. L. & TECH. 6, 23 (1999). *See also* Richard D. Harris, *Trademark and Copyright Law on the World Wide Web: A Survey of the Wild Frontier*, 588 PLI/PAT 553, 557 (2000).

19. Michael N. Schmitt, *Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 886 (1999).

Cases of computer crime and international electronic espionage were reported as early as 1986, as German hackers "attacked computers operated by Lawrence Berkeley Laboratory" and "obtained sensitive information—such as munitions information, information on weapons systems and technical data—and sold it to the KGB."[20] Subsequently, because computer systems are attacked, altered, and hacked with great frequency, the computer savvy of hackers has also increased apace.[21] The cost of technology has decreased significantly, making highly sophisticated equipment available even to those of modest means. This increased availability "means greater numbers of cheap, networked computers [are] available to the criminal elements of society."[22]

Only man's imagination seems to limit the range of crimes that can be committed through the Internet. Internet crimes include "fraud, hate crimes, stalking, gambling . . . money laundering," extortion, vandalism, and espionage, as well as many others.[23] It appears, however, the most frequent crimes are the creation and dissemination of computer viruses and computer hacking.[24] Accordingly, this Comment will focus on a hypothetical case that arises through the commission of either computer hacking or the spread of a computer virus.

20. David Goldstone & Betty-Ellen Shave, *Essay: International Dimensions of Crimes in Cyberspace*, 22 FORDHAM INT'L L.J. 1924, 1926–27 (1999). For an in-depth view of the German hacker case, see CLIFF STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989).

21. *See* Goldstone & Shave, *supra* note 20, at 1927–30 (examining six of the international computer crimes committed by hackers since 1993); *see also* Computer Intrusion Cases, Computer Crime and Intellectual Property Section (CCIPS), *at* http://www.cybercrime.gov/cccases.html (last accessed May 23, 2003) (providing a summary chart of recently prosecuted computer cases as a representative sample, including sixteen of those cases that encompass an international dimension (out of seventy cases posted)) [hereinafter Computer Intrusion Cases].

22. Marc D. Goodman, *Why the Police Don't Care about Computer Crime*, 10 HARV. J.L. & TECH. 465, 467 (1997) (discussing the reasons why domestic law enforcement, particularly the local and state entities, are unable and unwilling to put resources into investigating and prosecuting cybercrime).

23. *Id*. at 469. One can split computer crime into three different categories: computer target crimes, computer tool crimes, and crimes where the computer is merely incident to the actual crime (such as storing information regarding crimes or writing extortion letters on the computer). David Carter, *Computer Crime Categories: How Techno-Criminals Operate*, 64 FBI L. ENFORCEMENT BULL., at 21 (July 1995) (describing these three categories of computer crimes).

24. D.C. Kennedy, *In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty*, 9 RICH. J.L. & TECH. 3 (2002) (discussing Draft 19 of the proposed Cybercrime Treaty drafted by the Council of Europe).

B. *Cybercrime and the Fourth Amendment*

1. The Fourth Amendment Generally

For much of its history, the Supreme Court held that the Fourth Amendment applied only to physical searches of tangible property.[25] In 1967, however, the Court shifted away from a test based solely on physicality and began to define Fourth Amendment protections in terms of an individual's expectations of privacy.[26] Following the logic of *Katz*, the Court necessarily expanded Fourth Amendment rights considerably, with the reasonable expectation of privacy of the individual searched serving as the centerpiece of its analysis.[27] Though commentators have argued that the targeted individual is in the best position to know whether he or she had an expectation of privacy,[28] the Court has generally favored a more objective (rights-based) standard. Such an objective standard requires that the individual's expectation of privacy be one that society would be willing to recognize as reasonable (by allowing legally effective steps to enjoin the invasion of that privacy) and would serve as the basis for a legal right to enjoin law enforcement from conducting a search.[29]

---

25. *See* Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding that the use of a wiretap was not a search of a physical thing and that the Fourth Amendment did not prohibit the conduct of the police because there "was no entry of the houses or offices of the defendants"); Goldman v. United States, 316 U.S. 129, 131 (1942) (holding that the use of a "detectaphone" on the outside of a building did not involve physical trespass and therefore the Fourth Amendment did not apply to the conduct of the officials using that phone).

26. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that wiretapping by the government was prohibited without a warrant). "[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." *Id*.

27. *See* United States v. Knotts, 460 U.S. 276, 280–81 (1983); Smith v. Maryland, 442 U.S. 735, 740–41 (1979). Both cases accepted Justice Harlan's construction of the scope of Fourth Amendment protection in terms of the individual's reasonable expectation of privacy.

28. There are a couple of arguments about the expectation of privacy, among them the statistical-based justification for expectation of privacy and the rights-based (more objective) standard for expectation of privacy. The statistical-based Fourth Amendment conception draws on an "argument that an expectation of privacy is constitutionally 'reasonable' merely because a strong statistical likelihood exists that the information a person seeks to hide from others will remain private." *See* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 506 (2001). The rights-based Fourth Amendment conception allows for the reasonable expectation of privacy if a person has a right to take reasonably effective steps to enjoin the government's invasion of privacy "such as by obtaining an injunction or physically blocking a government search." *Id*. at 507–08. Kerr states that academic literature notes both types of conceptions, but that the "majority of the Supreme Court has consistently adopted a rights-based approach." *Id*.

29. *Id*. at 509–10. These cases include Florida v. Riley, 488 U.S. 445 (1989) (holding that agents in helicopters in public airspace did not need a warrant to view into defendant's

Under the current standard, the government may conduct searches in a number of circumstances without the express permission of the defendant.[30] Additionally, at trial the government may use information that the targeted individual has shared with a third party.[31] Current Fourth Amendment jurisprudence requires that "a warrant be obtained for any domestic criminal search of a home or business, unless there are exigent circumstances."[32] This latter exception allows a court to admit evidence as long as there is probable cause for the search and "a warrant cannot be obtained because of time and emergency."[33] Otherwise, the government is required to secure a warrant from a magistrate before conducting the search.[34]

2. Computers, Networks, and the Fourth Amendment

The Supreme Court has recognized that Fourth Amendment protections are generally required for physical searches and for searches conducted using new technologies.[35] Thus, the pivotal issues are the

property), United States v. Jacobsen, 466 U.S. 109 (1984) (holding that performing a field test on a legally seized substance did not require an additional warrant), and California v. Ciraolo, 476 U.S. 207 (1986) (holding that like *Jacobsen*, agents in planes in public airspace did not need a warrant to view into defendant's uncovered property).

30. Searches conducted at the border are deemed reasonable without any examination of the expectation of privacy. *See generally* Roberto Iraola, *Terrorism, the Border, and the Fourth Amendment*, 2003 FED. CTS. L. REV. 1, II.5 (2003) (exploring "the Fourth Amendment's exception for routine searches and seizures occurring at the border"); *see also* Michael Mello, *Friendly Fire: Privacy vs. Security After September 11*, 38 CRIM. L. BULL. 367, 376 (2002) ("[I]f a search occurs pursuant to probable cause and a warrant (or if the facts come within an exception to either or both of these requirements), then that search will be deemed 'reasonable' and therefore constitutional.").

31. Kerr, *supra* note 28, at 510–11. These cases include United States v. Hoffa, 385 U.S. 293 (1966) (holding that informant disclosures from a third party did not violate the Fourth Amendment); United States v. Matlock, 415 U.S. 164 (1974) (holding that consent by another party living in the same house to search the premises was not a violation of the defendant's Fourth Amendment rights). *But see* United States v. Sledge, 650 F.2d 1075, 1077–78 n.4 (9th Cir. 1981); United States v. Miller, 425 U.S. 435 (1976) (holding that information revealed to a third party and disclosed to the government did not result in Fourth Amendment violations to the defendant).

32. Ruth Wedgewood, *Decision: Extraterritorial Jurisdiction*, 84 AM. J. INT'L L. 747, 747 (1990) (citing to decisions by the U.S. Supreme Court, specifically Michigan v. Tyler, 436 U.S. 499 (1978) and McDonald v. United States, 335 U.S. 451 (1948) and discussing the *Verdugo* case as a recent development of extraterritorial jurisdiction on the applicability of constitutional restraints to U.S. officials acting abroad).

33. *Id*. at 747–48.

34. C. Ryan Reetz, *Warrant Requirements for Searches of Computerized Information*, 67 B.U. L. REV. 179, 184 (1987) ("The warrant requirement is an essential component of Fourth Amendment protection because it prevents the police from conducting searches at will.").

35. Alyson L. Rosenberg, *Passive Millimeter Wave Imaging: A New Weapon in the Fight Against Crime or a Fourth Amendment Violation*, 9 ALB. L.J. SCI. & TECH. 135, 141 (1998) ("In order to keep pace with . . . technological advancements in law enforcement

nature of the technology involved in conducting the search, how the search is conducted, what degree of intrusion is allowable, and what expectations of privacy are reasonable.

In order to more fully understand the conditions and limitations of constitutional searches with respect to the Internet, it is necessary to understand the fundamentals of Internet functionality and data storage on computers. All data is stored in binary form somewhere on some computer. In this sense, there is a physical depository of data. In our hypothetical, we will posit that the binary data and relevant codes are physically stored in a computer located in a foreign country.[36]

But one might argue that such data is also part of the mystical network of the Internet and, in that sense, it is stored everywhere, not necessarily just on the computer server in the United States or in a foreign country.[37] Thus, in addition to a physical search of an actual computer, law enforcement officials can also search the network used to commit the crime or search through the network into another server to which another computer is connected and upon which the desired data is stored.

One might argue that by extrapolating current Fourth Amendment doctrine it should apply to searches of these networks as well. *Katz*, for example, holds that Fourth Amendment protections are not solely limited to the physical search of physical locations.[38] *Katz* might extend to searches that are conducted through the use of technology that garners information, but which do not physically intrude into the target's home, office or other space. It is therefore important to define the precise nature and form of a search of the Internet or a computer network.

One view is that searches via the Internet or searches of networks do not require investigators to search any physical space and thus are not

---

surveillance, courts are forced to reconsider the scope of Fourth Amendment protections. In determining whether technology used by law enforcement officials constitutes a Fourth Amendment search, courts rely on the two-part test articulated by Justice Harlan . . . .").

36. Of course, we are not concerned about data that is physically stored in binary form on a computer located in the United States because with a physical search of a computer on which the police can actually get their hands, warrants are required just like in most other physical searches. *See generally* Reetz, *supra* note 34 (discussing Fourth Amendment requirements for searching computer records generally, and specifically mentioning the use of telephone access and warrant requirements for that access).

37. One court has stated that the "Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks." ACLU v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996). This means that it is a "network of networks." *See* Jennifer Hamilton, *Recent Development: Playboy Enterprises v. Chuckleberry Publishing*, 5 TUL. J. INT'L & COMP. L. 521, 521 (1997) (citing ACLU v. Reno). This "network of networks" can virtually exist everywhere, thereby allowing data to be stored along the network without actually residing in one area.

38. United States v. Katz, 389 U.S. 347, 359 (1967).

"searches" for the purposes of the Fourth Amendment. The opposite view is that a physical search does occur because the data and information, whether in a physical computer, a server network, or the Internet, still exists physically within a computer hard drive or server. This type of search is one step removed from tangible searches of a physical location; one might argue that such a search would be entitled to consideration under Fourth Amendment jurisprudence. Additionally, new technologies within computers, such as encryption devices for computer messages and files, raise the distinct possibility that wherever the data is actually stored, the owners of the data have expectations regarding privacy that might be deemed reasonable by the courts.

C. *Constructing the Hypothetical*

1. Recent Cases Involving International Cybercriminals and the Fourth Amendment

Two relatively recent cases offer an intriguing perspective on the treatment of foreign nationals relating to crimes committed through the use of computers and the Internet. In the most recent, a Russian national illegally gained access to a financial services website and then attempted to extort money by threatening to reveal his ability to gain access to all the financial services company's information.[39] Oleg Zezev successfully gained access to the server that contained all the Bloomberg Financial L.P. intranet information and developed a capacity to control all levels of information on the company's site.[40] This latter kind of access is called "root access."[41] After gaining access, Zezev sent messages under the name "Alex," stating that unless he received $200,000, he would reveal to the media his ability to gain complete and unfettered access to, and control of, the Bloomberg computer system.[42] By arranging a meeting in London between Zezev and Michael Bloomberg himself, U.S. officials

39. United States v. Zezev was decided on February 26, 2003, but has not yet been reported into either Lexis or Westlaw. The facts of the case and summary can be found on the Internet in the Department of Justice Cybercrime website. *See* U.S. Convicts Kazakhstan Hacker, *supra* note 7.

40. *Id*. Zezev gained access to legitimate employee and customer accounts, including Michael Bloomberg's personal account, copying internal emails, information, and Bloomberg's personal credit card numbers.

41. "Root access is a descriptive term meaning that the user is recognized as a system administrator and consequently obtains the authority to change passwords or destroy data-authority that normal users do not have." Reid Skibell, *Cybercrimes & Misdemeanors: A Re-evaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 925 (2003).

42. U.S. Convicts Kazakhstan Hacker, *supra* note 7. After concluding that the claims by "Alex" were correct, Bloomberg computer specialists fixed the computer server code so that he would not be able to subsequently access Bloomberg computers.

arrested Zezev and an accomplice and extradited them to the United States to stand trial. Zezev was subsequently convicted of several computer crimes.[43] According to the facts of this case, Zezev gained access by routing his hacking through a number of different countries into a computer server in the United States.[44] Despite his intentions to access information in the United States, at no time did Zezev enter the United States or otherwise subject himself to personal jurisdiction based on his location.[45]

United States v. Ivanov raises similar questions about what Fourth Amendment protections should be accorded to foreign nationals outside the United States.[46] Ivanov, along with an accomplice (Gorshkov from *United States v. Gorshkov*),[47] illegally gained accessed to a number of online service providers and e-commerce businesses, obtaining passwords and server access to these websites and computer systems.[48] Once they obtained these codes and passwords, Ivanov and Gorshkov threatened to destroy merchant computer systems and account databases unless they received a $10,000 payment to make each computer system secure.[49] In order to apprehend them, the FBI constructed a computer security firm called "Invita" and invited Ivanov and Gorshkov to travel to the United States to showcase their skills.[50] In the job interview, they were encouraged to show how they could illegally gain access to an

43. *Id*.

44. Press Release, U.S. Dep't. of Justice, Three Kazak Men Arrested in London for Hacking into Bloomberg L.P.'s Computer System (Aug. 14, 2000), *available at* http://www.usdoj.gov/criminal/cybercrime/bloomberg.htm (last visited Nov. 13, 2003).

45. *Id*.

46. 175 F. Supp. 2d 367 (D. Conn. 2001). This is the primary published case against Aleksey Vladimirovich Ivanov. There are three additional cases against Ivanov based in the Western District of Washington, the Central District of California, and the Eastern District of California. *See* Press Release, U.S. Dep't. of Justice, Russian Computer Hacker Indicted in California for Breaking Into Computer Systems and Extorting Victim Companies (June 20, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/ivanovIndict2.htm ("In addition to the charges brought today in California, Ivanov faces computer intrusion and fraud charges in Seattle and Connecticut.") (last visited Nov. 13, 2003).

47. Russian Computer Hacker Sentenced, *supra* note 15 (discussing Gorshkov's sentence for computer intrusion charges); *see also* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 *1 (W.D. Wash. May 23, 2001) (deciding that the Fourth Amendment does not apply to remote-cross border searches because the Russian defendant did not have a reasonable expectation of privacy and because the computer searched was physically in Russia). Judge Coughernour essentially glossed over the issues regarding a remote-cross border search and did not consider the *Verdugo* factors in deciding this order. *Id*. at *3–4.

48. *Ivanov*, at 369.

49. *Id*.; *see also* Press Release, U.S. Dep't. of Justice, Russian National Indicted on Computer Intrusion Charges (Aug. 16, 2001), *at* http://www.cybercrime.gov/ivanovIndict3.htm (last visited Nov. 13, 2003) [hereinafter Russian National Indicted].

50. Russian National Indicted, *supra* note 49.

FBI-created website.[51] With FBI agents watching, the hackers worked. What Ivanov and Gorshkov did not know, however, was that a special, FBI-installed keystroke program recorded the information the hackers put into the computer. The Russians accessed their own server networks in Russia in order to access the FBI-created website.[52] Once the "job interview" ended, agents arrested Ivanov and Gorshkov and indicted them on charges of computer intrusion.[53] Subsequently, the government used the information gathered during the "Invita job interview" to access the Russian hackers' own servers and files in Russia for evidence to be used in their trials.[54] With the data that the FBI provided during their trials, both Ivanov and Gorshkov were found guilty of computer intrusion and other crimes associated with that intrusion.[55]

2. Creating the Hypothetical

Taking these cases as a base, one can easily imagine a hypothetical that raises important and difficult questions about the application of the Fourth Amendment to searches conducted against foreign nationals who reside on foreign soil. Imagine a scenario in which Russian nationals, located in Minsk, gain illegal access to company computer servers along the Dulles Technology Corridor in Northern Virginia. These foreign nationals access a number of important documents and bank accounts within each company. In some manner, the FBI is able to take custody of these alleged criminals when they come to visit a friend in Portland, Maine. The FBI, while stationed at computers physically located in the United States, gains access to the Russians' own servers physically located within Russia, locating a number of documents and programs used

51. Ariana Enjung Cha, *A Tempting Offer for Russian Pair; The Bait: Chance for Jobs in U.S.*, WASH. POST, May 19, 2003, at A1. ("To catch Ivanov, U.S. authorities couldn't very well go to Russia and grab him so they had to figure out a way to get him here . . . the FBI was working behind the scenes to try to get the hackers to a place where they could be arrested.").

52. *Id*. ("[T]he hackers were asked to prove their skills. The FBI secretly videotaped the encounter.").

53. 18 U.S.C. § 1030 (2000) (Fraud and related activity in connection with computers).

54. Russian Computer Hacker Sentenced, *supra* note 15. "A few days after the two men [Ivanov and Gorshkov] were arrested the FBI obtained access via the Internet to two of the men's computers in Russia. The FBI copied voluminous data from the accounts . . . and examined the data pursuant to a search warrant issued . . . ." *Id*.

55. Although found guilty, Gorshkov tried to bring a motion to suppress the evidence seized through a remote-cross border search from his computer located in Russia. This motion to suppress the seized data was struck down by Judge Coughenour, stating, "The Fourth Amendment does not apply to the agent's extraterritorial access to computers in Russia and their copying of data contained thereon." United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 *1, *3 (W.D. Wash. May 23, 2001). The Judge continues, "Until the copied data was transmitted to the United States, it was outside the territory of this country and not subject to the protections of the Fourth Amendment." *Id*.

to break into the technology companies. All of this is carried out by the federal government without a warrant and without the assistance or knowledge of the Russian government, which presumably has physical jurisdiction over the Russians' computer servers.

To answer fully the Fourth Amendment questions raised by this hypothetical, we must start with the principal case allowing the federal government to search extraterritorially a foreign national's location without securing either permission or a warrant under the Fourth Amendment protections.

II. *UNITED STATES v. VERDUGO-URQUIDEZ* AND THE DEVELOPMENT OF A STANDARD

A. *The Facts of* United States v. Verdugo-Urquidez

In 1990, the United States Supreme Court faced a monumental decision regarding the rights of foreign nationals accused of crimes committed in the United States. The Drug Enforcement Agency ("DEA") believed Rene Martin Verdugo-Urquidez to be "one of the leaders of a large and violent organization in Mexico that smuggles Narcotics into the United States."[56] Mexican police officers, with U.S. Marshals standing by, arrested Verdugo-Urquidez in Mexico and transported him to the United States. Federal officials then arranged to have him tried in federal court in San Diego.[57] After his arrival in the United States, DEA agents began searching the premises of Verdugo-Urquidez's residences in Mexico to obtain evidence for his trial.[58] These DEA agents worked in concert with Mexican police authorities, along with the express permission of DEA authorities based in Mexico, to obtain evidence of drug smuggling and other activities that would be used against Verdugo-Urquidez.[59] Relying on *Reid v. Covert*,[60] the U.S. District Court concluded that the Fourth Amendment "applied to the DEA search because it was a joint venture of the American and Mexican police officers."[61] A divided panel for the Court of Appeals for the Ninth Circuit

56. United States v. Verdugo-Urquidez, 494 U.S. 259, 262 (1990).
57. *Id*.
58. *Id*.
59. *Id*.
60. 354 U.S. 1 (1957) (holding that U.S. citizens tried by the United States military authorities in a foreign country were entitled to the protections of the Fifth and Sixth Amendments). It concluded that "[t]he Constitution imposes substantive constraints on the federal government, even when it operates abroad." United States v. Verdugo-Urquidez, 856 F.2d 1214, 1218 (9th Cir. 1988).
61. Verdugo-Urquidez, 856 F.2d at 1217.

affirmed the District Court's holding.[62] The U.S. Supreme Court granted the Government's petition for certiorari.[63]

The Supreme Court addressed the scope of Fourth Amendment protection afforded to foreign nationals when their property abroad was searched by instrumentalities of the U.S. Government. Offering numerous rationales, most prominently the Court's disinclination to hinder the Executive Branch's foreign activities, the Court held that the Fourth Amendment did not apply to aliens without any "voluntary attachment to the United States" when the search was conducted outside the physical borders of U.S. territory.[64]

The Court emphasized the fact that the search took place outside of the United States. Normally, any resident alien that has property searched within the borders of the United States is accorded the same constitutional protections as a U.S. citizen.[65] Rather than extending these same rights to foreign nationals and their property lying outside of the United States, however, the Supreme Court held that the warrant requirement does not extend to government authorities conducting searches of property held by foreign nationals outside of U.S. jurisdiction. Despite the lack of Fourth Amendment protections to a foreign national in an extraterritorial search by the federal government, the Court indicated that the defendant would still receive his Fifth Amendment due process rights and that this might offset, to some extent, any disadvantage the defendant might suffer from the loss of Fourth Amendment protections.[66] This holding altered the landscape for protections of foreign defendants and significantly liberated criminal investigators operating abroad on behalf of the U.S. government.

B. *The Main Factors of the* Verdugo *Holding*

The *Verdugo* Court emphasized four factors as most relevant to its decision. First, the Court recognized that Verdugo-Urquidez was a foreign national and was in United States custody during the search, but that the search occurred outside of the sovereign territory of the United

62. *Id*.

63. United States v. Verdugo-Urquidez, 490 U.S. 1063 (1989).

64. *Verdugo*, 494 U.S. at 274–75. The Court concluded that "[i]f there are to be restrictions on searches and seizure which occur incident to such American action, they must be imposed by the political branches through diplomatic understanding, treaty or legislation." *Id*.

65. *See e.g.*, Pyler v. Doe, 457 U.S. 202, 211–12 (1982) (holding that illegal aliens are protected under the Equal Protection Clause); Kwong Hai Chew v. Colding, 344 U.S. 590, 596 (1953) (holding that a resident alien is a "person" for the purposes of the Fifth Amendment).

66. "All [of the Justices] would agree, for instance, that the dictates of the Due Process Clause of the Fifth Amendment protect the defendant." 494 U.S. at 278. (Kennedy, J., concurring).

States.[67] Second, DEA agents conducted the search with Mexican authorities present.[68] Third, Verdugo-Urquidez "had no previous significant voluntary connection with the United States" and therefore could not avail himself of the constitutional protections available to other aliens.[69] Finally, since the searches occurred abroad, the foreign affairs power of the Executive Branch was implicated, thus raising the possibility that the opposite decision could hinder the political decisions and the activities of other, co-equal branches of government.[70]

1. Government Action Takes Place Outside of the United States

First among the factors highlighted by the Court was the location of the search. The search by the federal government took place outside of U.S. territory. To distinguish this search from those conducted inside the United States, the Court relied upon *Johnson v. Eisentrager*,[71] which rejected the ability of aliens outside of the sovereign territory of the United States to claim Fifth Amendment rights.[72] Thus, even though the *Verdugo* defendant was in U.S. custody when the search occurred, the physical search itself took place outside of the sovereign territory of the United States. Utilizing a historical argument, the Court stated "that the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory."[73]

The same result can be expected from a "reasonable expectation of privacy" standpoint, although the analysis will differ slightly. A foreign national in another country would only be able to expect the same protections that his country would provide to him or her.[74] Therefore, the

67. *Id*. at 262.

68. *Id*. ("DEA agents working in concert with officers of the MFJP [Mexican Federal Judicial Police] searched respondent's properties in Mexicali and San Felipe and seized certain documents.").

69. *Id*. at 271.

70. *Id*. at 273 ("[T]he result of accepting [Verdugo-Urquidez's] claim would have significant and deleterious consequences for the United States in conducting activities beyond its boundaries.").

71. 339 U.S. 763 (1950).

72. *Verdugo*, 494 U.S. at 269. Since the defendant was within the custody of the United States, the Court stated that he was not to be denied his Fifth Amendment Due Process rights. The Court stated, however, that if the Fifth Amendment (which uses the term "person") is not to be due to aliens outside the United States, then "it would seem even truer with respect to the Fourth Amendment, which applies only to 'the people.'" *Id*.

73. *Id*. at 266.

74. Indeed, it would be odd for a foreign national to expect privacy protections accorded to U.S. citizens in his or her own country if that country does not provide the same privacy protections in its own country that U.S. courts provide to its own citizens.

Verdugo holding's first standard is that the U.S. government must be searching the property of a foreign national located outside of the sovereign territory of the United States.

2. Foreign Government Involvement in the Search

The Court also specifically notes that Mexican police authorities assisted the search of Verdugo-Urquidez's residence. Although the Court does not elaborate, measured reasoning supports the relevance of this factor: A foreign national's expectations of privacy are defined by those protections that his own government affords. If officials from his government are present and approve the search, then the foreign national's reasonable expectations have been considered. In other words, the presence of the Mexican police gave the Court some comfort that the DEA agents were conducting a search in conformity with Mexican law, which, after all, is the most a Mexican citizen residing in Mexico can expect.

In addition, excluding evidence legally gathered in Mexico because the processes of gathering that evidence are illegal in the United States potentially implicates foreign affairs. The Court rightly points out that "we live in a world of nation-states in which our Government must be able to 'function effectively in the company of sovereign nations.' "[75] To overturn a search that was valid in Mexico because it might not be valid in the United States would seriously undermine the notion of nation-state sovereignty. The Court dislikes condoning any federal government activity that might violate the sovereignty of other nations, even within the context of law enforcement searches or seizures.[76] Thus, a relevant factor of any subsequent case applying the *Verdugo* standard is whether the foreign government either facilitated or assisted with the search that occurs outside of U.S. territory.

3. Substantial and Voluntary Connections with the United States

The third point raised by the *Verdugo* Court centered on Verdugo-Urquidez's absence of any substantial connections with the United States. The Court specifically states that "[Verdugo-Urquidez] is an alien who has had no previous significant voluntary connection with the United States . . . ."[77] Verdugo-Urquidez tried to rely upon alien's rights cases in arguing that foreign nationals are able to claim Fourth Amend-

75. *Verdugo*, 494 U.S. at 275 (citation omitted).

76. Indeed, this appeared to be one of the concerns of the Court when it decided United States v. Alvarez-Machain, 504 U.S. 655 (1992).

77. *Verdugo*, 494 U.S. at 266.

ment protections.[78] The Court distinguished those cases by asserting that a foreign national claiming Fourth Amendment rights must have substantial connections with the United States.[79] Even the presence of Verdugo-Urquidez in the United States at the time of the search did not establish a voluntary connection with the United States.[80] The Court stated that a foreign national must possess voluntary connections with the United States in order to receive the same expectations of Fourth Amendment rights enjoyed by U.S. citizens and resident aliens.[81]

The Court did not indicate what significant and voluntary connections would suffice for foreign nationals to claim the desired Fourth Amendment rights.[82] Therefore, subsequent defendants may make myriad arguments to claim such connections.[83]

4. Concerns About the Court Hindering Other Foreign Activities of the Executive Branch

In addition to its concerns about the foreign policy power of the Executive Branch, as well as matters of interstate comity, the Court also notes that the provision of Fourth Amendment protections in this case might hinder other non-law enforcement foreign policy activities of the Executive Branch. The Court notes that "[t]he rule adopted by the Court of Appeals would apply not only to law enforcement operations abroad, but also to other foreign policy operations which might result in 'searches and seizures.'"[84] The Court recognized that the United States frequently employs armed forces on foreign soil and a holding that

78. *Id*. at 270–71. Verdugo-Urquidez cited such cases as Pyler v. Doe, 457 U.S. 202 (1982) (according illegal aliens Equal Protection Clause rights), Wong Wing v. United States, 163 U.S. 229 (1896) (holding that resident aliens enjoyed Fifth and Sixth Amendment rights) and Yick Wo v. Hopkins, 118 U.S. 356 (1886) (holding that resident aliens also enjoyed the protections of the Fourteenth Amendment) to bolster his claim that foreign nationals enjoyed the same constitutional protections as citizens, resident aliens, and illegal aliens.

79. *Verdugo*, 494 U.S. at 273.

80. "[T]his sort of presence [of Verdugo-Urquidez in the U.S.]—lawful but involuntary—is not of the sort to indicate any substantial connection with our country . . . . [R]espondent had no voluntary connection with this country that might place him among 'the people' of the United States." *Id*. at 271–73.

81. *Id*. at 274–75. ("At the time of the search, [Verdugo] was a citizen and resident of Mexico *with no voluntary attachment to the United States*, and the place searched was located in Mexico . . . . [T]he Fourth Amendment has no application.") (emphasis added).

82. Wedgewood, *supra* note 32, at 750. "An alien brought to the United States under arrest has a 'legal but involuntary presence' in the United States and should not be considered as having a sufficient connection to enjoy Fourth Amendment protections against an extraterritorial search." *Id*.

83. See *infra* Part III, evaluating whether a cybercriminal might be able to create such a reasonable expectation through his actions.

84. *Verdugo*, 494 U.S. at 273.

requires the federal government to always protect Fourth Amendment rights of foreign nationals would unnecessarily and inappropriately hamper those activities.[85] Succinctly put, the "[a]pplication of the Fourth Amendment to those circumstances could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest."[86] The Court recognized that it would not be in the best interests of the nation to unduly restrict the ability of the Executive Branch to respond appropriately to geopolitical demands.[87] To put the matter in balance of power terms, in "[s]ituations threatening to important American interests,"[88] it is not appropriate for the courts to impose upon the Executive Branch the same kinds of constitutional constraints that are mandated when the Executive Branch takes action in the domestic sphere. Rather, the Court opined, restrictions on searches and seizures abroad "must be imposed by the political branches through diplomatic understanding, treaty, or legislation."[89]

III. APPLYING THE *VERDUGO* STANDARD TO THE HYPOTHETICAL

In analyzing our hypothetical (based on *United States v. Ivanov*, *United States v. Zezev* and *United States v. Gorshkov*) in light of the *Verdugo* holding, we must start where the Court left off, determining the relevance of the intrusion by the U.S. government on the sovereignty of the foreign country when it conducts Internet and computer searches. We will then examine our hypothetical relative to each of the four *Verdugo* factors discussed in Part II, *supra*. In conclusion, we will see that the *Verdugo* standard can and should be used to determine the Fourth Amendment rights for a defendant in our hypothetical remote cross-

85. *Id*. at 275 ("Situations threatening to important American interests may arise halfway around the globe, situations which in the view of the political branches of our Government require an American response with armed force. If there are to be restrictions on searches and seizures which occur incident to such American action, they must be imposed by the political branches . . . .").

86. *Id*. at 273–74. The Court went on to examine how actions by the federal government in a number of different situations involving aliens abroad would result in "a sea of uncertainty" and that "aliens with no attachment to this country might well bring actions for damages to remedy claimed violations of the Fourth Amendment in foreign countries or in international waters." *Id*.

87. *Id*. at 273–74 ("Application of the Fourth Amendment to those circumstances [of employing armed forces abroad] could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest."); *see also* Wedgewood, *supra* note 32, at 750 ("To require a search warrant for an extraterritorial search would have a harmful effect on U.S. operations abroad, including use of armed forces.").

88. *Verdugo*, 494 U.S. at 275.

89. *Id*.

border search. However, in every case regarding a cross-border search, each factor of the *Verdugo* standard should be carefully analyzed, rather than merely glossing over certain factors.[90] Concurrently, it is clear that future courts must clarify and embellish the *Verdugo* standard in order to provide clear guidance to law enforcement officials when they deal with cybercrime and remote cross-border searches.

A. *Foreign Sovereignty and Computer Network Searches*

One critical question regarding remote cross-border searches afforded only passing attention in *Verdugo* is whether these searches violate a country's sovereignty. Several scholars argue that the Internet is immune from territorial regulation, that it is oblivious to geographical constraints, and should be treated as a different space.[91] Those who maintain this view support the legitimacy of Internet cross-border searches, arguing that "technological change alters the extraterritorial influence of purely territorial action[s]"[92] and that "remote cross-border searches fit into the long-accepted practice of officials in one nation acting within their territory (or from public spaces) to extract information from another."[93]

The diverging view is the argument that "territorial regulation of the Internet is no less feasible and no less legitimate than territorial regulation of non-Internet transactions."[94] But even those who believe

90. *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 *1, *3–4 (W.D. Wash. May 23, 2001); *see also supra* note 55. In *Gorshkov*, Judge Coughenour only stated that since the data was outside physical jurisdiction of the United States the Fourth Amendment did not apply. *Gorshkov*, at *3–4. However, when the defendant brought up the fact that *Verdugo* consisted of a search made by a joint effort with the knowledge of Mexican officials (one of the *Verdugo* factors stated above in Part II.B.2), the Judge merely dismissed this argument, stating: "Nothing in the [*Verdugo*] opinion, however, indicates that the reach of the Fourth Amendment turns on this issue. Therefore, the search of the Russian computers was not protected by the Fourth Amendment." *Id*.

91. *See, e.g.*, David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent": Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055, 1087 (1998) (arguing that the Internet calls for a higher degree of deference to rulemaking within non-geographical and decentralized associations, and that there is efficiency in self-regulation of the Internet space, rather than reliance on governmental associations); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (stating that the creation of the Internet has "undermin[ed] the feasibility—and legitimacy—of laws based on geographic boundaries").

92. Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. CHI. LEGAL F. 103, 111 (2001).

93. *Id*. at 115. Goldsmith ultimately concludes, "the early uses of unilateral extraterritorial enforcement measures should not be viewed as an illegitimate invasion of another nation's sovereignty." *Id*. at 118.

94. Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEG. STUD. 475 (1998). "Territorial regulation of the Internet

individual nation-states may regulate the Internet, at least within their territory, possess differing views on the implications of this regulation on foreign countries' searches for information. There is also the position that this type of search is merely an extension of information gathering, akin to what the United States and other countries have done to each other and in each other's territory for a number of years.[95] But, since it is possible to view a search as an intrusion into that country's sovereign territory—the likely view of the targeted country—nations will ultimately have natural incentives to "limit their searches to exigent circumstances, and to work out cooperative principles where possible" because of the extent to which aggressive searches could be reciprocated.[96]

Still, "there are strong arguments that the customary international law prohibit[s] . . . law enforcement functions in the territory of another sovereign . . . even when law enforcement officials do not enter the territory of another state,"[97] such as entering through remote Internet searches. According to this theory, such searches violate territorial integrity and, whatever the constitutional constraints that exist within the searching country, such searches are prohibited as violations of international law.[98]

Consequently, at the very outset, a foundational question surrounding unilateral cross border searches will be "whether remote cross-border searches conducted without the consent of the searched state violate the customary international law norm prohibiting law enforcement officials from performing their functions in the territory of another state without that state's consent."[99] This question cannot be answered by an individual country on a unilateral basis. Rather, it requires a cooperative, agreed-upon answer. To that end, several multilateral organizations have proposed an International Cybercrime Treaty that would address precisely this concern.[100]

---

transactions does not in fact lead to simultaneous universal regulation of the Internet . . . [and] the Internet is no more likely to undermine national sovereignty than did the telephone or satellite or television." *Id*. at 484, 491.

95. Goldsmith, *supra* note 92, at 114.

96. *Id*. at 117.

97. Bellia, *supra* note 4, at 100. Bellia also notes that "[t]his is not to say that *all* unilateral cross-border searches will violate international law; in some circumstances, it may not be possible for a state to know that the data it is searching is located beyond its borders." *Id*. (emphasis added).

98. *Id*. at 101 ("Customary international law and domestic law impose valid legal obstacles on foreign cross-border searches...").

99. *Id*. at 61–62. Bellia ultimately concludes that unilateral cross-border searches generally will violate customary international law. *Id.* at 100.

100. There are numerous articles and notes concerning the creation of an International Cybercrime Treaty, all discussing the Council of Europe's proposed Cybercrime Convention.

More to the point, for purposes of current judicial analysis, these competing views are largely irreconcilable and irresolvable. It is highly unlikely that a U.S. court would give an expansive reading to the Fourth Amendment or sharply limit the law enforcement—or foreign policy—powers of the Executive Branch on the basis of an ill-defined and still evolving standard of customary international law. Indeed, when commentators and nations themselves do not yet agree on this issue, it is clear that, by definition, *customary* international law does not exist. Accordingly, though the issue of sovereignty looms large over these searches, it is certain that U.S. courts will utilize *Verdugo*, and not customary international law, to resolve the issue. This Comment will do the same.

B. *Government Action Takes Place Outside the United States*

In our hypothetical, the defendant is a foreign national currently being held in custody by the U.S. government; this fact mirrors *Verdugo*. The defendant's status will not be analyzed as a U.S. citizen or a resident alien. Once these relevant factors are satisfied, one must then analyze the location of the search to decide whether *Verdugo* should apply.

The hypothetical created earlier imagines a scenario in which Russian nationals, located in Minsk, gain illegal access to company computer servers along the Dulles Technology Corridor in Northern Virginia. Through the Internet, these foreign nationals access a number of important documents and bank accounts within each company. The FBI is able to take custody of these alleged criminals when they come to visit their friend in Portland, Maine, and then while physically stationed at FBI computers in the United States, gain access to the Russians' own servers physically located within Russia. Through this remote cross-border search, the FBI locates numerous documents and programs used to break into the technology companies in the United States.

Much like the facts of *Verdugo*, one can plausibly argue that the search conducted by the U.S. government does not take place within U.S. territory. Searching a computer server located within Russia (whether or not a violation of the sovereignty of that country)[101] should

See, e.g., Albert I. Aldesco, *The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime*, 23 LOY. L.A. ENT. L. REV. 81 (2002); Ryan M. F. Baron, *A Critique of the International Cybercrime Treaty*, 10 COMMLAW CONSPECTUS 263 (2002); Jay Fischer, *The Draft Convention on Cybercrime: Potential Constitutional Conflicts*, 32 U. WEST. L.A. L. REV. 339 (2001); John T. Soma et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 HARV. J. LEGIS. 317 (1997); Shannon C. Sprinkel, *Global Internet Regulation: The Residual Effects of the "ILoveYou" Computer Virus and the Draft Convention on Cyber-crime*, 25 SUFFOLK TRANSNAT'L L. REV. 491 (2002).

101. *See* discussion *supra* Part III.A.

be considered an actual search outside the borders of the United States because the physical server location is in another sovereign territory. The physical act of gaining access to the computer server might take one through U.S. territory via the Internet, but the data that is retrieved and the information that is finally secured is actually searched and downloaded from a computer physically located in Russia. In *Verdugo*, "the place searched was located in Mexico."[102] In our instant hypothetical, the computer server actually searched was located in a foreign country. Thus, for purposes of *Verdugo* analysis, the place searched was in Russia.

Of course, one should recognize that the argument is not quite as simple as the preceding paragraph suggests. One might claim that the search is conducted in the United States because it is conducted through an Internet portal physically present in U.S. territory. FBI agents are sitting at a computer terminal in Kansas, not Minsk. They access the Russian defendant's computer files and download all his data without ever leaving the climes of Topeka. In *Verdugo*, DEA officials were actually physically present in Mexico to search through relevant documents and evidence. But, the FBI agents in our hypothetical are never physically present in Russia, searching the defendant's computer server.[103] Therefore, although the target computer server is located in Russia, one might argue that *Verdugo* should not apply because the search is taking place within the territory of the United States.

Resolution of this issue is difficult and likely the most uncertain part of the analysis. The development of the Internet is still relatively recent, and legal definitions often lag behind technological developments by a considerable distance.[104] One might even take these arguments to their ultimate conclusion, claiming that since the Internet is ultimately connected to numerous networks (and connected to networks within the jurisdiction of the United States) anything connected with that Internet is actually in the "territory" of the United States. This would be an argu-

102. United States v. Verdugo-Urquidez, 494 U.S. 259, 275 (1990).

103. One could also counter this argument by stating that the official is in fact "present" within the computer server when it is accessed. The metaphysics of these arguments would most likely become a difficult topic to contain, and these issues are not relevant to the overall topic I am currently discussing.

104. *See* Reetz, *supra* note 34, at 182–86 (examining the development of warrant requirements based on relevant technological advances); *see also* Henry H. Perritt, Jr., *The Internet as Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance*, 5 IND. J. GLOBAL LEG. STUD. 423, 426 (1998) ("Perhaps the most distinguishing feature of the Internet that makes it more threatening to sovereignty is that it is not susceptible to the same physical and regulatory controls as telegraph, telephone, radio, and television technologies.").

ment that the Internet is merely a "network of networks" and that those continuous networks are merely extensions of another network (and so on).[105] Because the Internet originated in the sovereign territory of the United States, then anything connected to the Internet would technically be within the confines of the United States.

One might take an even more extreme view and argue that because "[c]yberspace radically undermines the relationship between legally significant (online) phenomena and physical location,"[106] concepts of physicality and location are no longer even relevant to considerations of Fourth Amendment jurisprudence and all remote cross-border searches are actually not even remote, or are, at least, within U.S. jurisdiction.[107]

However, these arguments seem to prove too much. In the first place, this "network of networks" concept might actually cut against the claim that Internet cyberspace is within the jurisdiction of the United States. Each network, after all, is a separate entity and located within its own territorial confines. In fact, under this argument, only a very small part of the Internet might be deemed to be within the territorial jurisdiction of the United States.

At the other extreme, if the Internet has no location, then it is susceptible to regulation by anyone *and* everyone! Indeed, in October 2000, Minnesota announced that it would regulate all Internet transactions and uses within its jurisdiction, thereby attempting to protect Minnesota citizens that encounter activities, such as fraud and illegal gambling, on the Internet.[108] When physical location loses its relevance as a legal concept, then regulations are often justified under an effects-based test, premised on the notion that states have jurisdiction over all activities that create an effect on its citizens and territory.[109] Under this theory, not only can every U.S. state and nation-state regulate almost every computer based activity, but conversely, every citizen of every U.S. state and of any nation-state can claim the same protections that are afforded in every other state. In

105. Note, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75, 80 (1996) ("The crucial point is that the Internet, although globally accessible, is not a single network: it is a network of networks.").

106. Johnson & Post, *supra* note 91, at 1370.

107. *Id*.

108. Note, *A Proposal for Removing Road Blocks from the Information Superhighway By Using an Integrated International Approach to Internet Jurisdiction*, 10 MINN. J. GLOBAL TRADE 373, 383 n.80–81 (2001) (citing the Minnesota Attorney General website which stated, "Persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state and criminal laws").

109. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW 421(2)(i) (1987). Although the "effects-based" doctrine of jurisdiction is relatively limited, Minnesota applied it in order to claim the ability to regulate Internet fraud and other transactions.

short, all the reasoning of the Court in *Verdugo* goes out the window. No longer are we concerned about hampering the law enforcement or other foreign policy activities of the Executive Branch. No longer are we concerned about reasonable expectations of privacy. Every expectation, if reasonable anywhere in the world, is reasonable under this theory. And every restriction on the activities of an executive branch, any executive branch located anywhere in the world, is a valid restriction for courts to impose on the Executive Branch of the U.S. federal government.

In sum, in the absence of legislation or treaty, the better argument is that a remote cross-border search undertaken through the Internet is not within the territory of the United States because the end result of the search is to secure data and information located in Russia. This argument is not free from doubt, and certainly is not likely to be free from critics.[110] But, it seems reasonable to follow *Verdugo*'s lead and give weight to the physical location of the computer searched, which, in our case, would be in Russia.

C. *Foreign Government Involvement in the Search*

In a remote cross-border search, the federal government might or might not have the explicit or even tacit approval of the sovereign government of the territory where the target computer server is located. In the *Ivanov* case, the Department of Justice "sent a letter through diplomatic channels asking that Ivanov be detained and questioned" but there was no response to this formal request.[111] Additionally, no diplomatic request is mentioned in *Gorshkov*, as the entire search was conducted "by FBI fiat" without any approval or notification of the Russian government.[112] For remote cross-border searches, however, it appears that the *Verdugo* standard demands some approval from the foreign state.

As far as government approval is concerned, one might read the *Verdugo* case as requiring only that the government of the country in which the information is located be notified prior to the search, rather than requiring explicit or even tacit approval from the country prior to conducting the search. *Verdugo* expressly mentions the presence of Mexican government officials on the premises when the search was

110. A counterclaim would be that the search takes place in the location, such as a satellite or detectaphone, and that the end result location of the search should be the most important factor.

111. Cha, *supra* note 51 (noting that the United States does not have an extradition treaty with Russia (which is also the reason that FBI agents lured Zezev to the United Kingdom in order to arrest and extradite him to the United States)).

112. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 *1, *3 (W.D. Wash. May 23, 2001).

conducted.[113] This fact, however, is mentioned only in passing, making it unclear precisely what legal significance we should attach to the Court's mention of the presence of the Mexican legal authorities. Such presence might well have been required under the Court's reasoning, for example, because the DEA agents were physically present in Mexico. In order not to violate the territorial integrity of Mexico, a principal to which the Court pays ample deference, the presence—or at least the approval—of Mexican officials may well have been necessary. In a case where the U.S. government investigators are never actually physically present in the targeted country, then perhaps only notification, not approval, is necessary.

The holding in *Gorshkov* seems to support this interpretation. In that case, the Russian government was asked, but it never responded.[114] Notification was given, but approval never received.[115] Nevertheless, unilateral notification appeared sufficient to the court and the evidence was admitted.

Finally, it is worth noting that while even the presence of Russian officials might not have been enough in and of itself to immunize the action of the U.S. Government from subsequent charges of constitutional violations,[116] the U.S. Government can apparently try a suspect even if he is brought to the United States in violation of his constitutional rights, whatever they may be.[117] Thus, we can plausibly conclude that an appeal or notice to the foreign government is required, but the approval of that government is not essential.

Put slightly differently, the relevance of the presence or approval of Mexican officials really relates to the question of territorial integrity. If a remote cross-border search violates the sovereignty of the target country under international law, then perhaps approval is necessary.[118] If no U.S. officials actually enter the foreign country or otherwise intrude into its space, then it is not a violation of customary international law and

113. United States v. Verdugo-Urquidez, 494 U.S. 259, 262 (1990).

114. *Gorshkov*, 2001 WL 1024026, at *4 n.2.

115. *Id*. In fact, the Russian government subsequently opened a criminal investigation into the conduct of the FBI agent who gained access into the Russian servers. *See* Ariana Eunjung Cha, *Timeline: The FBI Sets a Trap*, NEWSBYTES, May 19, 2003.

116. *See* United States v. Alvarez-Machain, 504 U.S. 655 (1992) (holding that U.S. agents could not enter Mexico to physically remove a person from another sovereign territory and bring him back to the United States, especially without cooperation from the sovereign government). Indeed, if U.S. law enforcement agents conduct a forcible removal of a foreign national without the consent of that foreign government, the holding of *Alvarez-Machain* would apply. In such a case the U.S. government must release that foreign national because there was no cooperation with the foreign government in which the target resided.

117. *Id*.

118. *See supra* Part III.A.

approval of the foreign government is not necessary. Looking at our hypothetical, applying the *Verdugo* standard to remote cross-border searches requires at least notification of the foreign government through which the remote cross-border search is being conducted. In our hypothetical, notification will suffice.

D. *Substantial and Voluntary Connections with the United States*

The Court in *Verdugo* considers substantial voluntary connections with the United States to be an extremely important part of its analysis regarding Fourth Amendment protections of foreign nationals.[119] In our hypothetical, it is hard to argue that the defendant possesses the requisite substantial voluntary connections with the United States. Because the Court does not state the exact requirements needed for a "substantial voluntary connection" to be established, perhaps further analysis is necessary. Moreover, we need to consider the notion of "substantial voluntary connections" in light of the emerging technology that makes both the crime and the search possible in the first place.

In that regard, one might posit a number of different kinds of possible voluntary connections. For instance, if the foreign national maintained a website that recorded the number of hits from computers in the United States, one might argue that this constitutes a substantial voluntary connection. Since there are a number of countries that regulate the Internet, one might also argue that such regulation by the United States, if it actually extends to the defendant in question, gives that foreign national defendant a connection to U.S. territory, though perhaps not an entirely voluntary one.[120]

Conversely, the U.S. government would certainly argue that website contacts, especially mere measurement of website contacts, do not create a substantial connection with the United States. If this were the case, then anyone could establish a connection to the United States merely by creating an English language website. Even the most superficial action would be deemed to create a substantial connection to the United States and everyone would be entitled to the protections of the U.S. Constitution.

---

119. *See supra* Part II.B.3.

120. *See* John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207 (1997) (comparing the Internet regulation regimes of three different countries—the United States, Germany and China—and arguing for non-regulation of the Internet). *See supra* notes 104–107 and accompanying text.

To unravel these arguments it is important to understand why the connection is actually required in the first place. The substantial connection doctrine arises out of the reasonable expectations justification for Fourth Amendment protections. If the foreign national does have substantial connections with the United States, his expectations are more likely to be deemed reasonable. A substantial and voluntary connection with the United States entitles one to believe that one is protected by U.S. law when undertaking dealings within the United States. Viewed against this backdrop, it is hard to argue that the mere establishment of a website in English, even a website that U.S. citizens and resident aliens might visit, creates a genuine, substantial connection with the United States such that the creator should have the full panoply of Fourth Amendment protections attach to his activities.

A defendant might also claim that his Internet connections with U.S. servers or his connections that necessarily travel through servers located in the United States meets the *Verdugo* substantial connection standard. The *Verdugo* case was, of course, much easier to analyze in this regard because the defendant did not possess any actual connections, physical or electrical, with the United States. He did not even have any "societal obligations" or any other connections with the United States.[121]

But, under the Court's reasoning, one could argue that owning a company that does business within the United States, or actually offering services or items to U.S. citizens (such as a Internet security consulting service or software sales company) would be enough to constitute "substantial voluntary connections" under the *Verdugo* standard. One might even argue that living for a short time in the United States would create a substantial connection to the United States.[122] We know that absolutely no connection with the United States is not substantial voluntary connections. We know that residency within the United States does create such connections. Moreover, we strongly suspect that significant business activity in the United States will create the requisite connections. But the gradations in between these extremes are infinite; precisely where to draw the line is still undetermined.

Nevertheless, we can speculate a bit about where the line might be drawn when courts finally decide to draw such a line. Whether *Verdugo*-required connections can be established through travel in the United States, possessing gainful employment in the country, or even by taking

121. United States v. Verdugo-Urquidez, 494 U.S. 259, 273 (1990).

122. The court does not hold on this question. "The extent to which respondent might claim the protection of the Fourth Amendment if the duration of his stay in the United States were to be prolonged . . . we need not decide." *Id*. at 271–72.

on certain societal obligations in the United States (such as custody of a child living in the United States), is not established by the Court. But, in light of the events of September 11th and the passage of tighter controls on immigration, visa entitlements and alien status, it is unlikely that the Court would broaden the methods of establishing "voluntary substantial connections" as a *Verdugo* factor.[123]

Conversely, Ivanov and Gorshkov traveled to the United States for (what they thought was) a business deal and were trying to get jobs from a U.S. company (albeit an FBI-created front).[124] One could argue that Zezev was trying to establish a business relationship with Michael Bloomberg (and possibly an employment relationship with the Bloomberg Company).[125] Both of these defendants (and the ones in our hypothetical case) would argue that they established the required connections. These arguments seem tenuous at best, because a mere business relationship is not addressed by the Court in *Verdugo* and can be argued to be a weak link to the United States that does not exhibit a substantial voluntary connection. Concurrently, however, such arguments show that this *Verdugo* standard requires clarification.

It is likely that the *Verdugo* court did not create factors to govern how one establishes these connections because foreign nationals would always go through the motions to establish such connections before committing cybercrimes in the United States.[126] It remains clear that further elaboration of this important *Verdugo* factor is necessary for it to function as the standard that governs the rights of foreign nationals during remote cross-border searches of the Internet.

E. *Concerns About the Court Hindering the Activities of the Executive Branch*

An integral part of the *Verdugo* standard is the focus on how an adverse holding would affect the ability of the Executive Branch to conduct important activities protecting the national interest.[127] These same concerns arise when one discusses the ability of the Executive Branch and armed forces to retaliate for attacks on our national computer infrastruc-

123. *See* USA Patriot Act of 2001, 8 U.S.C. § 1182 (act enhancing domestic security against terrorism, including provisions on surveillance of terrorist, money laundering, and investigation of terrorism).

124. *Russian National Indicted*, *supra* note 49.

125. *See U.S. Convicts Kazakhstan Hacker*, *supra* note 7.

126. If the Court had determined the exact factors for establishing substantial voluntary connections to the United States, then many future criminals would create those connections so that *Verdugo* did not apply to their case. Such avoidance would significantly impair the prosecution of international cybercrime in the United States.

127. United States v. Verdugo-Urquidez, 494 U.S. 259, 273–74 (1990).

ture.[128] The *Verdugo* Court worried that a Fourth Amendment requirement would hinder the "ability of the political branches of the United States to respond to foreign situations involving our national interests."[129] The existence of coordinated attacks on U.S. computer networks by foreign entities would be extraordinarily serious and one would certainly want the political branches to be able to respond adequately and effectively to such an attack. Such a concern should be pertinent to the application of the *Verdugo* standard.[130]

The Executive Branch is charged with protecting the territorial sovereignty (as the Commander-in-Chief of the Armed Forces) and therefore also charged with ensuring the well-being of the United States and its citizens.[131] Computer attacks on government and private infrastructure would certainly constitute attacks on U.S. territory.[132] If the Court were to decide that all remote cross-border searches by the federal government are limited by the *Verdugo* standard, then the Executive Branch could less easily perform its duties with respect to these kinds of foreign activities.

One can argue that the underpinnings of these political outcomes are justified on three separate grounds. First, the Supreme Court articulated a general reluctance to impose conditions on law enforcement officials when it is not clear that constitutional rights are being violated.[133]

---

128. *See, e.g.*, Richard W. Aldrich, *How Do You Know You Are at War in the Information Age*, 22 HOUS. J. INT'L L. 223 (2000); Richard Clarke, *Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks*, 12 DEPAUL BUS. L.J. 33 (1999/2000); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207 (2002); Schmitt, *supra* note 19; James P. Terry, *Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?*, 46 NAVAL L. REV. 170 (1999) (all discussing whether Article 51 of the United Nations Charter permits self-defense through computer networks once a sovereign country has conducted an attack through that computer network).

129. 494 U.S. at 273–74.

130. Schmitt, *supra* note 19, at 888 ("[T]he extraordinary advances made possible by breakthroughs in computer technology represent dangerous vulnerabilities exploitable by opponents ranging from economic, *political, and military competitors, to terrorists* and criminals.") (emphasis added). *See also* THE WHITE HOUSE, CYBERSPACE THREATS AND VULNERABILITIES 5–12 (2002), *available at* http://www.whitehouse.gov/pcipo/case_for_action.pdf (describing the dependency of U.S. computer networks and the potential threats and vulnerabilities) (last visited Nov. 13, 2003).

131. U.S. CONST. art. II, § 2.

132. Eric Jensen recognizes the right of self-defense against computer network attacks, which is a partial step towards recognition of that right under customary international law. Jensen, *supra* note 128, at 239 ("The United States and other nations should develop robust passive and active CND [Computer Network Defense] programs and use them in response to any CNA [Computer Network Attacks] against critical national infrastructure.").

133. United States v. Verdugo-Urquidez, 494 U.S. 259, 267–68 (1990).

Second, law enforcement (and other Executive Branch) officials need some flexibility in their activities as technology continues to change and advance. Without such flexibility, courts might unduly hamper the ability of law enforcement officials to carry out legal searches using new technology. Third, as technology advances and borders become both more porous and less relevant as protective barriers, there is a heightened concern regarding crime committed by foreign nationals.[134] Accordingly, courts are generally unwilling to unduly hamper law enforcement activities targeted against technologically advanced crimes originating from foreign countries against the United States.

The criminal activity in this Comment's hypothetical undoubtedly raises all three of these concerns. The Internet is still a relatively new medium with great potential for criminal activity. Government officials are also rightly concerned about the vulnerability of U.S. computer networks to outside attacks.[135] In our hypothetical, a court would almost certainly be wary of unduly hampering law enforcement activities that are targeted against Internet crime, even if—indeed, especially if—the Internet itself is the tool the law enforcement officials use to ferret out that crime.

IV. TOWARDS A CLEAR *VERDUGO* STANDARD FOR REMOTE CROSS-BORDER SEARCHES

Since *Verdugo* still stands as good law on the question of how to analyze the protections of the Fourth Amendment for foreign nationals, it should also apply to remote cross-border Internet searches of foreign nationals. As this Comment has demonstrated, moreover, the holding and reasoning of *Verdugo* should be applied to each remote cross-border search that is conducted by the U.S. government and law enforcement entities on a case-by-case basis. It is clear, however, that simply applying *Verdugo* to remote cross-border searches may not answer all the relevant questions adequately. We must look to the courts for elaboration before law enforcement officials can be assured in the legality of their activities. This Part of the Comment discusses what additional elaboration is needed and what an appropriate standard for remote cross-border searches might look like.

134. This is evidenced by the fact that the U.S. government is establishing a new cyber-security center. Dennis Fisher & Caron Carlson, *Feds to Open Cyber-Security Ops Center*, EWEEK, May 26, 2003, *at* http://www.eweek.com/article2/0,3959,1109041,00.asp (last visited Nov. 13, 2003).

135. *Id*.

A. *Should There Be a Clear* Verdugo *Standard?*

If the threshold question of *Verdugo* depends solely on the nationality of the defendant and the fact that a search occurs outside the physical jurisdiction of the United States, then there would be no need for clarification of the *Verdugo* standard. This standard would act like a strict liability standard in torts, making it easy for law enforcement officials and the courts to determine whether a particular defendant was entitled to the full protection of the Fourth Amendment.

As this Comment demonstrates, matters are not that simple. The Court rightly identified a number of factors essential to the determination of the legality of a remote cross-border search. The application of these factors is greatly complicated, however, by the kind of technology now available to law enforcement officials to conduct such searches. The tremendously varied circumstances of potential defendants also make rigid application of bright line tests both difficult and ill-advised.

For instance, a search might be routed through servers in a number of different countries, ultimately ending up with the target server actually housed somewhere in the United States. The foreign cybercriminal might have substantial ties to the United States, either through business connections, family connections, or numerous years spent in the United States under some sort of legal capacity. Certain substantial voluntary connections might be established if the defendant had previously paid taxes or incurred some "societal obligation," as the *Verdugo* Court held.[136]

Each of these variables relates to the factors articulated by the *Verdugo* Court, and application of some or all of these variables against the *Verdugo* standard would be ill-advised or impossible.

B. *Clarifying and Constructing the* Verdugo *Standard*

We find a good beginning to the creation of appropriate standards in the very facts surrounding the cybercrime itself. First, the defendant's factual circumstances should be examined and understood, including the nationality of the defendant. This also encompasses such determinations as whether the defendant is a foreign national or resident alien, what type of connections the defendant possesses with the United States (including both the nature and extent of such connections), and, finally, the type of criminal activity of which the defendant has been accused.

These factual variables not only inform the reasonableness of the defendant's expectations of privacy, but they also help determine where the

136. *Verdugo*, 494 U.S. at 273.

presumptions lie. For example, the *Verdugo* holding states that, generally speaking, foreign nationals do not possess Fourth Amendment rights and expectations similar to U.S. citizens and resident aliens.[137] From this, one might well conclude that foreign nationals generally should not receive Fourth Amendment protections unless they can demonstrate some special reason for why they should receive them. The standard could be that once the government proves that a defendant is a foreign national, then the Fourth Amendment would not apply to government searches of that defendant's property conducted abroad unless the defendant can show reasons why he or she should receive Fourth Amendment protections.[138] Defendants could then, in turn, show that they possess substantial voluntary connections with the United States or that the U.S. officials actually intruded physically upon the soil of the foreign country when they conducted the search.

A second set of variables must revolve around the search itself. One question to ask, for example, is whether or not the search was truly conducted outside the territory of the United States. The Court would investigate the location of the target data, the methods that the government used to intercept or download that data, and the availability of that data within computers located in the physical confines of the United States. If the data is physically located on a computer server outside of the United States, such a factor counsels toward applying the *Verdugo* standard and denying Fourth Amendment protection to the defendant. If, on the other hand, the data crossed through servers located in a number of different territories, but ultimately ended up back in a computer server housed within the territory of the United States, then the search might appropriately be viewed as a search within the territory of the United States.

In addition, the Court would have to look at the accessibility factors of the target server. Easy accessibility of the computer server within the United States, such as an offshore storage web server designed to service only U.S. customers, would be a factor that cuts against the search being treated as a cross-border search under the *Verdugo* standard.[139]

---

137. *Id*. at 261.

138. Of course, Justice Brennan disagrees with this analysis, stating that "[w]hen our Government conducts a law enforcement search against a foreign national outside of the United States and its territories, it must comply with the Fourth Amendment. . . . When we tell the world that we expect all people, wherever they may be, to abide by our laws, we cannot in the same breath tell the world that our law enforcement officers need not do the same." 494 U.S. at 296–97 (Brennan, J., dissenting).

139. Factors that might cut in favor of this argument would be that the web-based storage facility is marketed to U.S. customers, built for U.S. customers, and that U.S. customers believe the server is actually within U.S. territory, even though it is not. In such a case, there

The overall presumption should be that the *Verdugo* standard applies to remote cross-border searches of foreign nationals unless the presumption could be rebutted. The defendant could rebut such a presumption through proof of his or her special circumstances or through evidence that the search actually culminated in securing data that was physically (and perhaps exclusively) present in, and only in, a server located within the United States. Each one of the *Verdugo* factors would be used to analyze a remote cross-border search, and each factor would carry equal weight in the summation of whether the Fourth Amendment would apply in such a circumstance. As long as the majority of these factors of the *Verdugo* standard weighed towards not requiring Fourth Amendment protections, then the case would be analyzed under this standard and no warrant would be required. However, if the majority of the factors were dissimilar from *Verdugo*, then the standard would not be applied, and a warrant would be required for the remote cross-border search conducted by law enforcement entities or the U.S. government.

C. *Interpreting the Clarified* Verdugo *Standard*

So, what precisely needs to be clarified for *Verdugo* to apply to remote cross-border searches? To date, the Court has placed the most emphasis on the fact that the search occurred outside U.S. territory. Accordingly, the area ripest for exposition relates to the definition of the location of a search in light of computer technology and the Internet. Second, in terms of connections to the United States, the Court ultimately needs to give content to both the ideas of "substantial" and "voluntary." All of these concepts need to be clarified, moreover, against the backdrop of the important foreign policy concerns that underlie the doctrine in the first place. Finally, even as it clarifies the *Verdugo* standard, the Court must be attentive to the need for flexibility in its application and its subsequent doctrinal development.

Indeed, as computers and technology continue to become more advanced and the territorial boundaries through the Internet continue to diminish, it becomes especially important for the Court to create a more explanatory standard of how *Verdugo* should apply to cybercrime. Without a clear standard or guidance from the courts, federal prosecutors will find it more difficult to conduct remote cross-border searches in the instances they are needed. This is especially important for computer crimes and Internet-based searches, because evidence can be destroyed, transferred or removed almost instantaneously in some cases. Thus, in

might be arguments that searches conducted into such servers are searches within U.S. territory because citizens and aliens alike have a reasonable belief that the server space is located within U.S. territory.

order not to hinder the federal government as it combats cybercrime and protects U.S. territory and U.S. citizens and residents, the Court should clarify the existing *Verdugo* standard so that prosecutors and law enforcement officials can understand precisely when a remote cross-border search must comply with the Fourth Amendment and when it need not.

CONCLUSION

Cybercrime and cyberterrorism are topics increasingly in the forefront of international criminal law and political regulatory discussions. As technology continues to advance and the numbers of Internet users continues to increase, the commission of crimes affecting the U.S. government, U.S. companies and U.S. residents undoubtedly will grow. Whether the federal government will be required to extend Fourth Amendment protections to foreign nationals engaged in cybercrimes is an issue potentially solved by the application of a clear *Verdugo* standard and through using this standard to analyze each remote cross-border search under the four factors stated in the *Verdugo* decision. Since no court has yet to completely analyze such a search under the factors stated in *Verdugo*, it is important to develop the doctrine of Fourth Amendment rights that apply against foreign nationals accused of committing crimes over the Internet, especially as the methods and techniques of crimes and searches become more technologically advanced and intricate.

Applying the current *Verdugo*-style reasoning to remote cross-border searches will not necessarily result in a clear standard, however, and more clarity is needed. Such clarity must be achieved without sacrificing the capacity of the law to change with changing technology. Technological advances must be met with responsive legal advances. The application of such a clear standard is essential to U.S. law enforcement personnel in their efforts to protect citizens and residents of the United States from criminals who can now strike from literally anywhere in the world.