2001

Chasing Bits Across Borders

Patricia L. Bellia
Notre Dame Law School, patricia.l.bellia.2@nd.edu

Chasing Bits across Borders

Patricia L. Bellia[†]

In February of 2000, the websites of at least eight major U.S.-based internet companies were crippled after a hacker programmed dozens of computers to make thousands of simultaneous requests to connect to the target systems each minute.[1] One market research firm estimated that these distributed "denial of service" attacks—so named because the crippled system is unable to serve its legitimate users[2]—could cause $1.2 billion in dam-

---

† Assistant Professor of Law, Notre Dame Law School. A.J. Bellia, Paul Berman, Bob Blakey, Paolo Carozza, Erika Dreifus, Jimmy Gurulé, Orin Kerr, John F. Murphy, John Nagle, Todd Peterson, Betty-Ellen Shave, Dinah Shelton, Jeff Singdahlsen, Kevin Smith, Allan Stein, Bill Treanor, and Jay Wexler provided helpful comments on an earlier draft of this Article. I am grateful for the assistance of research librarians Dwight King, Hector Escobar, Patti Ogden, and Warren Rees. Jennifer Camden and Jason Flaherty provided excellent research assistance.

[1] See Charles Cooper, *New Cybersport: Taking out Web Sites?*, ZDNet News (Feb 10, 2000), available online at <http://www.zdnet.com/zdnn/stories/news/0,4586,2435899,00.html> (visited Aug 12, 2000) [on file with U Chi Legal F] (listing the targeted sites). For a description of the incidents, see Internet Denial of Service Attacks and the Federal Response, Hearing before the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Justice Oversight of the Senate Committee on the Judiciary, 106th Cong, 2d Sess 35–37 (2000) (statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation) (detailing how the hacker's cyber attack functioned, listing how the FBI and security firms warned the public, and describing the series of attacks); Cybercrime, Hearing before the Subcommittee on Commerce, Justice, State, the Judiciary, and Related Agencies of the Senate Committee on Appropriations, 106th Cong, 2d Sess 25–26 (2000) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (detailing how the hacker's cyber attack functioned, listing how the FBI and security firms warned the public, and describing the series of attacks). The target systems included Yahoo!, eBay, Buy.com, Amazon.com, E*Trade, MSN.com, CNN.com, and ZDNet.

[2] A simple denial of service ("DoS") attack typically involves a single computer making repeated connection requests in an attempt to overpower the target system. In a "distributed" denial of service ("DDoS") attack, the connection requests originate from a large number of computers, making it difficult to distinguish attacking traffic from legitimate traffic. See Eric J. Bowden, *Of Zombies and Script Kiddies: Distributed Denial of Service Attacks—DoS v. DDoS Attacks*, ZDNet Help & How-To (Oct 26, 2000), available online at <http://www.zdnet.com/zdhelp/stories/main/0,5594,2645417-2,00.html> (visited Oct 27, 2000) [on file with U Chi Legal F] (explaining the different tactics used in DoS and DDoS attacks). To launch a DDoS attack, a hacker accesses a computer system without authorization and places on the system a program that renders the system a "master," capable of controlling other computer systems. The hacker also places code on the other computer systems, causing them to operate as "agents" of the master system. The master system

ages.[3] A few months later, the "I Love You" virus infected forty-five million computers around the world.[4] The virus spread rapidly by installing itself in a computer's system files and causing the computer to forward an infected electronic mail attachment to all addressees in the user's e-mail address book.[5] Along with some thirty copycat variants that surfaced in the succeeding weeks, the "I Love You" virus cost between $6.7 billion and $10 billion in lost productivity.[6]

These two widely publicized incidents brought greater public attention to the problem of computer crime. The FBI, computer security sites, and technology sites offered tools and technical advice to help prevent denial of service attacks and ward off viruses.[7] Congress promptly held hearings to consider whether fed-

---

instructs the agents to produce a flood of simultaneous requests to connect to the target system. See Internet Denial of Service Attacks Subcommittee Hearing at 36 (cited in note 1) (statement of Michael A. Vatis) (listing the tools hackers use to turn systems into "masters" and "agents" and explaining how they work); Cybercrime Subcommittee Hearing at 25 (cited in note 1) (statement of Louis J. Freeh) (listing the tools hackers use in DoS and DDoS attacks).

[3] See David Akin, *Officials Concede Arrest in Hacker Case Could be Weeks Away*, Natl Post C6 (Feb 24, 2000); Russ Banham, *Hacking It*, CFO Magazine 115 (Aug 1, 2000).

[4] See Paul Festa and Joe Wilcox, *Experts Estimate Damages in the Billions for Bug*, CNET News.com (May 5, 2000), available online at <http://news.cnet.com/news/0-1003-200-1814907.html> (visited Sept 14, 2000) [on file with U Chi Legal F]; Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act, Hearings on HR 5018, HR 4987, and HR 4908 before the Subcommittee on the Constitution of the House Committee on the Judiciary, 106th Cong, 2d Sess (2000) (statement of Kevin DiGregory, Deputy Assistant Attorney General, Criminal Division, Department of Justice).

[5] See Festa and Wilcox, *Experts Estimate Damages in the Billions for Bug*, CNET News.com (cited in note 4) (explaining how the "I Love You" virus installs and forwards itself).

[6] *Love Bug Damage Costs Rise to $6.7 Billion*, Computer Economics eFlash (May 9, 2000), available online at <http://www.computereconomics.com/cei/press/2000/pr000509.html> (visited Sept 12, 2000) [on file with U Chi Legal F] (noting damages of $6.7 billion five days after virus released); Rob Kaiser, *'Love Bug' Has Cousins; They Bite Too: Cyberattack Considered Most Disruptive Ever*, Chi Trib 1 (May 6, 2000) (projecting costs of $10 billion).

[7] See, for example, Cybercrime Subcommittee Hearing at 26 (cited in note 1) (statement of Louis J. Freeh) (FBI released to the public a software tool for detecting installed DDoS software); *CERT® Advisory CA-1999-17: Denial-of-Service Tools*, CERT Coordination Center Alerts (updated Mar 3, 2000), available online at <http://www.cert.org/advisories/CA-1999-17.html> (visited Oct 27, 2000) (suggesting that sites implement ingress filtering); Bradley F. Shimmin, *Deconstructing Denial of Service Attacks—What Can Be Done*, ZDNet Help & How-To (Feb 8, 2000), available online at <http://www.zdnet.com/zdhelp/stories/main/0,5594,2434548-3,00.html> (visited Oct 27, 2000) (noting the existence of tools to help internet service providers detect attacks and software used in such attacks); *Results of the Distributed-Systems Intruder Tools Workshop*, CERT Coordination Center Reports (Dec 7, 1999), available online at <http://www.cert.org/reports/dsit_workshop-final.html> (visited Oct 27, 2000) (providing suggestions for immediate

eral laws and resources designed to combat attacks on computer systems were adequate to the task.[8]

Despite this focus on the adequacy of American laws and American enforcement efforts, the denial of service attacks and the "I Love You" virus each provide a dramatic illustration of the fact that national borders are largely irrelevant when it comes to committing computer crime. The denial of service attacks targeted servers physically located in the United States, but a teenager in Canada staged the attacks.[9] The "I Love You" virus originated in the Philippines and spread rapidly through government and corporate systems in more than 20 countries.[10] An international element is often present, not only when a computer system is the target of a crime, but also when a system merely facilitates online forms of traditional crimes or serves as a repository for evidence of a crime.[11] Computer networks are used to offer online

---

short-term and long-term protection of internet service providers); [all internet materials cited in this note on file with U Chi Legal F].

[8] See Internet Denial of Service Attacks Subcommittee Hearing (cited in note 1) (discussing DDoS attacks and federal efforts to prevent and prosecute such crimes); Cybercrime Subcommittee Hearing (cited in note 1) (discussing the nature of cybercrime and the role of the government in promoting security on the internet); Internet Security and Privacy, Hearing before the Senate Committee on the Judiciary, 106th Cong, 2d Sess (May 25, 2000), available online at <http://www.senate.gov/~judiciary/wl525200.htm> (visited Apr 5, 2001) [on file with U Chi Legal F] (the transcript of this hearing has not yet been published; a list of witnesses and their respective submitted testimony is available at this web site); The Love Bug Computer Virus: Protecting Love Sick Computers from Malicious Attacks, Hearing before the Subcommittee on Technology of the House Committee on Science, 106th Cong, 2d Sess (May 10, 2000), available online at <http://www.house.gov/science/hearing_106.htm> (visited Apr 16, 2001) [on file with U Chi Legal F] (the transcript of this hearing has not yet been published; a list of witnesses and their respective submitted testimony is available at this web site).

[9] See *Canada Broadens Its Case Against Suspected Hacker*, NY Times C5 (Aug 4, 2000). The Canadian youth allegedly manipulated at least 54 computer systems to stage the February 2000 attacks, including systems at the University of California at Santa Barbara, Harvard, and Duke. Id; Lenny Savino, *MafiaBoy May Face Harsher U.S. Justice*, Natl Post A6 (Aug 5, 2000) (noting use of Harvard and Duke computers). The youth pleaded guilty to Canadian charges in January 2001. Graeme Hamilton, *Mafiaboy Pleads Guilty to Online Attacks*, Natl Post A6 (Jan 19, 2001).

[10] See *ISP Tracks "Love" Bug Through Caller ID*, CNET News.com (May 15, 2000), available online at <http://news.cnet.com/news/0-1003-200-1877238.html> (visited Sept 14, 2000) [on file with U Chi Legal F] (stating that the virus apparently originated in Manila); *"Love" Bug Release May Have Been Accidental*, CNET News.com (May 11, 2000), available online at <http://news.cnet.com/news/0-1003-200-1855997.html> (visited Sept 14, 2000) [on file with U Chi Legal F] (noting the virus' effect on government and corporate systems in more than twenty countries). Because the Philippines lacked any computer crime statute at the time of the attack, the main suspect was never prosecuted. See William Glanz, *"Love Bug" Creator Could Go Scot-Free*, Wash Times B10 (May 18, 2000).

[11] Commentators often distinguish between three different types of criminal conduct involving computers. First, the computer may be the target of the crime, as in the case of the denial of service attacks or the "I Love You" virus. Second, the computer may serve as

gambling,[12] convey threats,[13] transmit child pornography and lure children into sexual conduct,[14] commit fraud,[15] and evade protections on intellectual property.[16] Recent enforcement efforts illustrate that these offenses are often international in scope. New York and federal officials successfully targeted gaming operations based in Antigua that offered online gambling services to New York citizens.[17] In September of 1998, officials in twelve countries

---

a tool for communication, facilitating crimes that take place in the brick-and-mortar world. Third, the computer may be incidental to the crime; for example, it may hold evidence of the crime. See generally Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium*, 9 Duke J Comp & Intl L 451, 455 (1999) (distinguishing the three ways criminals use computers); Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 Harv J L & Tech 465, 468–69 (1997) (same); Scott Charney and Kent Alexander, *Computer Crime*, 45 Emory L J 931, 934 (1996) (same); Report of the President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet* 7–11 (Mar 2000), available online at <http://www.cybercrime.gov/unlawful.pdf> (visited Sept 14, 2000) [on file with U Chi Legal F] (same).

[12] See generally National Gambling Impact Study Commission, Final Report, ch 5 (June 1999), available online at <http://www.ngisc.gov/reports/fullrpt.html> (visited Jan 29, 2001) [on file with U Chi Legal F] (describing the emergence, rapid growth, and various forms of internet gambling and recommending methods of federal regulation).

[13] See generally Report from the Attorney General to the Vice President, *Cyberstalking: A New Challenge for Law Enforcement and Industry* (Aug 1999), available online at <http://www.cybercrime.gov/cyberstalking.htm> (visited Sept 14, 2000) [on file with U Chi Legal F] (discussing the growth of cyberstalking and the use of the internet to harass and threaten others).

[14] See Report of the President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, appendix C (Mar 2000), available online at <http://www.cybercrime.gov/unlawful.pdf> (visited Sept 14, 2000) [on file with U Chi Legal F] (cited in note 11) (addressing online child pornography, child luring, and related offenses and discussing federal laws and initiatives to protect children).

[15] In two widely reported stock manipulation cases, for example, individuals distributed false reports relating to the companies PairGain Technologies and Emulex. The releases were accessed widely on the internet and dramatically affected stock prices, allowing each individual to conduct trades at a significant profit. See Robin Fields, *Emulex Stock Hoax Was Triggered by E-Mail Release*, LA Times C1 (Aug 31, 2000) (describing how e-mail and the internet were used to distribute a false press release); John F.X. Peloso and Ben A. Indek, *Overview of SEC's Response to the Internet in Securities Markets*, NY L J 3 (Oct 19, 2000) (explaining various SEC actions taken in response to the rise in cases of internet securities fraud).

[16] Report of the President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet* appendix I (Mar 2000), available online at <www.cybercrime.gov/unlawful.pdf> (visited Sept 14, 2000) [on file with U Chi Legal F] (cited in note 11) (discussing software piracy and intellectual property theft and describing federal laws and initiatives to prevent such crimes).

[17] See *People v World Interactive Gaming Corp*, 714 NYS2d 844, 851–53 (NY Sup Ct 1999) (holding that Antigua-based corporation violated New York and federal gambling laws by offering gambling to internet users in the United States); *World Sports Official Is Found Guilty in Case of Internet Wagering*, Wall St J 20XX WL-WSJ 2004876 (Feb 29,

cracked down on an internet-based child pornography ring, seizing some one hundred thousand images.[18]

This Article examines the challenges that computer crimes cutting across international borders present for law enforcement officials. As unlawful conduct involving computer systems becomes more widespread, evidence of that conduct will increasingly take an electronic form and be stored beyond the reach of the investigating jurisdiction.[19] And traditional mechanisms through which countries ordinarily obtain evidence abroad are unlikely to prove satisfactory in such investigations.[20] The investigative difficulties computer crimes pose have prompted two related state responses. Some states have asserted that they possess a broad power to conduct "remote cross-border searches"[21]—that is, to use computers within their territory to access and examine data physically stored outside of their territory—so long as the data is relevant to an investigation of conduct over which they have jurisdiction and their own law authorizes the search.[22] In November 2000, for example, during an investigation of a Russian hacking ring that had targeted several U.S. companies, FBI agents downloaded extensive data from Russian computers.[23]

2000) (reporting the successful prosecution of the president of Antigua-based World Sports Exchange Ltd for accepting bets from Americans over the internet).

[18] See *Crackdown on Net Child Porn*, CNET News.com (Sept 2, 1998), available online at <http://news.cnet.com/news/0-1005-200-332841.html> (visited Sept 14, 2000) [on file with U Chi Legal F].

[19] See text accompanying notes 68–72.

[20] See id.

[21] I use the term "remote cross-border searches" to encompass not only circumstances in which officials examine data residing on a foreign computer, but also circumstances in which officials download the data to local computers for later viewing.

[22] For example, some states claim a power to conduct remote cross-border searches of data lawfully accessible to persons within their borders, on the theory that such data is "virtually present" there for law enforcement purposes. The simplest case is that of a corporation that structures its network so that subsidiaries in other countries can access centrally stored data. An early statement of a British official reflects this view. See Sussmann, 9 Duke J Comp & Intl L at 472 (cited in note 11), quoting Paul Boateng, Minister of State for the Home Office (UK), *Tomorrow's Challenges for Law Enforcement*, Keynote Address to the Second International Conference for Criminal Intelligence Analysts (Mar 1, 1999), ("Jurisdiction over a database should not now depend only on where it happens to be physically stored. Where the owners of the system have set it up to be accessible from another jurisdiction, it should be regarded as present in that jurisdiction for law enforcement purposes."). As the Russian case described in the text illustrates, however, states may claim a cross-border search power even when a network is simply connected to the internet, without the intention of providing access to specific persons in specific countries.

[23] See Application and Affidavit for Search Warrant at ¶¶ 11–15, 19–20, 22–29 (W D Wash filed Dec 1, 2000) (No 00-587M) [on file with U Chi Legal F]. Public accounts of the case suggest that the FBI lured two Russian suspects to the United States by inviting them to apply for positions with a bogus internet security firm. Once the suspects were in the United States, agents captured the passwords they used to connect to a Russian net-

Other states have merely pressed for recognition of a remote cross-border search power in international fora, arguing that such a power is an essential weapon in efforts to combat computer crime.[24]

This Article explores these state responses with two objectives in mind. The first is to develop an appropriate framework for evaluating the legality of cross-border searches, both as a matter of international law and as a matter of U.S. law. This task is growing increasingly pressing. The Russian hacking investigation represents the first case in which a government has publicly acknowledged engaging in a remote cross-border search without the target state's permission, but other states may quickly follow suit. In addition, one multilateral organization recently finalized a treaty on cybercrime containing extensive procedural provisions concerning states' cooperation in exchanging data physically located within their respective borders.[25] Although the treaty primarily envisions that a state will gather evidence from within its borders and will then pass the evidence on to the requesting state, it nevertheless recognizes limited but important powers to conduct remote cross-border searches.[26] Issues relating to cross-border searches are likely to take on increasing importance in the immediate future.

My second objective is to tie this analysis of the legality of cross-border searches to an important scholarly debate about how the law should adapt to the increasingly widespread use of com-

---

work. The agents then used the passwords to access and download data from the Russian servers. Once the agents seized the data, they sought a search warrant to view it. See Mike Carter, *E-sting Nets 2 Russian Hackers; FBI Alleges Pair Stole Credit Info*, Seattle Times A1 (Apr 23, 2001); Robert Lemos, *FBI Nabs Russian Hackers*, ZDNet News (Apr 23, 2001), available online at <http://www.zdnet.com/zdnnn/stories/news/0,4586,508199,00.html> (visited May 4, 2001) [on file with U Chi Legal F]; Robert Lemos, *FBI "Hack" Raises Global Security Concerns*, CNET News.com (May 1, 2001), available online at <http://news.cnet.com/news/0-1003-202-5785729.html> (visited May 12, 2001) [on file with U Chi Legal F]. In May 2001, a district court denied a motion to suppress the evidence downloaded from the Russian servers. See *United States v Gorshkov*, No CR00-500C (W D Wash May 23, 2001) [on file with U Chi Legal F]. One of the suspects was convicted of various computer crime charges in October 2001. See Michelle Delio, *'Stung' Russian Hacker Guilty*, Wired News (Oct 17, 2001) available online at <http://www.wired.com/news/print/0,1294,47650,00.html> (visited Oct 20, 2001) [on file with U Chi Legal F].

[24] See notes 88–89 and accompanying text.

[25] See notes 77–81 and accompanying text.

[26] See Council of Europe Committee of Ministers, 109th Sess, Convention on Cyber-Crime Art 32 (adopted Nov 8, 2001), available online at <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm> (visited Nov 14, 2001) [on file with U Chi Legal F] (establishing when parties may access computer data located within another party's borders without that party's authorization). The treaty will enter into force when five states, including at least three members of the Council of Europe, ratify it.

puter systems. The fact that online activities so often cut across international borders raises the question whether states can and should prescribe laws governing those activities. Underlying the debate over state regulation of internet activities are different conceptions of how the rise of online activities affects territorial sovereignty—that is, a state's power to exercise control over all persons and things within its territory.[27] At one end of the debate, commentators such as David Johnson and David Post have taken the position that states cannot and should not regulate online activities in the same way that they regulate other activities.[28] Because a state can only enforce its laws against persons and property located within its borders, they argue, rules designed to govern online activities cutting across borders will be unenforceable and illegitimate.[29] This view at least implicitly suggests that the appropriate conception of territorial sovereignty in the internet context is a narrow one, under which states lack the power to base regulations on harmful effects within the state's territory. At the other end of the debate, Jack Goldsmith has argued that regulation of transnational transactions involving the internet is no less feasible or legitimate than regulation of other transna-

---

[27] See Robert Jennings and Arthur Watts, eds, I *Oppenheim's International Law* 382 (Longmans 9th ed 1992) (discussing components of sovereignty, including "the power of a state to exercise supreme authority over all persons and things within its territory").

[28] See David R. Johnson and David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan L Rev 1367 (1996) (arguing that cyberspace is unique and cannot be governed by laws that rely on traditional territorial borders, instead requiring creation of distinct and separate doctrine to be applied to cyberspace). See also David G. Post and 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 (1998) (using a problem-solving dilemma to support of decentralized decision-making over the internet); David G. Post, *Governing Cyberspace*, 43 Wayne L Rev 155 (1996) (arguing that the nature of the internet destroys the significance of physical location, eliminating the possibility of a single, uniform legal standard); David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J Online L Art 3 (examining the various groups and organizations that can impose substantive rules on the internet and arguing that the lack of physical borders in cyberspace prevents effective rule-making by centralized governments). Others have expressed similar skepticism. See James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U Cin L Rev 177 (1997) (recognizing the difficulties states have encountered in attempting to regulate the global network, but arguing that certain private filtering and control mechanisms will facilitate greater state regulation); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 Emory L J 911 (1996) (arguing that the transnational nature of the internet requires governance by a collection of state, business, technical, and citizen forces); John T. Delacourt, Note, *The International Impact of Internet Regulation*, 38 Harv Intl L J 207 (1997) (contending that national regulation of the internet is inappropriate and that a consensual regime of user self-regulation should be adopted).

[29] See Johnson and Post, 48 Stan L Rev at 1368–78 (cited in note 28).

tional transactions.[30] In support of this view, Goldsmith draws upon a broader conception of territorial sovereignty, under which a state can prescribe rules governing conduct that has harmful effects within its borders, even if the conduct takes place outside of its borders.[31]

Analyzing state claims to conduct cross-border searches reveals that the underlying debate over territorial sovereignty in the internet context is even more complex and more important than commentators acknowledge. As I will argue, among the crucial tasks in evaluating the legality of cross-border searches is to explore how principles of territorial sovereignty apply when a state seeks not only to *regulate* extraterritorial conduct having an effect within its borders, but also to *investigate* that conduct by taking steps within its own borders that affect persons or property in another state. A state conducting a cross-border search and the target state are likely to have different perspectives on the issue. The searching state may view its actions as merely advancing a claimed power to regulate extraterritorial conduct causing harmful effects within its own borders. The target state, however, may view a remote cross-border search itself as extraterritorial conduct with harmful local effects. The target state may believe that principles of territorial sovereignty likewise permit it to "regulate" this harmful extraterritorial conduct—for example, by invoking certain privacy or property protections that

---

[30] See Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 Eur J Intl L 135 (2000) (arguing that unilateral regulation of the internet is legitimate, that the dangers of multinational regulation are exaggerated, and that the spillover effects do not delegitimize unilateral regulation); Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 Chi Kent L Rev 1119 (1998) (examining fallacies in the arguments against government regulation of the internet); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Ind J Global Legal Stud 475 (1998) (maintaining that territorial regulation of the internet is no less feasible or legitimate than territorial regulation of non-internet transactions); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U Chi L Rev 1199 (1998) (proposing that internet transactions be regulated the same as real-space transactions); Jack Goldsmith, *What Internet Gambling Legislation Teaches About Internet Regulation*, 32 Intl Law 1115 (1998) (explaining various regulatory tools governments can use to regulate the internet). See also Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 Cal L Rev 395 (2000) (concluding that selective government regulation of the internet is a better means to protect liberal democratic ideals than self-regulation); Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 Intl Law 1167 (1998) (arguing that internet transactions can be understood and resolved under traditional principles of territorial jurisdiction).

[31] Goldsmith, 65 U Chi L Rev at 1208 (cited in note 30) (noting that customary international law permits a state "to apply its law to extraterritorial behavior with substantial local effects").

prohibit the searching officials' conduct or by objecting to such conduct through diplomatic channels.

Which perspective should prevail? Exploring the competing views of territorial sovereignty underlying the poles of the regulation debate provides a useful starting point for this question; evaluating cross-border search claims, in turn, highlights certain normative bases for refining our understanding of how principles of territorial sovereignty apply in the internet context.

I begin in Part I by outlining certain background principles of international law relevant to a discussion of cross-border searches. First, I explore the principle of territorial sovereignty that, at least outside of the internet context, is thought to permit a state to prescribe laws governing extraterritorial conduct having harmful effects within its borders. I then contrast this principle with the customary international law prohibition on states investigating such conduct in the territory of another sovereign. States typically cope with this gap between their power to regulate conduct and their power to investigate that conduct by relying on legal assistance mechanisms. After examining these mechanisms, I argue that they are unlikely to prove effective in a substantial portion of computer crime cases. Indeed, as I discuss in Part II, the limitations of traditional legal assistance mechanisms have already prompted some states to assert that they possess a power to remotely acquire data accessible to persons within their territory and others to seek recognition of such a power in international instruments.

I explore the legality of these state responses under international law and U.S. constitutional law in Parts III and IV respectively. In Part III, I argue that how we evaluate the responses turns in part on whether the rise of online activities cutting across borders alters the international law principles introduced in Part I. The principle that states have power to regulate extraterritorial conduct with harmful local effects underlies the debate over whether states can and should regulate the internet. Drawing upon the competing views of territorial sovereignty represented in this debate, I examine whether the second principle—that states cannot conduct investigations in the territory of other states—applies to remote cross-border searches. I conclude that the line that allows a state to apply its law to extraterritorial activities but limits a state from investigating violations of those laws in the territory of another sovereign continues to have force, notwithstanding the widespread use of computer systems cutting

across international borders. The customary international law prohibition on conducting investigations in the territory of another sovereign should apply even when a state conducts cross-border searches remotely. This analysis, I argue, helps to refine our understanding of how concepts of territorial sovereignty apply in the internet context.

Having argued that customary international law generally prohibits unilateral cross-border searches, I turn in Part IV to an equally difficult question of U.S. law: whether, to eliminate any customary international law difficulties with cross-border searches, the United States could enter into bilateral or international agreements permitting countries to conduct cross-border searches under their own domestic law standards—standards potentially inconsistent with Fourth Amendment requirements. I argue that an arrangement permitting cross-border searches of data stored within the United States must track Fourth Amendment requirements. In Part V, I note some limitations on and implications of these conclusions.

I. JURISDICTION TO ENFORCE AND THE LIMITATIONS OF TRADITIONAL LEGAL ASSISTANCE MECHANISMS

Before analyzing the legal issues surrounding state claims regarding cross-border searches, it is important to establish certain background principles of international law that illustrate why computer crime investigations present difficulties for law enforcement officials, and that provide a starting point for our evaluation of cross-border search claims. First, at least outside of the internet context, states are not limited to regulating conduct that occurs within their borders.[32] Rather, international law permits states to prescribe laws governing extraterritorial conduct in certain circumstances, including when that conduct has harmful effects within its borders. Second, customary international law generally prohibits states from conducting investigations in another state's territory without that state's consent. Countries ordinarily cope with the gap between their power to prescribe laws and their power to enforce such laws by relying upon a range of legal assistance mechanisms. I argue that such mechanisms are unlikely to be adequate in a significant number of computer crime cases.

---

[32] I discuss the competing theories about whether this principle extends to the internet context in Part III B. See notes 98–124 and accompanying text.

A. Jurisdiction to Regulate and Jurisdiction to Enforce under International Law

International law permits in some circumstances, and most states have provided for, the application of the forum state's laws to activities carried on elsewhere. There are several theories under which a state can seek to prescribe laws governing extraterritorial conduct,[33] but the most important one for our purposes is the theory that a state is justified in regulating conduct producing harmful "effects" within its territory.[34] The widespread accep-

---

[33] Possible bases for a state's assertion of extraterritorial jurisdiction, beyond the effects principle discussed in the text, include the universality principle, which permits a state to enforce sanctions against crimes that have an independent basis in international law (such as genocide or hijacking of aircraft), see Restatement (Third) of Foreign Relations Law § 404 (1987); *United States v Yunis*, 924 F2d 1086, 1091 (DC Cir 1991) (holding that the court had jurisdiction over hijacking of aircraft pursuant to the universality principle); the nationality principle, which permits a state to regulate the conduct of its nationals wherever they are, see Restatement (Third) of Foreign Relations Law § 402(2) comment e (1987) ("a state has jurisdiction to prescribe law with respect to . . . the activities, interests, status, or relations of its nationals outside as well as within its territory"); and the protective principle, which allows a state to regulate extraterritorial activities that threaten its local security, id at § 402(3) comment f ("a state has jurisdiction to prescribe law with respect to . . . certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests"). Finally, the passive personality theory would allow a state to exercise jurisdiction over anyone who injures one of its nationals. Id at § 402 comment g. This theory is the most controversial of the bases for extraterritorial jurisdiction. Jimmy Gurulé, *Complex Criminal Litigation: Prosecuting Drug Enterprises and Organized Crime* 471 (Lexis 2d ed 1996). See also Jordan J. Paust, *Federal Jurisdiction Over Extraterritorial Acts of Terrorism and Nonimmunity for Foreign Violators of International Law under the FSIA and the Act of State Doctrine*, 23 Va J Intl L 191, 202 (1983) (noting that the United States does not recognize the passive personality principle and questioning whether more than a handful of nations accept its validity). The United States has, however, relied on this theory as the basis for exercising extraterritorial jurisdiction for terrorism-related crimes. See Gurulé, *Complex Criminal Litigation* at 472–73 (cited in note 33) (discussing federal statutes relying on passive personality principle).

[34] See, for example, *Strassheim v Daily*, 221 US 280, 285 (1911) ("Acts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a State in punishing the cause of the harm as if he had been present at the effect . . . ."); *Hartford Fire Insurance Co v California*, 509 US 764, 796 (1993) (recognizing applicability of the Sherman Antitrust Act to "foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States"); *Rivard v United States*, 375 F2d 882, 887 (5th Cir 1967) ("All the nations of the world recognize the principle that a man who outside of a country willfully puts in motion a force to take effect in it is answerable at the place where the evil is done . . . .") (internal quotation marks omitted); Goldsmith, 65 U Chi L Rev at 1208 (cited in note 30) (noting that customary international law and the United States Constitution permit extraterritorial jurisdiction over "behavior with substantial local effects"); Gurulé, *Complex Criminal Litigation* at 455 (cited in note 33) (describing the "widely accepted principle of international law" that a sovereign must be able to protect itself from injury, including from acts committed outside its borders that are intended to have detrimental effects within its territory); Paust, 23 Va J Intl L at 203–08 (1983) (cited in note 33) (explaining when a nation may extend jurisdiction to acts

tance of such a power is a relatively recent phenomenon. Until the early 20th century, there was little reason for states to assert such a power, because conduct in one country rarely had effects in another. In 1909, in the well known *American Banana* decision, Justice Holmes captured the view that a state lacked jurisdiction to apply its law to extraterritorial conduct: "[T]he character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done."[35] Dramatic developments in the economy and technology led to the abandonment of this view,[36] and by 1945 Judge Learned Hand found it to be

---

committed abroad but having effects within its territory); Restatement (Third) of Foreign Relations Law § 402(1)(c) (1987) ("a state has jurisdiction to prescribe law with respect to . . . conduct outside its territory that has or is intended to have substantial effect within its territory").

The effects principle is often treated as an application of the so-called "objective territorial" principle. Under the objective territorial principle, a country has jurisdiction over conduct, a constituent element of which occurs within its territory. See Ian Brownlie, *Principles of Public International Law* 304 (Clarendon 5th ed 1998) (describing objective territorial principle). Some commentators, however, treat the effects principle as distinct from the objective territorial principle, on the theory that an exercise of jurisdiction under the latter principle is not an instance of "extraterritorial" jurisdiction at all, in that an element of the conduct occurs within the territory of the regulating state. See Jennings and Watts, eds, I *Oppenheim's International Law* at 472–73 n 37 (cited in note 27) (noting that distinction between effects principle and objective application of the territorial principle "has not always been fully appreciated").

[35] *American Banana Co v United Fruit Co*, 213 US 347, 356 (1909).

[36] For arguments that developments in the economy and technology led to the abandonment of the strict territorial view, see Hannah L. Buxbaum, *The Private Attorney General in a Global Age: Public Interests in Private International Antitrust Litigation*, 26 Yale J Intl L 219, 227–28 (2001) (arguing that in commercial law areas, strict territorialism "proved ill-suited to dealing with the expansion of international commerce"); Stein, 32 Intl Law at 1169 (cited in note 30) ("As people and transactions became more mobile, jurisdictional rules based solely on the current location of the defendant were strained); Jonathan Turley, *"When in Rome": Multinational Misconduct and the Presumption against Extraterritoriality*, 84 Nw U L Rev 598, 609 (1990) (suggesting that "greater transnational commerce following World War I" led to abandonment of the strict territorial rule); R.Y. Jennings, *Extraterritorial Jurisdiction and the United States Antitrust Laws*, 33 Brit YB Intl L 146, 150 (1957) (noting that the strict territorial view "belonged perhaps to the days when communications and travel were still comparatively difficult. In our present shrunken world such a strictly territorial division of jurisdiction may, it can be suggested, be unworkable").

Movement in the United States away from the *American Banana* view can be seen as early as 1911, when the Supreme Court, without discussion, applied the Sherman Antitrust Act to contracts executed in England between American companies and an English company to restrain imports to and exports from the United States. *United States v American Tobacco Co*, 221 US 106, 171–72 (1911). Since American companies were parties to the agreements, jurisdiction did not rest solely on the effects of the agreements. By 1927, the Supreme Court's movement away from the *American Banana* view was more pronounced. See *United States v Sisal Sales Corp*, 274 US 268, 276 (1927) (applying the Sherman Antitrust Act to "a contract, combination, or conspiracy" between American corporations and a Mexican company to control Mexican sisal exports; concluding that

"settled law . . . that any state may impose liabilities, even on persons not within its allegiance, for conduct outside its borders that has consequences within its borders."[37] Although countries initially objected to the United States's application of its economic regulations, such as antitrust laws, to extraterritorial conduct,[38] the principle that a state can prescribe laws governing conduct causing harmful effects within its territory is now generally accepted.[39]

Although a state may have jurisdiction to *prescribe* rules limiting certain extraterritorial conduct, it generally may not *enforce* its law—whether through actions of its courts or actions of its executive officials—outside of its territory. As the Restatement (Third) of the Foreign Relations Law explains, "A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by

---

jurisdiction was proper based in part on the fact that "deliberate acts, here and elsewhere . . . brought about forbidden results within the United States").

[37] *United States v Aluminum Co of America*, 148 F2d 416, 443 (2d Cir 1945) ("*Alcoa*") (holding that Sherman Antitrust Act applies extraterritorially). The court of appeals decided the *Alcoa* case under a statute permitting the Supreme Court to refer a case to a court of appeals for a final decision if the Court could not gather a quorum. As the Supreme Court itself has recognized, the special circumstances under which the case was decided "add to its weight as precedent." *American Tobacco Co v United States*, 328 US 781, 811 (1946) (endorsing the reasoning of the *Alcoa* case).

[38] See, for example, Roger P. Alford, *The Extraterritorial Application of Antitrust Laws: The United States and European Community Approaches*, 33 Va J Intl L 1, 9 (1992) (noting that, in the antitrust context, the effects doctrine "generally was met with disapproval from abroad"); Jennings and Watts, eds, I *Oppenheim's International Law* at 475 (cited in note 27) (noting concern of other states with the United States's broad application of the effects doctrine).

[39] Although the Restatement (Third) of Foreign Relations Law recognizes various bases for exercising extraterritorial jurisdiction, it provides that a state should exercise such jurisdiction only where it is "reasonable" to do so. Restatement § 403(1) (1987) ("Even when one of the bases for jurisdiction under § 402 is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable."). The Restatement's approach has not been followed consistently in U.S. courts, compare *Hartford Fire Insurance Co*, 509 US at 798–99 (rejecting a claim that the Court should decline to exercise jurisdiction under Sherman Antitrust Act on comity grounds), with *Timberlane Lumber Co v Bank of America*, 549 F2d 597, 613–14 (9th Cir 1976) (discussing factors to be considered in determining reasonableness of exercising jurisdiction), and may not reflect a requirement of international law. See, for example, Phillip R. Trimble, Editorial Comment, *The Supreme Court and International Law: The Demise of Restatement Section 403*, 89 Am J Intl L 53, 55–57 (1995) (discussing how U.S. state practice and the Supreme Court have declined to follow § 403); Harold G. Maier, *Extraterritorial Jurisdiction at a Crossroads: An Intersection Between Public and Private International Law*, 76 Am J Intl L 280, 294 (1982) (discussing § 40 of the Restatement (Second) of Foreign Relations Law, the predecessor to § 403 of the Third Restatement).

duly authorized officials of that state."[40] In the criminal context, then, customary international law generally prohibits law enforcement officials from one country from exercising their functions—such as conducting searches or making arrests—in the territory of another state without that state's permission.[41] Wit-

---

[40] Restatement (Third) of Foreign Relations Law § 432(2) (1987). See also *The Case of the S.S. "Lotus,"* 1927 P C I J (ser A) No 10 at 18 ("[T]he first and foremost restriction imposed by international law upon a State is that the existence of a permissive rule to the contrary, it may not exercise its power in any form in the territory of another state."); Brownlie, *Principles of Public International Law* at 310 (cited in note 34) ("The governing principle is that a state cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter."); Jennings and Watts, eds, I *Oppenheim's International Law* at 385–86 (cited in note 27) (illustrating activities that constitute a breach of a state's "duty not to violate another state's independence or territorial or personal authority," including "carry[ing] out official investigations in foreign territory"); H. Lauterpacht, ed, I *Oppenheim's International Law* 327–28 (Longmans 8th ed 1955) ("It follows from the principle of territorial supremacy that States must not perform acts of sovereignty within the territory of other States."); id at 295:

> The duty to respect the territorial supremacy of a foreign State must prevent a State from performing acts which, although they are according to its personal supremacy within its competence, would violate the territorial supremacy of this foreign State. A State must not perform acts of sovereignty in the territory of another State.

[41] Principles of self-defense may justify certain breaches of another state's territorial integrity. Article 51 of the Charter of the United Nations, for example, recognizes an "inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations." Charter of the United Nations Art 51, 59 Stat 1031, Treaty Ser No 993 (1945). See also Jennings and Watts, eds, I *Oppenheim's International Law* at 421 (cited in note 27) ("The justification of self-defence for action which involves the violation of another state's territory is an exception to the general duty of all states to respect the territorial sovereignty of other states."). There is, however, considerable debate about the range of circumstances in which a state can invoke the self-defense exception. For a broad view of the scope of the exception, including an argument that the exception may permit law enforcement officials to take certain actions in response to narcotics trafficking activities on the theory that they present an "increasingly serious threat to the domestic security of the United States," see FBI Authority to Seize Suspects Abroad, Hearing before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 101st Cong, 1st Sess 37 (1989) (statement of Abraham D. Sofaer, Legal Adviser, United States Department of State). For a narrower view, suggesting that the exception only applies "in the context of invasion and national survival," see Jonathan A. Bush, *How Did We Get Here? Foreign Abduction After* Alvarez-Machain, 45 Stan L Rev 939, 981 (1993):

> [S]elf-defense, under Article 51 of the United Nations Charter or other international law, has never been interpreted as a license to use lesser levels of force in the pursuit of strongly sought ends, however virtuous . . . . The self-defense justification applies in the context of invasion and national survival, not as an attempt to ensure individual accountability for foreign crimes.

See also Jennings and Watts, eds, I *Oppenheim's International Law* at 421 (cited in note 27) ("Like all exceptions, [the self-defense exception] is to be strictly applied."). But compare Malvina Halberstam, *In Defense of the Supreme Court Decision in* Alvarez-Machain,

ness, for example, the international outcry when the United States, in investigating the murder of Drug Enforcement Agency agent Enrique Camarena-Salazar, kidnapped a defendant in Mexico in order to bring him to trial in the United States.[42] The gap between a state's power to prescribe rules and its power to enforce them may arise even when a state seeks evidence related to activities within its own territory but located abroad. Such difficulties are more likely, however, when a state is investigating extraterritorial conduct.

States have dealt with this gap between their ability to prescribe laws governing extraterritorial conduct and their ability to investigate such conduct through a variety of legal assistance mechanisms. I survey these mechanisms below, with specific focus on the example of the United States.

---

86 Am J Intl L 736 n 5 (1992) (stating that self-defense principles may justify certain breaches of territorial integrity, including forcible abductions, but confining the argument to circumstances in which a state suspects an individual is involved in terrorist acts).

[42] For discussion of the facts surrounding the U.S. actions, see *United States v Alvarez-Machain*, 504 US 655, 657–58 (1992) (discussing the Alvarez-Machain abduction); Abraham Abramovsky, *Extraterritorial Abductions: America's "Catch and Snatch" Policy Run Amok*, 31 Va J Intl L 151, 161–70 (1991) (describing tactics used during the Camarena investigation and multiple abductions by the United States). For discussion of the international reaction, see, for example, Jimmy Gurulé, *Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad*, 17 Hastings Intl & Comp L Rev 457, 458 n 6 (1994) (noting that several Latin American countries questioned the international juridical validity of *Alvarez-Machain* and its impact on treaties, and that the Canadian Minister of External Affairs stated that a U.S. attempt to kidnap someone from Canada would be seen as a criminal act). Although some of the outcry against the U.S. seizure of Alvarez-Machain was based on the claimed violation of an extradition treaty between the United States and Mexico, see Brief of the Government of Canada as Amicus Curiae in Support of Respondent at 2–4, *United States v Alvarez-Machain*, 504 US 655 (1992) (No 91-712, filed Mar 4, 1992); Brief for the United Mexican States as Amicus Curiae in Support of Affirmance at 2–5, *United States v. Alvarez-Machain*, 504 US 655 (1992) (No 91-712, filed Mar 5, 1992), much of it was based on the view that the unconsented arrest violated customary international law, see Brief of the Government of Canada at 4, 5 (arguing that under the law, customs and usages of nations, official abductions are unlawful); Brief for the United Mexican States at 10–12 (arguing that sovereign equality and territorial integrity are fundamental to an international legal order). Even contemporaneous statements of U.S. government officials support that view. See *Authority of the Federal Bureau of Investigation to Override Customary or Other International Law in the Course of Extraterritorial Law Enforcement Activities*, 13 Op Office Legal Counsel 163, 170–71 (1989) (discussing whether Congress and the Executive can override limitations imposed by customary international law); FBI Authority to Seize Suspects Abroad at 11–12 (cited in note 41) (statement of William P. Barr, Assistant Attorney General, Office of Legal Counsel, United States Department of Justice) (same); id at 32–38 (statement of Abraham D. Sofaer, Legal Adviser, U.S. Department of State) (acknowledging that the principle of territorial integrity bars states from conducting law enforcement activities in the territory of other states, but stating that some breaches of territorial integrity may be justified on the grounds of self-defense).

B. Development of Legal Assistance Mechanisms

Historically, countries seeking evidence from other states relied on formal "letters rogatory" in both civil and criminal matters. Letters rogatory are requests for evidence issued by a court in one country, transmitted through diplomatic channels and seeking the assistance of a court in another country.[43] These letters, however, have limited use. Because courts may issue letters rogatory only in pending cases, from the perspective of the United States they cannot be used to obtain foreign evidence before the grand jury stage of a criminal proceeding.[44] In addition, states honor letters rogatory only as a matter of comity[45] and often provide the requested evidence after a substantial delay.[46]

The limits of letters rogatory prompted countries to develop other methods of securing evidence in criminal matters. First, countries have entered into a variety of multilateral and bilateral arrangements containing procedures for obtaining and providing legal assistance in criminal matters. The first major legal assistance treaty, the European Convention on Mutual Assistance in Criminal Matters, entered into force in 1962.[47] Its signatories undertook "to afford each other . . . the widest measure of mutual assistance" in investigating criminal offenses.[48] Although the treaty contemplated that states would request assistance through letters rogatory, with limited exceptions it *obligated* the parties to carry out such requests.[49] The European experience spurred the

---

[43] See Marjorie M. Whiteman, 6 *Digest of International Law* 204 (Dept of State 1968).

[44] See Michael Abbell and Bruno A. Ristau, 3 *International Judicial Assistance* § 12-3-3(2) at 86 (Intl Law Institute 1990 & Supp 1997) (noting the limited use of letters rogatory in criminal investigations and cases). Letters rogatory can, however, be used to obtain evidence at the grand jury stage. See, for example, *United States v Reagan*, 453 F2d 165, 171–73 (6th Cir 1971).

[45] Whiteman, 6 *International Law* at 204 (cited in note 43) ("such request being made, and being usually granted, by reason of the comity existing between nations in ordinary peaceful times").

[46] Abbell and Ristau, 3 *International Judicial Assistance* § 12-3-3(2) at 87 (cited in note 44) (noting that the circuitous system of using letters rogatory creates significant delays); Jordan J. Paust, et al, *International Criminal Law: Cases and Materials* 551 (Carolina 2d ed 2000) (describing the multi-stage process and noting it can take three to six months to complete). See also Alan Ellis and Robert L. Pisani, *The United States Treaties on Mutual Assistance in Criminal Matters*, in M. Cherif Bassiouni, ed, 2 *International Criminal Law* 403, 403 (Transnational 2d ed 1999).

[47] European Convention on Mutual Assistance in Criminal Matters, 472 UN Treaty Ser 185 (1962).

[48] Id at Art 1, 472 UN Treaty Ser at 186.

[49] See id at Art 3, 472 UN Treaty Ser at 192 (providing that the requested party "shall" execute letters rogatory); id at Art 2, 472 UN Treaty Ser at 186, 192 (setting forth grounds for refusing a request); David McLean, *International Judicial Assistance* 133–34

United States to develop bilateral agreements containing similar obligations.[50] In 1968, the United States entered into negotiations with Switzerland that culminated in the signing of the first bilateral mutual legal assistance treaty (MLAT) in 1973.[51] The United States currently has MLATs in force with more than forty countries.[52] All U.S. MLATs obligate the parties to designate a "cen-

---

(Clarendon 1992) (explaining the procedures under the Convention for use of letters rogatory).

[50] See Ellis and Pisani, *United States Treaties* at 412 (cited in note 46) (discussing the role played by the Convention in the United States developing similar bilateral agreements).

[51] See Treaty with the Swiss Confederation on Mutual Assistance in Criminal Matters, Senate Executive Report 94-29, 94th Cong, 2d Sess 1 (1976); Treaty on Mutual Assistance in Criminal Matters, U.S.-Switzerland, 27 UST 2019, TIAS No 8302 (1977).

[52] In addition to the Swiss treaty, see Treaty on Mutual Legal Assistance in Criminal Matters with Antigua and Barbuda, Dominica, Grenada, and St. Lucia, Senate Treaty Doc 105-24, 105th Cong, 1st Sess (1997) (U.S.-Antigua and Barbuda, entered into force July 1, 1999); Treaty with Argentina on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 102-18, 102d Cong, 1st Sess (1991) ("U.S.-Argentina Treaty") (U.S.-Argentina, entered into force Feb 9, 1993); Treaty with Australia on Mutual Assistance in Criminal Matters, Senate Treaty Doc 105-27, 105th Cong, 1st Sess (1997) (U.S.-Australia, entered into force Sept 30, 1999); Treaty with Austria on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 104-21, 104th Cong, 1st Sess (1995) (U.S.-Austria, entered into force Aug 1, 1998); Treaty with the Bahamas on Mutual Assistance in Criminal Matters, Senate Treaty Doc 100-17, 100th Cong, 2d Sess (1988) (U.S.-Bahamas, entered into force July 18, 1990); Treaty with Barbados on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-23, 105th Cong, 1st Sess (1997) (U.S.-Barbados, entered into force Mar 3, 2000); Treaty with Belgium on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 100-16, 100th Cong, 2d Sess (1988) (U.S.-Belgium, entered into force Jan 1, 2000); Treaty with Brazil on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-42, 105th Cong, 2d Sess (1998) (U.S.-Brazil, entered into force Feb 21, 2001); Treaty with Canada on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 100-14, 100th Cong, 2d Sess (1988) (U.S.-Canada, entered into force Jan 24, 1990); Treaty with the United Kingdom Concerning the Cayman Islands Relating to Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 100-8, 100th Cong, 1st Sess (1987) (U.S.-U.K., concerning the Cayman Islands, entered into force Mar 19, 1990); Treaty with the Czech Republic on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-47, 105th Cong, 2d Sess (1998) (U.S.-Czech Republic, entered into force May 7, 2000); Treaty on Mutual Legal Assistance in Criminal Matters with Antigua and Barbuda, Dominica, Grenada, and St. Lucia, Senate Treaty Doc 105-24, 105th Cong, 1st Sess (1997) (U.S.-Dominica, entered into force May 25, 2000); Treaty with Estonia on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-52, 105th Cong, 2d Sess (1998) (U.S.-Estonia, entered into force Oct 20, 2000); Treaty with France on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 106-17, 106th Cong, 2d Sess (2000) (U.S.-France, entered into force Dec 1, 2001); Treaty with Greece on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 106-18, 106th Cong, 2d Sess (2000) (U.S.-Greece, entered into force Nov 20, 2001); Treaty on Mutual Legal Assistance in Criminal Matters with Antigua and Barbuda, Dominica, Grenada, and St. Lucia, Senate Treaty Doc 105-24, 105th Cong, 1st Sess (1997) (U.S.-Grenada, entered into force Sept 14, 1999); Treaty with Hong Kong on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-6, 105th Cong, 1st Sess (1997) (U.S.-Hong Kong, entered into force Jan 21, 2000); Treaty with Hungary on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 104-20, 104th Cong, 1st Sess (1995) (U.S.-Hungary, entered into force Mar 18,

tral authority" to expeditiously process assistance requests; the requested country can only refuse assistance on the grounds

---

1997); Treaty with Israel on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-40, 105th Cong, 2d Sess (1998) (U.S.-Israel, entered into force May 25, 1999); Treaty with the Italian Republic on Mutual Assistance in Criminal Matters, Senate Treaty Doc 98-25, 98th Cong, 2d Sess (1984) ("U.S.-Italy Treaty") (U.S.-Italy, entered into force Nov 13, 1985); Treaty with Jamaica on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 102-16, 102d Cong, 1st Sess (1991) (U.S.-Jamaica, entered into force July 25, 1995); Treaty with Latvia on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-34, 105th Cong, 2d Sess (1998) (U.S.-Latvia, entered into force Sept 17, 1999); Treaty with Lithuania on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-41, 105th Cong, 2d Sess (1998) (U.S.-Lithuania, entered into force Aug 26, 1999); Treaty with Luxembourg on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-11, 105th Cong, 1st Sess (1997) (U.S.-Luxembourg, entered into force Feb 1, 2001); Mutual Legal Assistance Cooperation Treaty with Mexico, Senate Treaty Doc 100-13, 100th Cong, 2d Sess (1987) (U.S.-Mexico, entered into force May 3, 1991); Convention with the Kingdom of Morocco on Mutual Assistance in Criminal Matters, Senate Treaty Doc 98-24, 98th Cong, 2d Sess (1984) (U.S.-Morocco, entered into force June 23, 1993); Treaty with the Netherlands on Judicial Assistance: Criminal Investigations, 35 UST 1361, TIAS No 10734 (1981) (U.S.-Netherlands, entered into force Sept 15, 1983); Treaty with Panama on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 102-15, 102d Cong, 1st Sess (1991) (U.S.-Panama, entered into force Sept 6, 1995); Treaty with the Philippines on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 104-18, 104th Cong, 1st Sess (1995) (U.S.-Philippines, entered into force Nov 22, 1996); Mutual Legal Assistance Treaty with Poland, Senate Treaty Doc 105-12, 105th Cong, 1st Sess (1997) (U.S.-Poland, entered into force Sept 17, 1999); Treaty with Romania on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 106-20, 106th Cong, 2d Sess (2000) (U.S.-Romania, entered into force Oct 17, 2001); Treaty with St. Kitts and Nevis on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-37, 105th Cong, 2d Sess (1998) (U.S.-St. Kitts and Nevis, entered into force Feb 23, 2000); Treaty on Mutual Legal Assistance in Criminal Matters with Antigua and Barbuda, Dominica, Grenada, and St. Lucia, Senate Treaty Doc 105-24, 105th Cong, 1st Sess (1997) (U.S.-St. Lucia, entered into force Feb 2, 2000); Treaty with St. Vincent and the Grenadines on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 105-44, 105th Cong, 2d Sess (1998) (U.S.-St. Vincent and the Grenadines, entered into force Sept 8, 1999); Treaty with South Africa on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 106-26, 106th Cong, 2d Sess (2000) (U.S.-South Africa, entered into force June 25, 2001); Treaty with the Republic of Korea on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 104-1, 104th Cong, 1st Sess (1995) (U.S.-South Korea, entered into force May 23, 1997); Treaty on Mutual Legal Assistance in Criminal Matters between the Kingdom of Spain and the United States of America, official 1730 UN Treaty Ser 113 (1990) ("U.S.-Spain Treaty") (U.S.-Spain, entered into force June 30, 1993); Treaty with Thailand on Mutual Assistance in Criminal Matters, Senate Treaty Doc 100-18, 100th Cong, 2d Sess (1988) (U.S.-Thailand, entered into force June 10, 1993); Treaty on Mutual Legal Assistance in Criminal Matters with Trinidad and Tobago, Senate Treaty Doc 105-22, 105th Cong, 1st Sess (1997) (U.S.-Trinidad and Tobago, entered into force Nov 29, 1999); Treaty with Turkey on Extradition and Mutual Assistance in Criminal Matters, 32 UST 3111, TIAS No 9891 (1979) (U.S.-Turkey, entered into force Jan 1, 1981); Treaty with Ukraine on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 106-16, 106th Cong, 1st Sess (1999) (U.S.-Ukraine, entered into force Feb 27, 2001); Treaty with the United Kingdom on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 104-2, 104th Cong, 1st Sess (1995) (U.S.-U.K , entered into force Dec 2, 1996); Treaty with Uruguay on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc 102-19, 102d Cong, 1st Sess (1991) (U.S.-Uruguay, entered into force Apr 15, 1994).

specified in the treaty.[53] The treaties generally require the requested state to locate persons believed to be in its territory, to execute requests for searches and seizures, to compel a witness's appearance and production of documents, and to produce records in the government's possession.[54] The treaties ordinarily also provide that states must execute requests in a manner consistent with their own laws.[55] Thus, for example, if a foreign country requests that U.S. officials conduct a search within the United States, the officials must meet the requirements of the Fourth Amendment and other applicable U.S. law.

In addition to country-specific MLATs, the United States has entered into a number of offense-specific treaties and executive agreements containing legal assistance provisions. Two of the earliest agreements, the Hague Convention for the Suppression of Unlawful Seizure of Aircraft[56] and the Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation,[57] obligate states in general terms to provide "the greatest measure of assistance in connection with criminal proceedings brought" in connection with offenses covered by the conventions.[58] The more recent Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[59] contains more detailed legal assistance provisions.[60] Like most bilateral MLATs, the Convention requires signatories to execute searches and seizures, to serve judicial documents and to produce relevant records.[61] The United States has also entered into a variety of tax treaties and executive agreements obligating the parties to exchange such information as is pertinent or necessary to prevent evasion of in-

---

[53] The treaties ordinarily permit a party to refuse to honor a request if the request for assistance relates to a political offense or an offense "under military law which would not be an offense under ordinary criminal law" or the execution of the request would prejudice the "security" or "essential interests" of the requested state. See, for example, US-Argentina Treaty at Art 3(1) (cited in note 52).

[54] See, for example, U.S.-Italy Treaty at Arts 1, 14–15 (cited in note 52) (establishing obligations to render assistance and procedures for taking testimony from witnesses).

[55] See, for example, U.S.-Spain Treaty at Art 5(3) (cited in note 52).

[56] Hague Convention for the Suppression of Unlawful Seizure of Aircraft, 22 UST 1641, TIAS No 7192 (1970) ("Unlawful Aircraft Seizure Convention").

[57] Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage), 10 ILM 1151 (1971) ("Civil Aviation Safety Convention").

[58] Unlawful Aircraft Seizure Convention, Art 10, ¶ 1, 22 UST at 1647 (cited in note 56); Civil Aviation Safety Convention, Art 11, ¶ 1, 10 ILM at 1155 (cited in note 57).

[59] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, UN Doc E/CONF 82/15 (1988), reprinted in 28 ILM 493 (1989).

[60] Id.

[61] Id at Art 7(2), reprinted in 28 ILM at 508–09.

come taxes.[62] Finally, the United States has entered into nonreciprocal agreements with certain bank secrecy jurisdictions—that is, territories with laws providing sufficient protection of bank records as to attract deposits in connection with illegal activities, such as narcotics trafficking. Under these agreements, such jurisdictions must produce and authenticate documentary evidence.[63]

All of the mechanisms described above obligate states to provide legal assistance to another country in the early phase of an investigation—that is, before a state begins a prosecution against a specific target. Cooperation at the police level may supplement these agreements. The United States is one of 178 members of the International Criminal Police Organization (Interpol), an organization that routes requests for police-level assistance from one country to another and facilitates cooperation in combating international crime.[64] In addition, the United States transmits a significant number of requests for investigative information from other countries through Federal Bureau of Investigation or Drug Enforcement Agency legal attachés or liaisons stationed at embassies and consulates abroad.[65] Finally, officials from two countries may agree to conduct a joint investigation of conduct that took place in one country but violated both countries' laws. Even when no violation of its own law has taken place, a country may assist or supervise foreign officials in conducting an investigation within its territory.[66]

---

[62] See generally Abbell and Ristau, 3 *International Judicial Assistance* § 12-3-6 at 101–08 (cited in note 44).

[63] See id § 12-3-5 at 95–97 (explaining the type of information available under these agreements and the lack of reciprocity).

[64] See generally *About Interpol: The Fundamental Principles of Interpol*, available online at <http://www.interpol.int/Public/icpo/Guide/principles.asp> (visited Jan 25, 2001) [on file with U Chi Legal F]. For a discussion of U.S. involvement in Interpol, see Ethan A. Nadelmann, *Cops Across Borders: The Internationalization of U.S. Criminal Law Enforcement* 181–86 (Pennsylvania 1993) (discussing the development of U.S. involvement in Interpol).

[65] Nadelmann, *Cops Across Borders* at 147–60 (cited in note 64).

[66] Abbell and Ristau, 3 *International Judicial Assistance* § 12-3-1 at 82–83 (cited in note 44). For examples of joint investigations, see *United States v Barona*, 56 F3d 1087, 1089–90, 1094 (9th Cir 1995) (holding that in a drug distribution investigation, Danish wiretaps constituted a "joint venture," considering that American agents requested wiretaps and were involved in decoding transmissions and interpreting their relevance); *United States v Peterson*, 812 F2d 486, 490 (9th Cir 1987) (finding that narcotics investigations between the United States and the Philippines was a "joint venture" when United States authorities believed marijuana was destined for the United States and assumed a substantial role).

C. Legal Assistance in Computer Crime Cases

As this discussion illustrates, cooperative arrangements obligating states to assist one another in investigations touching more than one jurisdiction are now widespread. These traditional arrangements, however, are unlikely to prove effective in computer crime investigations.

As online activities become more widespread, more evidence will take electronic form. That fact alone may make it difficult for investigating officials to gather the evidence they seek: evidence in electronic form is fleeting in nature, and gathering it may require a technical expertise that many officials lack.[67] The fact that computer systems cut across international boundaries makes the matter even more complicated. Law enforcement officials attempting to use traditional legal assistance mechanisms to obtain evidence in computer crime cases will encounter two problems. First, more and more evidence will be located across international borders. An overseas gambling operation targeting local users, for example, would likely keep its database of user IDs and passwords on an overseas server. Digital images of child pornography might be stored in one state but viewed in another; even an investigation of the local user might require access to the images stored on the foreign server as well as connection data not readily available to the investigating state.[68] A foreign hacker might gain access to a local computer by using one or many foreign computer systems as staging points; tracing the hacker's route would require securing data available only from those foreign systems.[69]

Although transnational crimes are becoming more common even outside of the computer context, cases in which evidence is primarily located abroad still remain the exception rather than the rule. In computer crime cases, a country with a strong interest in investigating a transaction will often find that crucial evi-

---

[67] See Report of the President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet* 27 (Mar 2000), available online at <http://www.cybercrime.gov/unlawful.pdf> (visited Sept 14, 2000) [on file with U Chi Legal F] (cited in note 11) (noting the complexity and rapid technological changes involved in computer crime cases and emphasizing the need for specialists dedicated to investigating and prosecuting such crimes).

[68] See *Crackdown on Net Child Porn*, CNET News.com (cited in note 18) (noting the arrest of one hundred people in twelve different countries following the seizure of images in the United States).

[69] See *Canada Broadens Its Case Against Suspected Hacker*, NY Times C5 (Aug 4, 2000) (noting that a Canadian hacker used computers in the United States and Korea in his attacks).

dence is beyond its borders. Indeed, evidence may be stored across international borders even when a crime has no other international element. Consider the simplest case—where law enforcement officials seek to obtain evidence that is stored on a computer. For papers to be useful in crime, they generally must be physically located near the criminal. Electronic information, in contrast, need not be physically stored nearby in order to be useful to a criminal. The physical location of electronic evidence therefore often depends upon the fortuity of network architecture: an American subsidiary of a French corporation may house all of its data on a server that is physically located in France; two Japanese citizens might subscribe to America Online and have their electronic mail stored on AOL's Virginia servers.[70] Alternatively, a criminal might deliberately store files on a foreign server to take advantage of the privacy protections of an off-shore data haven.[71] Traditional cooperative arrangements do not contemplate evidence of domestic crime routinely being found only abroad.

The second problem that law enforcement officials relying on traditional legal assistance arrangements will face is that electronic evidence can so easily be lost or destroyed. Electronic evidence located in one country may be readily accessible to a criminal in another, who can remove, alter, or destroy the evidence with a few keystrokes from thousands of miles away. The United States has defended FBI agents' recent cross-border search of data on Russian servers in part on the ground that data otherwise would have been lost.[72] Even when evidence is not deliberately destroyed, it might be unavailable after a short period. Suppose, for example, that a hacker seeks to extract proprietary information from a corporate computer system linked to the internet. Investigating officials may find that the attack originates from a computer outside of the United States and may seek information from a foreign internet service provider. The investigating officials may secure the cooperation of foreign officials in contacting the service provider, only to find that the provider's

---

[70] Sussmann, 9 Duke J Comp & Intl L at 470–71 (cited in note 11) (noting how corporate data is usually maintained at company headquarters and explaining the structure of AOL's network).

[71] See, for example, Jonathan I. Edelstein, Note, *Anonymity and International Law Enforcement in Cyberspace*, 7 Fordham Intel Prop, Media & Enter L J 231, 265–67 (1996) (discussing the possibility of countries using anonymous remailers and computer secrecy laws to create such data havens for criminals).

[72] See Carter, *E-Sting Nets 2 Russian Hackers*, Seattle Times at A1 (cited in note 23) (reporting assistant U.S. attorney's claim that investigators feared destruction of data).

system no longer holds the relevant information. Because traditional cooperative arrangements require time to execute requests for assistance, they are likely to be ineffective with respect to evidence that is fleeting.

Because widespread use of the internet increases the likelihood that electronic evidence will be physically located outside of the boundaries of the investigating state—beyond the reach of investigating officials but accessible to and capable of being deleted by the target of the investigation—unlawful conduct involving computers creates new legal challenges for cooperation among domestic and foreign law enforcement officials. No matter how effectively states streamline current international legal assistance procedures, it is unlikely that governments relying exclusively on such mechanisms can be assured of seizing electronic evidence located within another jurisdiction. In the next Part, I explore state responses to these challenges.

II. MOVING BEYOND TRADITIONAL LEGAL ASSISTANCE MECHANISMS

The difficulties that law enforcement officials have in coping with electronic evidence have prompted states to move beyond traditional legal assistance arrangements in computer crime cases. In negotiations in two multilateral organizations, countries have considered adopting domestic measures that would require internet service providers and other entities to rapidly preserve data based on requests from foreign states. First, in October 1999, the Group of Eight industrialized nations ("G-8")[73] adopted certain principles relating to cross-border access to stored computer data.[74] Under these principles, each state "shall ensure" its ability to secure rapid preservation of data stored in a computer system within its territory when another state requests such preservation.[75] The principles contemplate that a foreign state will follow its request for rapid preservation of such data with a formal legal assistance request to search, seize, copy, or disclose

---

[73] The G-8 includes Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.

[74] See *Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime Communiqué* annex 1 (Moscow, Oct 19–20, 1999) [on file with U Chi Legal F].

[75] Id at annex 1 ¶¶ 1–3 (establishing the rights and duties of member States in the preservation of data stored in a computer system).

the data.[76] Second, member states of the Council of Europe (COE),[77] with the United States participating as an observer, have also considered requiring providers to preserve data on behalf of foreign states. The COE's Committee of Ministers recently adopted a Convention on Cyber-Crime that, among other things, would require states to "adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation" of stored computer data, including "traffic" data concerning the origin, path, and destination of a communication,[78] in response to a request from a foreign state.[79] Under the Convention's procedures, the state seeking the preserved data would request its disclosure, and the target state would obtain the data in a manner consistent with its law.[80] The Convention would also obligate parties to assist one another in obtaining stored content and in collecting traffic data and content in real time.[81]

Although these multilateral efforts to expand cooperation in computer crime investigations have met with much criticism, particularly in the United States, on the ground that they would impermissibly expand the reach of national police authorities and threaten privacy,[82] they in fact represent a relatively modest

---

[76] Id at annex 1 ¶ 4 (establishing that states receiving requests for "access, search, copying, seizure or disclosure of data" must execute requests as "expeditiously as possible").

[77] The Council of Europe is an intergovernmental organization with 43 member states.

[78] Convention on Cyber-Crime at Art 16 (cited in note 26) (defining "traffic data").

[79] Id at Arts 29(1), 29(3). Final approval by the COE's Committee of Ministers opens the Convention for signature and ratification by participating states.

[80] Id at Art 29(3).

[81] Id at Arts 31, 33, 34.

[82] See, for example, Bryan Brumley, *Cybercrime Treaty Raises Concern*, AP Online (Oct 27, 2000), available at 2000 WL 28616521 (stating that groups criticize the treaty for broad powers it gives governments to collect information on citizens); James Evans, *European Cyber-Crime Proposal Blasted*, e-Business World, available online at <http://www.e-businessworld.com/English/crd_council_470984.html> (visited Apr 3, 2001) (noting opposition to provisions requiring internet service providers to retain data); Juliana Gruenwald, *Europeans Defining the Long Arm of the Cyberlaw*, ZDNet Inter@ctive Week Online (Sept 25, 2000), available online at <http://www.zdnet.com/intweek/stories/news/0,4164,2631389,00.html> (visited Sept 25, 2000); Brian Krebs, *E-Mail Campaign Targets International Cyber-Crime Treaty*, Newsbytes (Nov 13, 2000), available online at <http://www.newsbytes.com/news/00/158083.html> (visited Apr 3, 2001) (discussing privacy concerns raised by a coalition of business, privacy, and human rights groups); Declan McCullagh, *Police Treaty a Global Invasion?*, Wired News (Oct 17, 2000), available online at <http://www.wired.com/news/print/0,1294,39519,00.htm> (visited Oct 24, 2000) (noting that thirty civil liberties groups from around the world say the treaty "improperly extends the police authority of national governments" and endangers the privacy of internet users); *Cybercrime Treaty Draft: Take 23*, Wired News (Nov 13, 2000), available online at

means of dealing with the problem. The multilateral efforts, while going far beyond ordinary mutual assistance mechanisms, still generally leave in the hands of the state where the data is physically stored the power to search or seize the data in question.[83] Countries have, however, claimed or sought even broader powers. Some states claim a unilateral power to search and seize data remotely, without assistance from the country in which the data is stored; the United States recently acknowledged that it exercised such a power in connection with an investigation of a Russian hacking ring.[84] Some such assertions of power rest on the view that data accessible from a computer within a territory is "virtually present" there, and can be searched under the same principles as if it were physically present.[85] In other words, data is simultaneously present for law enforcement purposes in all jurisdictions from which a person—for example, the target of an investigation—could lawfully access the data.[86] Even if multilat-

<http://www.wired.com/news/politics/0,1283,40134,00.html> (visited Nov 20, 2001) (discussing opposition to treaty among civil liberties activists and anti-censorship groups); *Europe Slaving Over Cybercrime*, Wired News (Mar 6, 2001), available online at <http://www.wired.com/news/politics/0,1283,42228,00.html> (visited Apr 3, 2001) (discussing opposition voiced at a hearing held by Council of Europe). For specific privacy-oriented comments on drafts of the treaty released between April and November 2000, see, for example, *Comments of the Center for Democracy and Technology on the Council of Europe Draft "Convention on Cyber-crime" (Draft No 24)* (Dec 11, 2000), available online at <http://www.cdt.org/international/cybercrime/001211cdt.shtml> (visited Jan 29, 2001) (recommending specific changes to the treaty to safeguard privacy and human rights); Global Internet Liberty Campaign, Member Letter to Council of Europe Secretary General Walter Schwimmer and COE Committee of Experts on Cyber Crime (Dec 12, 2000), available online at <http://www.gilc.org/privacy/coe-letter-1200.html> (visited Oct 25, 2001); Letter from Bruce Heiman, Executive Director, Americans for Computer Privacy, to Martha Stansell-Gamm and Betty Shave, Computer Crime and Intellectual Property Section, U.S. Department of Justice, Re: Comments of Americans for Computer Privacy on Draft No. 24 of the Council of Europe Convention on Cybercrime (Dec 7, 2000), available online at <http://www.cdt.org/international/cybercrime/001207acp.shtml> (visited Jan 21, 2001); [all internet materials cited in this note on file with U Chi Legal F].

[83] See note 91 and accompanying text.

[84] See note 23 and accompanying text.

[85] An early statement of a British official reflects this view. See Sussmann, 9 Duke Comp & Intl L at 472 (cited in note 11), quoting Paul Boateng, Minister of State for the Home Office (UK), *Tomorrow's Challenges for Law Enforcement*, Keynote Address to the Second International Conference for Criminal Intelligence Analysts (Mar 1, 1999) ("Jurisdiction over a database should not now depend only on where it happens to be physically stored. Where the owners of the system have set it up to be accessible from another jurisdiction, it should be regarded as present in that jurisdiction for law enforcement purposes.").

[86] Such claims are somewhat analogous to the position taken by the United States with respect to records held in foreign jurisdictions by banks with a branch in the United States—that a U.S. court can compel production in the United States of the records held in the foreign jurisdiction, notwithstanding the protections that the records receive under the law of the foreign jurisdiction. See *In re Grand Jury Proceedings Bank of Nova Scotia*,

eral arrangements such as the COE Convention prove useful in some cases, it is all the more likely that states will engage in unilateral cross-border searches; indeed, some view such searches as an essential weapon in any successful strategy to combat certain forms of computer crime.[87]

Other states that have not asserted a broad power to conduct cross-border searches have advocated that such a power be recognized in international instruments. In December of 1997, the Justice and Interior Ministers of the G-8 issued a communiqué advocating the development of principles regarding cross-border searches as well as searches of data whose location is unknown.[88] Despite the Ministers' broad mandate, thus far there has been little agreement on the circumstances in which states should be permitted to engage in cross-border searches. Under the G-8 principles adopted in October 1999, a state can engage in cross-border searches of "open-source" (publicly available) data and data the searching state obtains the lawful consent to search.[89] The COE Convention contains similar provisions.[90] Although the actual cross-border search provisions are fairly limited, both the G-8 and COE have committed to future examination of broader provisions. In addition, states may pursue broader cross-border search provisions in bilateral arrangements.

All three responses to the investigative difficulties that computer crime cases create—proposals for multilateral regimes requiring states to secure a quick freeze of data and to grant expedited access to that data; unilateral assertions of a power to conduct remote cross-border searches; and attempts to gain recognition of cross-border search powers in international forums—raise difficult questions of law and policy. For present purposes, I leave to one side the policy questions raised by the G-8 and COE provi-

---

740 F2d 817, 826–29 (11th Cir 1984) (upholding a district court-imposed fine on a Canadian-based bank where the bank had a pervasive U.S. presence and failed to produce records held in a Cayman Islands branch subject to Cayman Islands' confidentiality laws).

[87] See Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U Chi Legal F 103, 105–06 (describing the practical need for remote cross-border searches to investigate cross-border cybercrimes).

[88] See *Action Plan to Combat High-Tech Crime*, annex to Meeting of Justice and Interior Ministers of the Eight, Communiqué (Dec 10, 1997), available online at <http://www.usdoj.gov/criminal/cybercrime/action.htm> (visited Jan 27, 2001) [on file with U Chi Legal F] (directing officials of member States to undertake certain policies and actions to prevent abuses of information technologies).

[89] *Principles on Transborder Access to Stored Computer Data*, in *Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime Communiqué* annex 1, ¶ 6 (Moscow, Oct 19–20, 1999) [on file with U Chi Legal F].

[90] Convention on Cyber-Crime at Art 32 (cited in note 26).

sions calling for each country to adopt mechanisms for preserving and disclosing data in response to a foreign request. As noted, whatever the wisdom of such an arrangement, it leaves the state in which the data is stored in control of the legal standards upon which preservation or disclosure can occur.[91] I discuss in Parts III and IV the two responses that would create far greater privacy threats: that states will unilaterally claim a power to engage in remote cross-border searches or that states will seek recognition of such a power in multilateral or bilateral arrangements.

III. UNILATERAL CROSS-BORDER SEARCHES UNDER INTERNATIONAL LAW

The main question that unilateral cross-border search claims raise is whether remote cross-border searches conducted without

---

[91] For this reason, two popular criticisms of the COE Convention—that it is inconsistent with the Fourth Amendment and that it would require the United States to jettison certain statutory privacy protections—are off the mark. As discussed below, no treaty can obligate the United States to engage in actions inconsistent with the Fourth Amendment. See text accompanying notes 147–51. To the extent that a multilateral arrangement would obligate the United States to order the preservation of data, the United States could do so only in circumstances meeting Fourth Amendment requirements. The Fourth Amendment would likely permit preservation where there is probable cause to believe that data will be lost if not preserved. As the Supreme Court has repeatedly recognized, officials may lawfully seize control of an item they have probable cause to believe contains contraband, even if they must obtain a warrant before searching the item. See *United States v Jacobsen*, 466 US 109, 114 (1984) (holding that government agents may lawfully seize a package to prevent loss or destruction of suspected contraband without violating the Fourth Amendment, but that a warrant is required to examine the contents after the agents have control of the package); *United States v Ross*, 456 US 798, 809–12 (1982) (reviewing cases holding that government agents must obtain a warrant to search closed packages and containers after gaining control over them); *Arkansas v Sanders*, 442 US 753, 761–62 (1979) (recognizing that police acted properly in seizing luggage they suspected to contain contraband when they had probable cause to believe that the luggage would otherwise be driven away), overruled in part on other grounds, *California v Acevedo*, 500 US 565 (1991); *United States v Chadwick*, 433 US 1, 13 & n 8 (1977) (holding that a warrant was required to search a footlocker in exclusive control of federal agents because there was no danger of the contents being removed or destroyed before a warrant could be obtained), overruled in part on other grounds, *California v Acevedo*, 500 US 565 (1991). In *California v Acevedo*, the Supreme Court overruled portions of its prior opinions holding that officials must obtain a warrant to search containers found within a moving vehicle that officials have probable cause to search. That conclusion does not undermine—and indeed reinforces—the rationale underlying the generally applicable rule that officials may lawfully seize an item without a warrant to prevent its loss or destruction.

Under current U.S. law, the government can require that a service provider preserve certain electronic communications by making a backup copy, even if the government has not obtained a warrant to examine the contents of the communications. 18 USC § 2704(a) (1994) (permitting a governmental entity to include a backup requirement with respect to communications it seeks under a subpoena or court order). The constitutionality of this provision has not been tested.

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. To resolve this issue, we must consider how the rise of online activities affects the principles of international law introduced in Part I A. The views of territorial sovereignty underlying the opposing positions in the debate over the feasibility and legitimacy of state regulation of the internet provide a useful starting point for addressing this question, even if they do not fully resolve it. I ultimately conclude that remote cross-border searches are not distinguishable in legally relevant ways from physical searches. As a result, at least at present, unilateral cross-border searches generally will violate customary international law.

A. The Issue

The starting point for analyzing the legality of unilateral cross-border searches is the principle, discussed in Part I A, that one state generally has no power to conduct a law enforcement investigation within the territory of another state without that state's permission. This limitation reflects a well established rule of customary international law.[92] If foreign officials physically entered the United States and conducted a search without U.S. permission, they would violate customary international law, at least in the absence of a colorable claim that they took these actions in response to a threat to the searching state's integrity or security.[93] The question is whether a principle generally barring a state from conducting law enforcement activities in another state's territory applies when the investigating officials never physically enter the other state, but rather remotely search or manipulate data found on servers within that state.

In examining the applicability of the rule of customary international law just described, it is important to address at the outset the means by which rules of customary international law develop. In the standard account,[94] a rule of customary interna-

---

[92] See, for example, Restatement (Third) of Foreign Relations Law § 432(2) (1987) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."). See also note 40.

[93] See notes 40–42 and accompanying text.

[94] I do not attempt to address the debate over whether this conception or any of several others should prevail. For an outline of the perceived difficulties of this standard

tional law arises from a practice of states consistently followed out of a sense of legal obligation.[95] It is possible to argue, based on this understanding of what constitutes customary international law, that by definition customary international law can impose no limitations upon unilateral cross-border searches, because no consistent state practice as to cross-border searches has yet developed. This view depends on two premises: first, that norms of customary international law operate with a high degree of specificity, such that a particular rule of customary international law does not constrain a state when there are variations in the factual circumstances surrounding the state's potential action; and second, that a remote cross-border search is sufficiently different from other investigative activities barred by the customary international law rule so as to render the rule inapposite.

The first premise is not self-evidently correct. States can almost always point to different factual circumstances justifying departure from a custom; if variations in factual circumstances always exempt states from rules of customary international law, such rules would rarely constrain state conduct. Moreover, in the specific context of the customary international law rule against conducting investigations in the territory of another sovereign, factual variations have not prevented states from objecting to perceived violations of the broad principle.[96] But even if the first

---

formulation, see, for example, Jack L. Goldsmith and Eric A. Posner, *A Theory of Customary International Law*, 66 U Chi L Rev 1113, 1117–18 (1999).

[95] See Restatement (Third) of Foreign Relations Law § 102(2) (1987) ("Customary international law results from a general and consistent practice of states followed by them from a sense of legal obligation."); Brownlie, *Principles of Public International Law* at 4–7 (cited in note 34) (describing practice and obligation components of customary international law); J.L. Brierly, *The Law of Nations; An Introduction to the International Law of Peace* 59–62 (Clarendon 6th ed 1963) (same); Paust, et al, *International Criminal Law: Cases and Materials* at 4–5 (cited in note 46) (same).

[96] For example, states have objected to efforts by the United States to compel foreign banks with branches in the United States to produce certain records in the United States. See *In re Grand Jury Proceedings Bank of Nova Scotia*, 740 F2d 817, 826–29 (11th Cir 1984); Tamar Levin, *Business and the Law: United States vs. Bank of Nova Scotia*, NY Times D2 (Dec 13, 1983) (quoting Canadian criticisms of purportedly extraterritorial enforcement of U.S. subpoenas); Andreas F. Lowenfeld, *International Litigation and the Quest for Reasonableness: Essays in Private International Law* 173 (Clarendon 1996) (noting that Canada and the United Kingdom oppose the enforcement of foreign subpoenas).

More recently, one commentator has suggested that states have come to accept such actions. See Brownlie, *Principles of Public International Law* at 310–12 (cited in note 34) (stating that U.S. courts "have taken the view that whenever activity abroad has consequences or effects within the United States which are contrary to local legislation then the American courts may make orders requiring . . . the production of documents"; noting foreign opposition to such actions but stating that the present position is probably that "a state has enforcement jurisdiction abroad only to the extent necessary to enforce its legislative jurisdiction," and that this position rests upon principles permitting the exercise of

premise is correct, we must determine whether remote cross-border searches are qualitatively different from the sort of physical investigative activities the rule clearly covers. In other words, we must evaluate the second premise—that remote cross-border searches are distinguishable from physical searches in legally relevant ways.

The customary international law rule that one state cannot conduct investigative activities in the territory of another state reflects the basic principle that a state is "sovereign" within its own territory.[97] It is generally not necessary to define precisely what gives rise to the affront to sovereignty in this context, because two objectionable actions go hand in hand: the physical entry of a foreign state's officials and the subsequent search or seizure of persons or property. In the case of a remote cross-border search, however, the search or seizure forms the sole basis for any sovereignty-based objection to the foreign state's conduct. The question, then, is whether the absence of a physical entry eliminates the searched state's sovereignty-based objection to the foreign state's action.

We can view this question as one in a larger set of issues concerning how the law should adapt to the increasingly widespread use of computer systems cutting across borders. Thus far, the scholarly debate over these questions has focused on whether states can and should prescribe laws governing online activities—that is, on whether the first international law principle discussed in Part I A, permitting states to regulate extraterritorial conduct with harmful effects within its borders, applies in the internet context. The views of territorial sovereignty that seem to underlie the opposing poles in this debate, however, can shed some light on how the second principle, prohibiting states from conducting investigations in the territory of another state, applies in the internet context. In the next section, I introduce the poles in the regulation debate and the views of territorial sovereignty underlying those poles. I then draw upon those views to evaluate whether the customary international law prohibition on extrater-

---

jurisdiction over "corporations with complex structures and foreign-based subsidiaries"). Even this view does not necessarily support the first premise discussed in the text. At most, it suggests that the customary international law rule eventually evolved to allow actions such as those taken by the United States, not that the U.S. actions were at the time consistent with customary international law on the theory that the prevailing norm did not apply in the particular factual circumstances.

[97] See Jennings and Watts, eds, I *Oppenheim's International Law* at 382 (cited in note 27) (discussing components of sovereignty, including "the power of a state to exercise supreme authority over all persons and things within its territory").

ritorial enforcement activities should apply when the investigating state's officials never enter the target state's territory, but rather remotely search data stored there.

B. The Regulation Debate

In their provocative article *Law and Borders—The Rise of Law in Cyberspace*, David Johnson and David Post argue that states generally should not attempt to apply geographically based regulations to internet transactions.[98] They first claim that such regulations will be ineffective.[99] Legal institutions, they argue, generally correspond to a particular physical space and exercise control only over conduct that occurs within that space.[100] This fact ordinarily does not interfere with a state's ability to protect persons or property within its borders, because harmful effects tend to occur in close proximity to the conduct that produces them.[101] Because the global computer network allows communications to travel great distances at low cost and with no degradation, Johnson and Post argue, activities to which a state may wish to attach legal consequences can occur as easily outside of a state's borders as within those borders.[102] Recent examples abound. Until December 2000, the web portal Yahoo! permitted users of its auction site to offer Nazi memorabilia for sale. Anti-discrimination groups in France objected to the accessibility of the materials to French internet users, even though Yahoo!'s server operates in California.[103] Similarly, German officials re-

---

98 Johnson and Post, 48 Stan L Rev at 1368–78 (cited in note 28).

99 Id at 1372 ("[E]fforts to control the flow of electronic information across physical borders—to map local regulation and physical boundaries onto Cyberspace—are likely to prove futile, at least in countries that hope to participate in global commerce.").

100 Id at 1368 ("Territorial borders, generally speaking, delineate areas within which different sets of rules apply. There has until now been a general correspondence between borders drawn in physical space . . . and borders in 'law space.'").

101 Id at 1369 (arguing that the correspondence between physical boundaries and "law space" boundaries reflects the fact that harmful effects usually occur in close proximity to the behavior producing them).

102 Johnson and Post, 48 Stan L Rev at 1375 (cited in note 28) (arguing that "the effects of online activities" are not "tied to geographically proximate locations").

103 Two groups, the League Against Racism and Antisemitism ("LICRA") and the French Union of Jewish Students ("UEJF"), sued Yahoo! in French court. Jason Straziuso, *French Anti-Racist Group Sues Yahoo*, AP Online, 2000 WL 19049132 (Apr 11, 2000) (reporting LICRA's suit); Complaint in *Yahoo! Inc v La Ligue Contre Le Racisme et L'Antisemitisme*, No C00-21275, ¶¶ 8, 17–18 (N D Cal Dec 21, 2000) [on file with U Chi Legal F] (noting the location of Yahoo!'s servers in Santa Clara, California, and providing a chronology of complaints filed by LICRA and UEJF). The groups claimed that Yahoo! violated a provision of the French penal code providing:

cently sought to prosecute the operator of a site questioning whether the Holocaust occurred for violating Germany's laws against inciting racism or anti-Semitism, even though the site was based in Australia.[104] In Johnson and Post's view, the fact that the harm a state seeks to prevent can come from anywhere in the world undermines the efficacy of the state's regulation: a state can only enforce its law by exercising physical control over, and imposing sanctions upon, those who violate it.[105]

Johnson and Post also claim that state attempts to regulate online phenomena will largely be illegitimate. First, any attempt to impose a law upon persons situated outside the state's borders is inconsistent with the notion that "those subject to a set of laws must have a role in their formulation."[106] In addition, a physical border provides persons crossing it with notice that they may be subject to different legal rules.[107] Johnson and Post argue that if a state attempts to impose its laws upon online transactions cutting across borders, the state will be subjecting to its legal regime persons who neither consented to the regime nor had notice of its applicability.[108] Moreover, other states in a similar position will

---

> It shall be punished by the fine provided for violations of the fifth class, except for the needs of a film, show, or exhibit including an historical evocation, to wear or to display in public a uniform, insignia, or emblem evoking the uniforms, insignia, or emblems worn or displayed either by the members of an organization declared to be criminal pursuant to Article 9 of the statute of the international military tribunal annexed to the London agreement of August 8, 1945, or by a person found guilty by a French or international court of one or several crimes against humanity provided by Articles 211-1 to 212-3 or provided in law number 64-1326 of December 26, 1964.

Code Pénal Art R 645-1 (France) (translation by author).

In November 2000, a French court ordered Yahoo! to block French users from accessing the material. See Mylene Mangalindan and Kevin Delaney, *Yahoo! Ordered to Bar the French from Nazi Items*, Wall St J B1 (Nov 21, 2000). For an English translation of the French court's November 2000 decision, see <http://www.cdt.org/speech/international/001120yahoofrance.pdf> (visited Dec 13, 2001) [on file with U Chi Legal F]. For a discussion of the case, see Joel Reidenberg, *The Yahoo! Case and International Democratization of the Internet*, Fordham University School of Law Research Paper No 11 (2001), available online at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=267148> (visited Nov 7, 2001) [on file with U Chi Legal F].

[104] See Peter Finn, *Neo-Nazis Sheltering Web Sites In the U.S.; German Courts Begin International Pursuit*, Wash Post A1 (Dec 21, 2000).

[105] Johnson and Post, 48 Stan L Rev at 1369 (cited in note 28).

[106] Id at 1370.

[107] Id.

[108] Id (arguing that the rise of the global computer network destroys the link between geographical location and "the *legitimacy* of a local sovereign's efforts to regulate global phenomena; and . . . the ability of physical location to give *notice* of which sets of rules

have equal claim to regulate the conduct in question, thereby subjecting online actors to an array of potentially inconsistent legal regimes.[109]

As discussed in Part I A, international law generally permits states to regulate extraterritorial conduct causing harmful effects within a state's borders. Although Johnson and Post do not discuss this principle, their analysis implicitly rejects its application in the internet context. If we assume that it is generally legitimate for a state to prescribe laws governing conduct with harmful local effects,[110] Johnson and Post's arguments provide a useful basis for exploring why application of the effects principle might nevertheless be problematic in the internet context. First, the internet dramatically expands the number of transactions that cut across international borders,[111] and a state therefore cannot control data flows into and out of its territory.[112] Second, a state has a limited ability to enforce its regulations against those who use the global computer network to cause harm within its terri-

---

apply"); id at 1375 ("Territorial regulation of online activities serves neither the legitimacy nor the notice justifications.").

[109] Johnson and Post, 48 Stan L Rev at 1374 (cited in note 28) ("[A]ssertions of lawmaking authority over Net activities on the ground that those activities constitute 'entry into' the physical jurisdiction can just as easily be made by any territorially-based authority."); id at 1376 ("[N]o physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws.").

[110] It is possible that Johnson and Post or other commentators who argue that states should not apply geographically based regulations to internet transactions would reject this principle even outside of the internet context. I do not intend to ascribe one view or the other to Johnson and Post. In light of the widespread acceptance of the effects principle, it is useful to ask whether Johnson and Post's arguments call into question the application of the principle in the internet context, even if Johnson and Post or other commentators would question its application more broadly.

[111] Johnson and Post, 48 Stan L Rev at 1372 (cited in note 28) (noting that "[t]he volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities").

[112] Id ("[E]fforts to control the flow of electronic information across borders . . . are likely to prove futile, at least in countries that hope to participate in global commerce."). Of course, a state could control, through ownership or regulation, the internet service providers operating in its territory so as to limit the information its citizens can access. See Timothy S. Wu, Note, *Cyberspace Sovereignty?—The Internet and the International System*, 10 Harv J L & Tech 647, 651 (1997) ("By exercising control over the physical components required for Internet access, the state can regulate cyberspace. At the most basic level, a state can simply choose not to have any connection to the Internet."). Different states have pursued this approach. For a catalog of states that control or regulate internet service providers or attempt to screen out internet content, see *Enemies of the Internet*, Excerpt & Table of Contents (Reporters without Borders & Transfert.net Feb 28, 2001), available online at <http://www.00h00.com/direct.cfm?titre=4802011802> (visited Dec 13, 2001) [on file with U Chi Legal F].

tory,[113] particularly since participants in such transactions are as likely to be individual consumers as companies with foreign assets and presence.[114] These arguments support the view that the internet narrows the conception of territorial sovereignty that ordinarily would support a state's regulation of extraterritorial conduct. In other words, even if regulation of extraterritorial conduct with harmful local effects is generally permissible, the fact that states are less able to control data flows and enforce regulations in the internet context makes state regulation of harmful effects in the internet context less legitimate.

Jack Goldsmith challenges Johnson and Post's conclusions on a number of points,[115] and his conclusions rest on a broader view of territorial sovereignty. Goldsmith accepts both the principle of international law permitting a state to regulate extraterritorial conduct with harmful effects in its territory, and the application of this principle in the internet context. He argues that online activities cutting across international borders are, from jurisdictional and choice-of-law perspectives, similar to other transnational transactions that states have successfully regulated for many years.[116] Although a state generally can enforce its laws only against persons present or holding assets within its territory,[117] or persons the state can successfully bring within its jurisdiction through extradition or other means,[118] the state has a

---

113 Johnson and Post, 48 Stan L Rev at 1371–74 (cited in note 28) (describing how the internet undermines states' power to control online activities).

114 Id at 1370–71 (noting how the internet allows communications to be transmitted great distances at low cost, "without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another"). See also Lawrence Lessig, *Code and Other Laws of Cyberspace* 193 (Basic Books 1999) (arguing that the difficulties in resolving the question of how states should regulate the internet arise in part from the fact that existing tools for resolving conflict of law questions were designed to deal with conflicts among "institutions, or relatively sophisticated actors," not ordinary citizens).

115 The most detailed critique appears in Goldsmith, 65 U Chi L Rev 1199 (cited in note 30). See also sources cited in note 30.

116 Goldsmith, 65 U Chi L Rev at 1211–12 (cited in note 30).

117 Id at 1216.

118 Id. Extradition treaties generally contain a requirement of "dual criminality"—that the offense for which extradition is sought be criminal both in the requesting and requested jurisdictions. See M. Cherif Bassiouni, *International Extradition: United States Law and Practice* 384, 388–93 (Oceana 1996); Michael Abbell and Bruno A. Ristau, 4 *International Judicial Assistance* § 13-2-4 at 66–71 (Intl Law Institute 1990 & Supp 1997). This requirement has already proven to be an obstacle in computer crime cases. For example, the Philippines could neither prosecute nor extradite the individual accused of releasing the "I Love You" virus, because the Philippines had no law banning computer crime at the time of the incident. See Glanz, *"Love Bug" Creator Could Go Scot-Free*, Wash Times at B10 (cited in note 10).

number of other regulatory alternatives. For example, a state can target local end-users who participate in a disfavored transaction[119] or impose obligations on parties that facilitate the transaction, such as internet service providers or financial institutions with a local presence.[120] Accordingly, Goldsmith concludes, state regulation of internet transactions will be more successful than Johnson and Post believe.

Goldsmith also challenges the view that regulation of such transactions is illegitimate. He argues that a conception of territorial sovereignty that does not account for a state's power to regulate activities having harmful local effects is unduly narrow.[121] In addition, even if territorially based regulation will subject online actors to multiple legal obligations, that fact alone does not make such regulation illegitimate[122]—particularly in light of the limitations on a state's power to enforce its regulations.[123] Finally, if one who provides content over the internet can reasonably foresee that the content will then be available across international boundaries and subject to other states' laws, Goldsmith argues, then Johnson and Post's concern about the lack of notice of legal obligations in cyberspace has less force.[124]

As this discussion illustrates, the competing perspectives on the feasibility and legitimacy of internet regulation support different conceptions of territorial sovereignty. If we accept the proposition that states generally have the power to regulate extraterritorial conduct with harmful local effects, the view that states should not regulate internet transactions implicitly rests on the theory that the internet narrows the conception of territorial sovereignty that ordinarily legitimizes extraterritorial regulation. The view that regulation of internet transactions is no less

---

119 See Goldsmith, 65 U Chi L Rev at 1222 & n 98 (cited in note 30).

120 Id at 1222.

121 Id at 1240 ("Under current conceptions of territorial sovereignty, a jurisdiction is allowed to regulate extraterritorial acts that cause harmful local effects unless and until it has consented to a higher law (for example, international law or constitutional law) that specifies otherwise."). See id at 1205 ("The [regulation] skeptics are in the grip of a nineteenth century territorialist conception of how 'real space' is regulated and how 'real-space' conflicts of law are resolved.").

122 Id at 1240 ("[T]here is nothing extraordinary or illegitimate about unilateral regulation of transnational activity that affects activity and regulation in other countries.").

123 Goldsmith, 65 U Chi L Rev at 1220 (cited in note 30).

124 Id at 1244 (arguing that, with respect to notice of the application of local law to extraterritorial conduct, the U.S. Constitution and international law at most require that the defendant be able to reasonably foresee the application of the law; "the standard of foreseeability depends on a complex mixture of what the content provider knows or reasonably should have known about the geographical consequences of its acts, the significance of the extrajurisdictional harms caused by the acts, and the costs of precautions").

feasible or legitimate than regulation of other transactions, in contrast, rests on the theory that the modern conception of territorial sovereignty is broad enough to permit states to regulate extraterritorial activities with harmful effects within their borders, and nothing about the internet undermines this approach.

C. Territorial Sovereignty and Jurisdiction to Enforce

Having identified different views of territorial sovereignty underlying the competing perspectives on the feasibility and legitimacy of internet regulation, it is useful to ask what light, if any, these views shed on the permissible scope of enforcement activities in the internet context. The contours of states' power to conduct enforcement activities affecting persons and property in other states have largely gone unexplored.

In examining states' authority to prescribe rules governing extraterritorial conduct, Johnson and Post and Goldsmith acknowledge the gap between a state's power to regulate extraterritorial conduct and its power to enforce those regulations.[125] For Johnson and Post, the gap between a state's regulatory power and its enforcement power supports an argument that states should not seek to apply territorially based regulations to online activities, because the state's inability to enforce its regulations against law-violators not located within its territory renders any attempt to regulate both futile and illegitimate.[126] In contrast, Goldsmith believes that this gap reinforces, rather than undermines, the legitimacy of territorially based regulation. The fact that a state can principally enforce a regulation only against persons with presence or assets within its jurisdiction is an important check against inconsistent or overzealous regulation of online transactions by multiple sovereigns.[127]

Although limitations on states' jurisdiction to enforce thus figure prominently in the regulation debate, scholars have largely confined their discussion of enforcement authority to the power of courts to exercise jurisdiction and thereby to subject persons or property to a final, binding judgment, whether civil or criminal.

---

[125] See text accompanying notes 105, 117–18.

[126] Johnson and Post, 48 Stan L Rev at 1369 (cited in note 28) ("Law-making requires some mechanism for law enforcement, which in turn depends on the ability to exercise physical control over, and impose coercive sanctions on, law-violators.").

[127] Goldsmith, 65 U Chi L Rev at 1220 (cited in note 30) ("[T]he [regulation] skeptics exaggerate the threat of multiple regulation of cyberspace information flows. This threat must be measured by a regulation's enforceable scope, not by its putative scope. And the enforceable scope is relatively narrow.").

As a result, scholars seem to assume that the limitations are relatively static. Whether the limitations are static in the internet context, however, is precisely the question we must address. As more and more evidence is stored in electronic form, does the line between a state's jurisdiction to regulate extraterritorial conduct—permissible if extraterritorial conduct causes harm in the state's territory—and a state's jurisdiction to investigate activities in the territory of another sovereign—impermissible even in the face of harmful effects within its territory—begin to blur? I use the views of territorial sovereignty underlying the competing perspectives on the feasibility and legitimacy of internet regulation as a starting point for answering this question.

As noted above, the position that states cannot and should not regulate internet transactions—despite the fact that states regulate other transnational transactions—seems to rest upon the premise that the rise of online activities narrows state power.[128] This narrower view of state power presumably would not support a state's claim to a right to engage in a remote cross-border search: if a state cannot legitimately regulate online activities occurring outside its borders, there is no basis for it to conduct investigative or other enforcement activities. The problem, however, is that states can invoke a remote cross-border search power not only in investigations of extraterritorial conduct, but also in connection with an otherwise domestic investigation involving evidence fortuitously or deliberately stored abroad.[129]

Moreover, the existing customary international law limitation on one state conducting investigative activities in the territory of another sovereign is itself premised on robust principles of territorial sovereignty. If the position that states cannot and should not regulate internet transactions rests on the premise that the internet narrows state sovereignty, then this narrower conception of state sovereignty tends to undermine the limitation. For example, to the extent that a state's objection to cross-border investigative activities would rest on the state's power to control the flow of electrons into its borders, Johnson and Post's arguments with respect to state regulation essentially concede that states lack this power.[130] And to the extent that a state could ob-

---

[128] See text accompanying notes 110–14.

[129] See text accompanying notes 70–71.

[130] See Johnson and Post, 48 Stan L Rev at 1372 (cited in note 28) (noting limitations on states' power to control flow of electronic information).

ject to a cross-border search on the ground that the activities of foreign officials violate its laws—such as prohibitions on hacking or protections on privacy—Johnson and Post's regulation arguments would suggest that these protections cannot legitimately apply to extraterritorial conduct. After all, laws protecting privacy or prohibiting hacking are not, in jurisdictional terms, distinguishable from state laws governing the accessibility of harmful content over the internet; all of these forms of regulation are designed to prevent extraterritorial conduct with harmful effects in the target state.[131]

As this discussion suggests, the narrow conception of territorial sovereignty underlying the view that states cannot regulate internet transactions would arguably suggest that all geographically based protections of data are illegitimate—and that principles of territorial sovereignty therefore do not constrain cross-border searches. Returning to Johnson and Post's arguments, however, it is possible to arrive at a different conclusion.[132] Although Johnson and Post speak in very broad terms about the ineffectiveness and illegitimacy of territorially based regulation of internet transactions, they seem primarily concerned with state regulation of internet content that is merely accessible from within a state's territory, and not with regulation of activities specifically targeted at a state's territory and intended to cause harm there. The distinction between the two types of regulation is important. The perceived injustice in regulating internet content is that an individual providing content may be unable to make that content publicly available where the content is lawful, with certainty that it will not be accessed where it is unlawful.[133]

---

[131] For a similar argument, see Goldsmith, 65 U Chi L Rev at 1244 (cited in note 30) (arguing that, in terms of fairness, there is no distinction between subjecting a content provider to the laws of a foreign jurisdiction and subjecting one who releases a virus that destroys computers connected to the internet to the laws of a foreign jurisdiction).

[132] Again, while Johnson and Post's assumptions and arguments provide a useful tool for exploring conceptions of territorial sovereignty, I do not intend to attribute to Johnson and Post any conclusions about states' power to conduct remote cross-border searches. Because Johnson and Post argue that states should not regulate the internet, they might well conclude that any state enforcement activities associated with such regulation are also illegitimate. Even so, the arguments underlying their conclusions are useful in exploring a more moderate view—that, even conceding that a state can regulate some transnational transactions, regulation of internet transactions cutting across international borders is illegitimate.

[133] Johnson and Post, 48 Stan L Rev at 1373–74 n 20 (cited in note 28) ("It is our contention that posting offensive materials in areas where unwilling readers may come across them inadvertently raises problems that are best addressed by those who understand the technology involved, rather than by extrapolating from the conflicting laws of multiple geographic jurisdictions.").

In other words, even a provider who intends that users view his or her content only where it is lawful to do so may fear liability in a state where it is unlawful.[134]

This concern does not, of course, support the conclusion that all territorially based regulation of internet activities is illegitimate. Rather, it supports the narrower conclusion that states should not seek to regulate a content provider when the provider makes content available in such a manner that only the affirmative, intentional conduct of a local end-user triggers the harm the state seeks to avoid. This narrower conclusion leads to a different view of whether states can conduct remote cross-borders searches. Such searches are not analogous to the mere provision of content without intent that the content be accessed where it is unlawful, but rather to activities directed at and intended to cause harm in another territory. Here, the harm in question is an

---

[134] See note 34 and accompanying text. The distinction drawn in the text between activities directed at a particular state and intended to cause harm there and activities that cause harm only by virtue of the intervening acts of a local user is somewhat analogous to the distinction U.S. courts draw between different types of websites when determining whether a court's exercise of personal jurisdiction over a defendant comports with due process. Due process requires that a defendant have "minimum contacts" with the forum such that the exercise of jurisdiction would not offend notions of fair play and substantial justice. *International Shoe Co v Washington*, 326 US 310, 316 (1945). If a defendant lacks the continuous and systematic contacts that would support an exercise of general jurisdiction, a court will determine whether to exercise specific jurisdiction by inquiring whether the defendant has purposefully availed itself of the privilege of conducting activities within the forum, see *Burger King Corp v Rudzewicz*, 471 US 462, 475 (1985), and whether an exercise of jurisdiction would be reasonable, see *World-Wide Volkswagen Corp v Woodson*, 444 US 286, 297 (1980). In applying these principles to internet cases, courts generally have declined to exercise jurisdiction over a defendant who operates a "passive" site—that is, one that merely makes information available to persons in another jurisdiction. See, for example, *Cybersell, Inc v Cybersell, Inc*, 130 F3d 414, 419–20 (9th Cir 1997) (holding that an Arizona court lacked personal jurisdiction over operators of a Florida-based website because the site was merely informational and was geared for local activity); *Bensusan Restaurant Corp v King*, 937 F Supp 295, 301 (S D NY 1996) (concluding that a defendant who operated a website providing general information about a local jazz club did not purposely avail himself of the laws of another state in which the site could be accessed). Courts have, however, exercised personal jurisdiction over defendants who operate "interactive" sites designed to permit users to exchange information with the site. See *Maritz, Inc v Cybergold, Inc*, 947 F Supp 1328, 1332–33 (E D Mo 1996) (holding that jurisdiction was proper where a website encouraged users to add addresses to an automated mailing list to receive updates about upcoming service). In addition, courts have exercised jurisdiction over defendants who "do business" over the internet, thus specifically directing activities at particular forums. See *CompuServe v Patterson*, 89 F3d 1257, 1264–65 (6th Cir 1996) (holding that defendant who used CompuServe's website to market and sell his software in Ohio purposefully directed activities toward Ohio); *Zippo Manufacturing Co v Zippo Dot Com, Inc*, 952 F Supp 1119, 1125–26 (W D Pa 1997) (finding personal jurisdiction where defendant contracted with seven internet providers within the forum state to provide services for more than three thousand customers residing in that state).

intentional interference with the searched state's power to provide privacy or property protections within its territory. Viewed this way, the effect of the remote search or seizure is functionally equivalent to the sort of actions at issue in the *Alvarez-Machain* case, where the United States intentionally interfered with Mexico's power to protect its nationals.[135] Thus, even if the internet narrows a state's territorial sovereignty, by rendering regulations of certain conduct—specifically, conduct not directed toward causing harm in a particular territory—illegitimate, the resulting principle cuts against, not in favor of, state claims to a unilateral remote cross-border search power.

As this discussion suggests, the view that geographically based regulation of internet transactions is illegitimate does not call into question the customary international law principle prohibiting a state's law enforcement officials from performing activities in the territory of another sovereign, or its application to remote cross-border searches. Indeed, evaluating state claims regarding cross-border searches helps bring into focus the concerns underlying the view that states should not regulate internet transactions. The perceived legitimacy problems arise not when a user specifically directs its activities to a particular country seeking to cause harm there, but rather when a content provider merely makes material available and the local harm follows from the affirmative conduct of a local user.

I now turn to the other pole in the regulation debate. Goldsmith argues that the modern conception of territorial sovereignty permits a state to regulate activities having harmful effects wherever the activities occur.[136] At first glance, this approach would seem to suggest that concepts of territorial sovereignty likewise empower a state to protect property or persons within its territory against the actions of a foreign state, even when foreign officials never set foot in the target state's territory.

Focusing on the effects principle on which Goldsmith's view about regulation relies, however, reveals that the matter is not so simple. Just as the target state would likely argue that it can legitimately prevent or respond to a foreign state's remote search because of the harm the search would cause within its borders, the searching state would likely argue that its actions are simply

---

[135] See text accompanying notes 41–42.

[136] Goldsmith, 65 U Chi L Rev at 1208 (cited in note 30) (noting that customary international law permits a state "to apply its law to extraterritorial behavior with substantial local effects").

a response to conduct occurring in the target state but causing harm within its borders. In other words, the view that states have the power to conduct remote cross-border searches presents a conflict between two claimed sovereignty interests: the interest of the target state in regulating harm caused by the extraterritorial conduct of the searching state's officials; and the interest of the searching state in regulating the harm giving rise to the search.

The view of territorial sovereignty underlying Goldsmith's position thus highlights, but does not resolve, a stark conflict between competing sovereignty claims. How do we resolve this conflict? Do the competing sovereignty claims at issue in cross-border search situations render the general customary international law rule against performing law enforcement activities in the territory of another state inapplicable? We can approach these questions by noting that this same conflict exists when foreign officials physically enter another state to conduct investigative activities. The searching state may believe that international law permits it to regulate certain activities, and the power to enforce its regulations is a necessary incident to this power even when doing so would interfere with another state's sovereignty. This approach, of course, is not consistent with the distinction typically drawn between a state's jurisdiction to regulate and a state's jurisdiction to enforce; while a state can regulate extraterritorial conduct, it generally cannot take enforcement actions extraterritorially.[137] The argument that cross-border searches are outside of the customary international law rule barring extraterritorial law enforcement activities, then, must rest on the conclusion that the line between jurisdiction to regulate and jurisdiction to enforce collapses in the internet context. Accordingly, we must examine the basis for this line and ask if features of the internet alter it.

The gap between states' power to regulate and states' power to enforce such regulation is actually of relatively recent vintage. As previously noted, until the mid-twentieth century, states' regulatory powers were thought to extend only to their borders.[138] Indeed, other states protested U.S. attempts to apply its regulations to extraterritorial activities.[139] When a state regulates extraterritorial activities, its actions interfere to some extent with

---

137 See Part I A.

138 See text accompanying notes 35–36.

139 See note 38 and accompanying text.

the foreign state's sovereignty, in the sense that the regulating state's action might disrupt certain policy goals in the state where the regulation's effects are felt. For example, within the United States, the First Amendment permits only limited government regulation of speech; the policy goals underlying this provision are to some extent frustrated when France seeks to enforce a ban on the display of certain objectionable materials against a company that operates servers in the United States and caters principally to a U.S. audience.[140] Similarly, the application of a U.S. rule that would prohibit British reinsurers from refusing, in concert, to sell certain types of insurance in the United States indirectly affects a British rule permitting such actions, in that those companies seeking to comply with the U.S. rule will take actions that British law would not require.[141]

These interferences, however, are largely indirect. Nothing prevents a state from adopting its own regulatory scheme and applying it where its sovereignty permits. An extraterritorial regulation may frustrate certain policy goals by forcing private parties within one state's territory to adjust their activities to conform to a foreign state's law. But the primary purpose of such regulation is likely to be the advancement of certain regulatory goals within the regulating state; frustration of the foreign state's policy goals is merely a byproduct of the regulating state's action. The interference with the sovereignty of the state in which the regulated conduct occurs is relatively minor, in the sense that the regulating state's actions are not specifically directed toward interfering with the other state's sovereign interests.

When a foreign state's officials enter a state's territory to perform investigative functions, the interference with sovereignty is in no sense indirect: the investigating state specifically intends to interfere with the target state's ability to exert exclusive control over persons and property within its borders. This distinction between direct and indirect interferences with a state's sovereign interests parallels the distinction previously noted between private activities specifically directed at a particular state and intended to cause harm there and private activities that cause harm indirectly by virtue of the intervening acts of a local user.[142] Activities specifically directed at a particular state implicate a

---

[140] See note 103 and accompanying text.

[141] See *Hartford Fire Insurance Co v California*, 509 US 674 (1993) (applying the Sherman Antitrust Act to actions of British reinsurers).

[142] See text accompanying notes 132–34.

state's sovereignty interests even under a narrow conception of territorial sovereignty. If we distinguish between a state's power to regulate and its power to conduct investigative activities based on the impact that each power has on the affected state's sovereign interests, then the question with respect to remote cross-border searches is whether the fact that searching officials never enter the target state's territory renders this distinction inapplicable. In other words, does the fact that the searching officials never enter the target state's territory 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—here, a regulatory scheme designed to protect persons or property within its territory?

There are three potential bases for arguing that a remote cross-border search, like mere regulation, presents only an indirect affront to another state's sovereignty and that states should therefore have more freedom to conduct remote cross-border searches than they do to enter the target state and conduct physical searches. First, it could be argued that a remote search is less invasive than a physical search. It is not clear, however, why this is so.[143] If the sovereignty interest at issue is the target state's power to protect persons and property within its borders, it does not matter whether interference with that power comes from inside or outside of the target state. If this interference were irrelevant to the sovereignty analysis, then a foreign state could, without objection, rely upon persons already legitimately within the target state's territory to conduct its investigative activities. And in the case of a remote cross-border search in which the

---

[143] As U.S. courts have suggested, the sort of unauthorized access to a computer system involved in a cross-border search is analogous to a trespass to chattels. See note 161. This interference with property interests—as well as personal privacy interests—distinguishes a remote cross-border search from other activities, such as the use of satellites for remote sensing related to management of natural resources and environmental protection, that are not thought to violate international law. See Principles Relating to the Remote Sensing of the Earth from Outer Space, UN General Assembly Res 41/65, 42 UN GAOR Annex at 2 (95th Plenary Meeting), UN Doc A/RES/41/65 (1987) (adopting principles relating to remote sensing of the Earth from space); United Nations: Committee on the Peaceful Uses of Outer Space, Draft Principles on Remote Sensing, 25 ILM 1331, 1331 (1986) (explaining that the principles do not adopt the proposition that "national sovereignty required the consent of a sensed State prior to foreign sensing"); Hamilton DeSaussure, *Remote Sensing Satellite Regulation by National and International Law*, 15 Rutgers Comp & Tech L J 351, 353–58 (1989) (explaining the debate over whether remote sensing violates international law). Analogously, the notion that a foreign country's manipulation of data is akin to a trespass and to interference with protected privacy interests distinguishes a cross-border search from activities such as using powerful equipment to view events occurring across a border but otherwise in plain view.

searching state knows where the data is located, this interference is not merely a byproduct of a policy intended to operate both within and without its borders, but an intentional harm directed at the target state's territory.

Second, in some circumstances it will not be possible for a searching state to know where the data it seeks is located. Even if this observation is correct, it does not lead to the broad conclusion that states are free to engage in cross-border searches in all circumstances; at most, it suggests that an accidental search of data in a foreign state does not have the sort of direct, intended effect on state sovereignty that justifies the distinction between jurisdiction to regulate and jurisdiction to enforce, not that all cross-border searches fail to produce such effects.

Third, the architecture of the internet is such that the location of data may be fortuitous. The target state's interest in protecting persons and property within its borders is therefore likely to be attenuated in some circumstances. A searching state may have a stronger interest in the data than the state in which the data is stored. For example, if two French citizens communicate by e-mail, their communications may be stored in the United States.[144] But it is easy to imagine analogous circumstances in which a foreign state has a much stronger interest in physically acquiring persons or property than the target state has in sheltering such persons or property. For example, a person facing criminal charges in one state may flee to another. Though the second state may have an obligation to return the accused to the first state, the first state's officials are not free to enter the target state's territory merely because of its stronger interest in bringing the accused to justice or because of the target state's lack of interest in sheltering the individual. Relatedly, the possibility that an individual will deliberately store data so as to take advantage of a favorable legal regime does not justify a departure from the customary international rule against conducting searches in the territory of another state. Bank secrecy jurisdictions present similar problems, and states do not take the view that they can physically seize evidence within such jurisdictions merely because of the interest they may have in retrieving the evidence.[145]

---

[144] See note 70 and accompanying text.

[145] As discussed earlier, the United States has taken the position that it can compel the production of the records of foreign banks with branches in the United States. See notes 86 and 96; *In re Grand Jury Proceedings Bank of Nova Scotia*, 740 F2d 817, 826–29 (11th Cir 1984) (upholding district court order compelling a bank to produce records held

This discussion suggests that the customary international law rule against one state conducting investigative activities in another state's territory provides a strong basis for states to object to remote cross-border searches of data within their territory. Of course, it may be that over time states come to accept such searches as legitimate. Customary international law, after all, is formed through the practice of states.[146] But to the extent that states seek to conform their actions to perceptions of applicable international law rules, there is a strong argument that the general rule against conducting investigative activities in the territory of another sovereign applies even when the searching state's officials do not enter the target state's territory, but merely interfere with the target state's power to provide privacy or property protections there.

Notions of state sovereignty underlying the various views about the internet do not alter this conclusion. A broad reading of Johnson and Post's conclusions would lead to the view that there is no basis for a state to object to a remote cross-border search. But we should be reluctant to accept this broad reading, since the specific examples on which Johnson and Post rely do not point toward this view to the exclusion of others, and since it would undermine the basis for geographically based protections of data from intentional harms caused by private parties as well. A narrower understanding of Johnson and Post's conclusions leads to the view that a remote cross-border search, unlike merely making content accessible, is an act directed at specific territories and intended to cause harm there.

Goldsmith's broader acceptance of a state's power to regulate online activities would support two conclusions: the conclusion that cross-border searches are improper because the searched state's sovereignty extends to protecting persons and property within its territory against harmful extraterritorial conduct, including that of a foreign state; or the conclusion that cross-border searches are proper because they are merely incident to the

---

in a foreign jurisdiction). Other states, at least initially, viewed these U.S. actions as violative of international law. See note 96. Even if such actions are permissible under international law, it does not follow that customary international law permits cross-border searches. To request the U.S. branch of a bank to secure production of records of another branch located abroad is essentially to impose a regulatory requirement on the local bank that has the collateral effect of frustrating the policy underlying the foreign jurisdiction's bank secrecy laws. Compelling the U.S. branch to secure the production of records is, from the perspective of the foreign state, less invasive than conducting a search of records in the foreign state.

[146] See note 95 and accompanying text.

searching state's lawful power to regulate extraterritorial conduct causing local harm. Which view prevails depends upon whether one views the distinction between jurisdiction to regulate and jurisdiction to enforce as having continuing force with respect to internet activities. I have argued that several possible claims that the distinction lacks continuing force are unpersuasive.

IV. COOPERATIVE CROSS-BORDER SEARCH ARRANGEMENTS

I argued above that remote cross-border searches conducted without the permission of the state in which the searched data is stored generally will violate customary international law. The logical answer to this problem is, of course, that a state can simply give the searching state permission to examine data located within its territory. Some states have responded to the investigative challenges that computer crime cases present by proposing a consent-based regime, under which states would permit other states to conduct cross-border searches in their territory under defined circumstances.

A consent-based regime permitting foreign searches of U.S. data would raise difficult policy questions, particularly in light of the fact that the United States is the repository of so much data. Such a regime would also raise difficult legal questions. In particular, one hurdle to such an arrangement is the protection that domestic law may afford electronic data against certain means of investigation, even by domestic officials. From the perspective of the United States, an arrangement recognizing a broad power to conduct cross-border searches would raise a difficult question of constitutional law—whether foreign searches of data located within the United States could proceed on foreign law standards lower than those of the Fourth Amendment.

I begin addressing this question by examining what constraints the Constitution imposes on the United States's ability to enter into international agreements. It is well established that such agreements must conform to the Constitution; but whether a cross-border search arrangement would trigger constitutional requirements at all is precisely the question we must address. The answer to that question depends on whether a foreign state's conduct under the agreement is attributable to the United States for constitutional purposes. To evaluate the significance of foreign conduct under a cross-border search arrangement, we can draw again upon the different conceptions of territorial sovereignty

discussed in Parts III B and III C. I argue that because states retain the power to protect data stored within their territory, as against competing claims by other states with an interest in that data, a consensual cross-border search arrangement has the significant effect of removing legal obstacles to a foreign state's search. This fact makes the resulting state conduct attributable to the United States for constitutional purposes. Accordingly, any agreement permitting remote foreign searches of data located within the United States must take account of Fourth Amendment concerns.

A. Constitutional Constraints on International Arrangements

On the surface, the question whether the Constitution constrains the United States in entering into an arrangement governing cross-border searches might seem to be relatively straightforward. It is well established that treaties must conform to constitutional standards and are invalid insofar as they do not.[147] This principle means that an agreement cannot confer upon U.S. officials a power that the Constitution would otherwise prevent them from exercising. The leading case reflecting this principle, *Reid v Covert*,[148] involved executive agreements and a provision of the Uniform Code of Military Justice (UCMJ) authorizing U.S. military courts to try dependents of members of the armed services for offenses committed overseas.[149] The Court granted habeas relief to two dependents who claimed that their trials by U.S. courts martial in England and Japan violated Article III, section 2 of the Constitution and the Fifth and Sixth Amendments, which imply a requirement of a trial by jury following presentment or indictment by a grand jury.[150] Writing for a plurality,

---

147 See, for example, *Boos v Barry*, 485 US 312, 324 (1988) (stating the long-standing principle that international agreements are subject to the Bill of Rights and must conform to the requirements of the Constitution); *Reid v Covert*, 354 US 1, 16 (1957) (plurality opinion) (same); Restatement (Third) of Foreign Relations Law § 302(2) (1987) ("No provision of an agreement may contravene any of the prohibitions or limitations of the Constitution applicable to the exercise of authority by the United States."); id at § 302(2) comment b ("The view, once held, that treaties are not subject to constitutional restraints is now definitely rejected.").

148 354 US 1 (1957).

149 See id at 3–4 (describing the use of Article 118 of the Uniform Code of Military Justice to try the wife of a sergeant in the United States Air Force who murdered her husband at an airbase in England).

150 Id at 7–8:

> The language of Art. III, § 2 manifests that constitutional protections for the individual were designed to restrict the United States Government

Justice Black concluded that the article of the UCMJ authorizing courts martial to exercise jurisdiction over crimes committed by persons accompanying members of the armed services overseas could not be sustained as legislation necessary to carry out U.S. obligations under the international agreements: "The obvious and decisive answer to this, of course, is that no agreement with a foreign nation can confer power on the Congress, or on any other branch of Government, which is free from the restraints of the Constitution."[151]

Reid and like cases provide guidance for certain aspects of an agreement governing cross-border searches: to the extent that an agreement would confer power upon *U.S.* officials to conduct remote computer searches of data located *abroad*, that power must be exercised in conformity with the Fourth Amendment.[152] To the

---

> when it acts outside of this country, as well as here at home. . . . The Fifth and Sixth Amendments, like Art. III, § 2, are also all inclusive with their sweeping references to "no person" and to "all criminal prosecutions."

[151] Id at 16. Justices Frankfurter and Harlan each concurred in the result in *Reid* on narrow grounds, thereby confining the Court's holding to circumstances in which dependents of members of the armed forces sought to invoke the protections of the Constitution in capital cases in time of peace. See id at 45 (Frankfurter concurring); id at 65 (Harlan concurring). While declining to hold that U.S. citizens are entitled to the full range of constitutional protections in all overseas criminal prosecutions, neither Justice questioned the proposition that, in circumstances in which constitutional protections apply, a treaty cannot authorize the United States to contravene those protections. See id at 56 (Frankfurter concurring) ("Governmental action abroad is performed under both the authority and the restrictions of the Constitution—for example, proceedings before American military tribunals, whether in Great Britain or in the United States, are subject to the applicable restrictions of the Constitution.").

[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. In *United States v Verdugo-Urquidez*, 494 US 259 (1990), the Supreme Court held that U.S. officials could conduct a search in a foreign country without meeting Fourth Amendment requirements where the searched party lacked any voluntary connection to the United States. Id at 261, 274–75. *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—that is, a citizen or resident. Id at 274–75 (denying a defendant the right to claim Fourth Amendment protection for a search occurring when "he was a citizen and resident of Mexico with no voluntary attachment to the United States"); id at 277–78 (Kennedy concurring) ("[T]he Constitution does not require U.S. agents to obtain a warrant when searching the foreign home of a nonresident alien.").

If U.S. officials seek to search the foreign data of a person who lacks a substantial connection to the United States, *Verdugo* provides a basis for arguing that Fourth Amendment requirements do not apply. In the Russian hacking case, see note 23 and accompanying text, the district court denied the defendant's motion to suppress the data U.S. agents downloaded from Russian servers in part because the defendant lacked any significant voluntary association with the United States. *United States v Gorshkov*, No CR00-550C at 5 (W D Wash May 23, 2001) [on file with U Chi Legal F] (denying the defendant's motion to suppress evidence). The counterargument, of course, is that the

extent that the agreement would contemplate remote cross-border searches by *foreign* officials of data located *in the United States*, the principles of *Reid* and its progeny are less helpful. The question in such a case is not whether actions of U.S. officials taken pursuant to an agreement would violate the Constitution; as relevant, the agreement would not authorize the United States to take action at all. Rather, the agreement would authorize foreign officials to search data physically located in the United States. Absent U.S. involvement, foreign officials would not violate the Constitution by conducting such searches: the Fourth Amendment acts upon U.S., not foreign, officials.[153] It is equally clear that if a foreign official acted jointly with, or on behalf of, U.S. officials in particular searches, standard agency principles might trigger Fourth Amendment requirements.[154] A cross-border

---

Fourth Amendment constrains the actions of officials situated on U.S. territory, even if their actions are directed at a foreign state. Under this theory, the Russian hacking case is distinguishable from *Verdugo* because the U.S. officials were situated in the United States in the former and abroad in the latter.

If U.S. officials seek to search the foreign data of a person with a substantial connection to the United States, pre- and post-*Verdugo* cases in the lower courts suggest that they must comply with the Fourth Amendment, although there is a conflict over whether the Fourth Amendment requires probable cause and a warrant or merely reasonableness in these circumstances. Compare, for example, *Powell v Zuckert*, 366 F2d 634, 640 (DC Cir 1966) (holding that a search of serviceman's home in Japan, conducted by U.S. and Japanese officials pursuant to a Japanese warrant, violated the Fourth Amendment); *Berlin Democratic Club v Rumsfeld*, 410 F Supp 144 (D DC 1976) (holding that the Fourth Amendment warrant requirement applies to wiretapping of U.S. citizens overseas), with *United States v Barona*, 56 F3d 1087, 1092 n 1 (9th Cir 1995) ("Reasonableness, not probable cause, is undoubtedly the touchstone of the Fourth Amendment."); *United States v Juda*, 46 F3d 961, 968 (9th Cir 1995) ("the Fourth Amendment's reasonableness standard applies to United States officials conducting a search affecting a United States citizen in a foreign country"); *United States v Peterson*, 812 F2d 486, 490 (9th Cir 1987) (measuring whether a search was consistent with the Fourth Amendment by consulting foreign law "as part of the determination whether or not the search was reasonable"). Even assuming that the warrant requirement does not generally apply to U.S. searches wholly conducted abroad, the requirement may still apply when officials launch a search from U.S. territory, since such officials are within the supervisory jurisdiction of a court.

In many cases in which U.S. officials seek to search data abroad, officials may be unaware whether the searched individual has a substantial connection to the United States. If so, then the Fourth Amendment in practice is likely to constrain U.S. searches of data physically stored in foreign territory.

153 See *Barona*, 56 F3d at 1091; *United States v Behety*, 32 F3d 503, 510 (11th Cir 1994); *United States v Heller*, 625 F2d 594, 599 (5th Cir 1980); *United States v Morrow*, 537 F2d 120, 139 (5th Cir 1976). Some courts have stated that where the federal government seeks to introduce in federal court evidence obtained by foreign officials without any participation by U.S. officials, the court may exclude the evidence under an exercise of the court's supervisory powers if the foreign officials obtained the evidence in a manner that shocks the conscience. See *Behety*, 32 F3d at 510; *Morrow*, 537 F2d at 139.

154 *Barona*, 56 F3d at 1091–93 ("The second exception to the inapplicability of the [Fourth Amendment's] exclusionary rule [to the acts of foreign officials] applies when

search arrangement, however, would not involve joint U.S.-foreign conduct. Under such an arrangement, U.S. officials would not participate in, approve on a case-by-case basis, or receive the fruits of a foreign search in most cases; rather, the arrangement would simply set forth the circumstances under which the foreign state could conduct a search.

Cases involving agency principles, however, merely constitute a subset of a larger body of case law addressing when conduct undertaken by someone other than a state or federal official is nevertheless "attributable" to the government. That larger body of case law forms the Supreme Court's "state action" doctrine. For our purposes, the relevant question under the state action doctrine is whether the United States's involvement in negotiating or approving a binding instrument permitting foreign searches of U.S. computers is sufficient to make the United States responsible for searches later conducted by foreign law enforcement agents.

It may be thought that the fact that the United States has any role at all in negotiating a cooperative arrangement and approving that arrangement makes the question a simple one: the U.S. involvement is plain, and that is the end of the matter. If so, it would follow that, since the foreign conduct is attributable to the United States, the foreign officials cannot conduct searches that U.S. officials could not conduct. In other words, the United States could not enter into a treaty arrangement contemplating foreign searches on terms lower than those in the Fourth Amendment. Two counterpoints, however, suggest that the matter is not so straightforward. First, a search cannot be "attributable" to the United States unless the United States has actually empowered the foreign state to do something. It is easy to conceive of a treaty similar to the remote cross-border search arrangement contemplated here, but that, rather than granting its

---

'United States agents' participation in the investigation is so substantial that the action is a joint venture between United States and foreign officials.'"); *United States v Maturo*, 982 F2d 57, 61 (2d Cir 1992) (noting that constitutional requirements may attach to evidence obtained in a foreign jurisdiction "where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials"); *Peterson*, 812 F2d at 490 (noting that the Fourth Amendment applies to searches by foreign authorities in their own countries when "United States agents' participation in the investigation is so substantial that the action is a joint venture between United States and foreign officials"); *Heller*, 625 F2d at 599 (noting that "if American officials participated in [a] foreign search or interrogation . . . the [Fourth Amendment's] exclusionary rule should be invoked"); *Morrow*, 537 F2d at 139 (noting that "if American law enforcement officials participated in [a] foreign search . . . the [Fourth Amendment's] exclusionary rule can be invoked").

signatories the power to engage in certain conduct, merely recognizes or even constrains their power. For example, the United States might enter into a bilateral treaty with France stating that each state may, under its own domestic law standards, intercept on its own territory telephone calls between France and the United States. If France would have the power to intercept the call in the absence of the treaty, the treaty has not empowered France to intercept the call, but merely has recognized France's preexisting power to do so. It is difficult to argue that a subsequent French interception would be attributable to the United States merely by virtue of the fact that the United States and France have entered into the treaty.

Second, even if we view the arrangement as authorizing or empowering certain foreign conduct, it is not clear that such action is sufficient to trigger the state action doctrine. The law permits private parties to engage in conduct in which the government could not constitutionally engage; the failure of the government to prevent such conduct is not thought to create constitutional liability.[155] There is no conceptual difference, moreover, between failing to outlaw conduct and lifting an existing ban on such conduct. If the United States were to decriminalize hacking,[156] for example, surely it would not follow that a private individual who gains unauthorized access to a computer system and examines the contents of another person's e-mail violates the Fourth Amendment. The fact that the government lifts a legal barrier to the conduct does not necessarily make the conduct "attributable" to the government for constitutional purposes. It thus could be argued that a cooperative arrangement allowing a foreign state to engage in a search of data located in the United States should not be regarded differently from any other U.S. action that lifts an existing legal barrier to the conduct in question.

To resolve whether U.S. participation in a cooperative arrangement will make foreign conduct under that arrangement attributable to the United States, we must consider two questions. First, how do we conceive of a treaty recognizing certain

---

155 See, for example, *DeShaney v Winnebago County Department of Social Services*, 489 US 189, 196 (1989) (holding that the Due Process Clause places no affirmative duty on states to provide governmental aid, "even where such aid may be necessary to secure life, liberty, or property interests of which the government itself may not deprive the individual").

156 The federal Computer Fraud and Abuse Act currently prohibits various conduct involving intentionally accessing a computer without right. See 18 USC § 1030 (1994 & Supp 1999) (addressing fraud and related activities in connection with computers).

circumstances in which states could conduct searches of data physically located across their borders? When the United States enters an arrangement envisioning that foreign governments will search computers located in the United States, is the United States actually authorizing the foreign search, in the sense of removing legal impediments to the search? Or is it simply recognizing the power that a foreign government already has to conduct that search, since the foreign government is merely launching an investigation from its own territory, without setting foot on U.S. soil? If the treaty merely confirms an existing power of a foreign state, the U.S. should not be responsible for how the foreign state chooses to exercise that power. Second, assuming the United States does remove legal barriers that limit a foreign state's conduct—and thus authorizes the search—is the conduct that follows necessarily attributable to the United States? In other words, could the United States authorize a foreign search of data located in the United States without creating state action? I address these questions in turn.

B. The Significance of a Cooperative Cross-Border Search Arrangement

In evaluating the significance of a cooperative cross-border search arrangement,[157] we can draw upon the principles discussed

---

[157] The approach outlined in the text—of determining the extent to which a cooperative arrangement confers, rather than confirms or constrains, power—is consistent with the approach that the Supreme Court has taken in cases involving status-of-forces agreements (SOFAs) with other countries. In *Wilson v Girard*, 354 US 524 (1957) (per curiam), for example, an agreement between the United States and Japan provided that the United States could exercise jurisdiction over offenses committed in Japan by members of the U.S. armed forces in the performance of their official duties. Id at 526–28. The United States could waive jurisdiction in a particular case. After the United States waived its jurisdiction in Girard's case—thereby permitting Japan to prosecute him—Girard brought a habeas petition claiming that the waiver was unconstitutional, because it would subject an American citizen to trial in a tribunal that did not provide basic constitutional guarantees. The Supreme Court summarily rejected the argument, stating: "A sovereign nation has exclusive jurisdiction to punish offenses against its laws committed within its borders, unless it expressly or impliedly consents to surrender its jurisdiction." Id at 529. The case can be understood as recognizing that Japan's prosecution of Girard was not attributable to the United States for constitutional purposes, despite the fact that it was the U.S. waiver that enabled the prosecution. Rather than granting Japan jurisdiction that it otherwise lacked, the United States merely waived application of an agreement that had *constrained* Japan's jurisdiction.

Similarly, courts have rejected claims that the United States cannot constitutionally turn a defendant over to a foreign country for trial or to serve a sentence if the foreign country does not guarantee basic trial rights. See, for example, *Holmes v Laird*, 459 F2d 1211, 1217–19 (DC Cir 1972) (holding, in a case regarding extradition-like provisions of a SOFA, that the Constitution does not bar serviceman's return to West Germany to serve a

in connection with the international law implications of unilateral cross-border searches. As noted above, if a foreign official physically entered the United States and conducted a search without U.S. permission, his conduct would likely violate international law.[158] Accordingly, we would view an arrangement granting a foreign official such permission as "authorizing" what foreign officials could not otherwise do. We would not view the arrangement as confirming or constraining a power that the foreign officials already possess.

A cross-border search arrangement for computer data presents a slightly more complex problem. If a foreign state's domestic law authorizes a search of data, wherever located, that is accessible from its territory, the state would likely argue that it already possesses the power to conduct the search, and that any treaty setting forth circumstances in which its officials could do so would cabin, not create, that power. The searched country, in contrast, would likely argue that the treaty removes the constraints that its law imposes upon a foreign search. In addition, the searched state might view the arrangement as providing consent for activity that would otherwise interfere with its territorial integrity. Which perspective governs the analysis?

We can answer this question by examining the legal obstacles that a searched state could impose upon a foreign search of data located within its territory.[159] The first obstacle, of course, is

---

sentence for a crime committed in Germany). The court's approach in *Holmes* can be understood as reflecting the principle that although U.S. action, as a practical matter, enables foreign action that does not comport with the Constitution, the extradition agreement with the United States does not itself confer on the foreign country any power to try the defendant that the foreign nation does not already possess. Id at 1216 (noting that even without U.S. action, "West Germany's power to try and convict for those offenses was complete"). Because the power the foreign country exercises does not depend upon the United States's authorization or consent, the foreign country's action is not attributable to the United States for constitutional purposes. See also *Neely v Henkel*, 180 US 109, 122–23 (1901) (examining and rejecting the argument that a statutory provision authorizing extradition to a foreign jurisdiction in the absence of an extradition treaty is void "in that it does not secure to the accused, when surrendered to a foreign country for trial in its tribunals, all of the rights, privileges and immunities that are guaranteed by the Constitution"; concluding that "[w]hen an American citizen commits a crime in a foreign country he cannot complain if required to submit to such modes of trial and to such punishment as the laws of that country may prescribe for its own people . . .").

158 See notes 40–42, 92–93 and accompanying text.

159 In discussing "legal obstacles" to a foreign state's conduct, I am referring to sources of law that would prohibit the conduct, whether or not the prohibition could successfully be enforced against the foreign official. Even if the United States may choose not to prosecute a foreign official for certain conduct or may have difficulty obtaining jurisdiction over such an individual, the possibility of a diplomatic protest remains. In other words, the fact

the norm of customary international law prohibiting a state from conducting investigative activities in the territory of another state. I argued in Part III that this prohibition applies even when officials search data remotely. Domestic law may pose additional obstacles. In the case of the United States, federal and state privacy and anti-hacking statutes,[160] as well as state common law trespass doctrines,[161] would likely prohibit foreign searches of

---

that a prosecution or suit may not be successful does not mean that there are no legal obstacles to foreign conduct.

[160] The federal anti-hacking statute prohibits intentionally accessing without right a computer that is used in interstate or foreign commerce or communication and obtaining information from it, if the conduct involved an interstate or foreign communication. 18 USCA § 1030(a)(2)(C), (e)(2)(B) (2000). The statute also prohibits knowingly or intentionally accessing without right a computer that is used in interstate or foreign commerce if such conduct causes damage. 18 USCA § 1030(a)(5)(B), (C) (2000). In addition, the federal Electronic Communications Privacy Act prohibits intentionally accessing a facility through which an electronic communication service—that is, a service offering users the ability to send or receive communications, 18 USC § 2510(15) (1994)—is provided, and thereby obtaining access to an electronic communication in storage with such service. 18 USC § 2701(a)(1) (1994).

All fifty states have adopted some form of computer crime statute. Ala Code § 13A-8-100–13A-8-103 (1994); Alaska Stat § 11.46.484(a)(5), 11.46.740 (Lexis 2000); Ariz Rev Stat Ann § 13-2316.01–13-2316.02 (West 2001); Ark Code Ann § 5-41-101–5-41-108 (Michie 1997); Cal Penal Code § 502 (West 1999); Colo Rev Stat Ann § 18-5.5-101–18-5.5-102 (West Supp 2000); Conn Gen Stat Ann § 53a-250–53a-261 (West 1994 & Supp 2001); 11 Del Code Ann §§ 931-39 (1995 & Supp 2000); Fla Stat Ann § 815.01–815.07 (West 2000); Ga Code Ann § 16-9-90–16-9-94 (Michie 1999); Hawaii Rev Stat Ann § 708-890–708-893 (Michie 1993); Idaho Code § 18-2201–18-2202 (1997); 720 ILCS 5/16D-1–5/16D-7 (West 1998 & Supp 1999); Ind Code § 35-43-1-4 (1998); Iowa Code Ann §§ 714.1(8), 716.6B (West Supp 2001); Kan Stat Ann § 21-3755 (1995 & Supp 2000); Ky Rev Stat Ann § 434.840–434.860 (Michie 2000); La Rev Stat Ann § 14:73.1–14:73.5 (West 1997); 17-A Me Rev Stat Ann §§ 431–33 (West Supp 2000); Md Ann Code Art 27, § 146 (1996 & Supp 2000); Mass Ann Laws ch 266, § 120F (Law Co-op Supp 2000); Mich Comp Laws Ann § 752.791–752.797 (West 1991 & Supp 2000); Minn Stat Ann § 609.87–609.893 (West Supp 2001); Miss Code Ann § 97-45-1–97-45-13 (1999); Mo Ann Stat § 556.063, 569.099 (West 1999 & Supp 2001); Mont Code Ann § 45-6-310–45-6-311 (1997); Neb Rev Stat § 28-1341–28-1348 (1995); Nev Rev Stat § 205.473–205.497 (1997); NH Rev Stat Ann § 638:16–638:19 (1996); NJ Stat Ann § 2C:20-23–2C:20-34 (West 1995); NM Stat Ann § 30-45-1–30-45-7 (Michie 1997); NY Penal Law § 156.00–156.50 (McKinney 1999); NC Gen Stat Ann § 14-453–14-458 (Michie 1999); ND Cent Code § 12.1-06.1-08 (1997); Ohio Rev Code Ann § 2913.04 (West 1999); 21 Okla Stat §§ 1951–58 (Supp 2001); Or Rev Stat § 164.377 (1999); 18 Pa Cons Stat Ann § 3933 (West Supp 2000); RI Gen Laws § 11-52-1–11-52-8 (2000); SC Code Ann § 16-16-10–16-16-40 (Law Co-op 1987 & West Supp 2000); SD Cod Laws § 43-43B-1–43-43B-8 (Michie 1997); Tenn Code Ann § 39-14-601–39-14-603 (1997); Tex Penal Code Ann § 33.01–33.04 (West 1994 & Supp 2001); Utah Code Ann § 76-6-701–76-6-705 (1999); 13 Vt Stat Ann § 4101–07 (Supp 2000); Va Code Ann § 18.2-152.1–18.2-152.15 (Michie 1996 & Supp 2000); Wash Rev Code Ann § 9A.52.110–9A.52.130 (West 2000); W Va Code Ann § 61-3C-1–61-3C-21 (Michie 2000); Wis Stat Ann § 943.70 (West 1996 & Supp 2000); Wyo Stat Ann § 6-3-501–6-3-505 (Michie 1999). Although the provisions differ widely, most states prohibit unauthorized access to a computer system.

[161] For state law cases suggesting that unauthorized access to a computer system constitutes a trespass, see *Thrifty-Tel Inc v Bezenek*, 54 Cal Rptr 2d 468, 473 (App 1996) (holding that unauthorized use of confidential codes to gain computer access is sufficient

data located in the United States. So long as these obstacles to the foreign search are valid ones, the fact that a cooperative arrangement would remove these obstacles suggests that the arrangement would expand, rather than affirm, a foreign state's power to conduct the search.

Are the legal obstacles that U.S. and state law might impose upon a foreign search of data valid as against a foreign state's competing claim that it has a strong interest in accessing the data? Our previous discussion of the competing conceptions of territorial sovereignty sheds some light on this question.

The analysis of the Johnson and Post and Goldsmith positions in connection with the discussion of unilateral cross-border searches suggests that such obstacles would be valid at least as against private conduct launched from another state. Although Johnson and Post generally oppose territorially based regulation of online activities, their position has the most force when the activities in question involve making particular content available without intending that it reach a state where it would be deemed harmful. When activity is directed at one or many states and intended to cause harm there, the objections to territorially based regulation are less powerful. There is nothing illegitimate, for example, about applying a statute outlawing hacking when the conduct originates from outside of the state's territory. And from Goldsmith's perspective, the effects principle unquestionably permits a state to protect data within its territory, even when the harm originates from outside of its territory.

If these obstacles are valid as against private foreign conduct, are they also valid as against official foreign conduct? The discussion of unilateral cross-border search claims in Part III suggests that they are. Analyzing unilateral cross-border search claims yields a concept of territorial sovereignty that is not so narrow as to prevent a state from protecting privacy or property interests in data stored in its territory, and not so broad as to permit a state to intentionally interfere with those protections as an incident to its power to regulate.[162]

---

to constitute trespass); *State v McGraw*, 480 NE2d 552, 554 (Ind 1985) (dictum). At least two federal district courts have also held that interference with a computer system can constitute a state law trespass. See *eBay v Bidder's Edge*, 100 F Supp 2d 1058, 1069–72 (N D Cal 2000) (finding likelihood of success on the merits of a claim that competitor's use of automated software to gather data from plaintiff's web site constituted a trespass to chattels); *CompuServe Inc v Cyber Promotions, Inc*, 962 F Supp 1015, 1020–24 (S D Ohio 1997) (holding that repeated transmission of unsolicited commercial electronic mail through an internet service provider's system constitutes a trespass under Ohio law).

[162] See text accompanying notes 125–46.

If we accept that the individual states and the United States have the power to create and protect property rights in electronic data, through criminal or civil means, based on the data's location, the significance of a cooperative arrangement permitting searches of such data becomes clear. It is proper to look at a treaty as one that "authorizes" or "empowers" a foreign state to affect U.S. persons or property in a certain way.

C. The Significance of Authorization under the State Action Doctrine

I have argued that a treaty contemplating foreign remote cross-border searches is properly viewed as removing certain legal obstacles validly imposed by the federal or state governments. The question, then, is under what circumstances does removing legal obstacles to foreign conduct make the conduct now authorized or permitted attributable to the government for constitutional purposes? Answering this question requires us to delve more deeply into the Supreme Court's state action doctrine—one of the most complex and, some would argue, problematic areas of constitutional law.[163] In particular, many critics claim that the

---

[163] See, for example, Charles L. Black, Jr., *The Supreme Court, 1966 Term—Foreword: "State Action," Equal Protection, and California's Proposition 14*, 81 Harv L Rev 69, 95 (1967) (describing the state action doctrine as a "conceptual disaster area"); Lawrence A. Alexander, *Cutting the Gordian Knot: State Action and Self-Help Repossession*, 2 Hastings Const L Q 893, 894–96, 906, 934 (1975); Erwin Chemerinsky, *Rethinking State Action*, 80 Nw U L Rev 503, 505 (1985) (noting that scholars for twenty years argued that the state action doctrine "never could be rationally or consistently applied"); Jesse H. Choper, *Thoughts on State Action: The "Government Function" and "Power Theory" Approaches*, 1979 Wash U L Q 757, 757 (1979) (commenting on how the state action doctrine "continues to confound both courts and commentators"); Robert J. Glennon, Jr. and John E. Nowak, *A Functional Analysis of the Fourteenth Amendment "State Action" Requirement*, 1976 S Ct Rev 221, 221 (noting the difficulties in defining state action because of the lack of "generally accepted formulas for determining when a sufficient amount of government action is present in a practice to justify subjecting it to constitutional restraints"); Alan R. Madry, *Private Accountability and the Fourteenth Amendment: State Action, Federalism and Congress*, 59 Mo L Rev 499, 500 (1994) (arguing that the problem with the state action doctrine is that "[i]t reflects a profound ignorance of the workings of federalism and the origins and concerns of the Fourteenth Amendment"); William P. Marshall, *Diluting Constitutional Rights: Rethinking "Rethinking State Action"*, 80 Nw U L Rev 558, 570 (1985) (stating that the current interpretation of the state action doctrine can only be defended through "intellectual dishonesty"); Cass R. Sunstein, *Lochner's Legacy*, 87 Colum L Rev 873, 888 (1987) (noting apparently incoherent Supreme Court state action rulings and arguing that "the search for state action can be made coherent only against a background normative theory of the legitimate or normal activities of government. Without such a theory, the search is unguided"). But see Laurence H. Tribe, *Constitutional Choices* 248 (Harvard 1985) ("The conventional wisdom on this subject—that the 'doctrine' of state action is too deeply incoherent and internally conflicted to be taken seriously—seems to me flatly wrong and, if anything, obstructive of serious critical efforts.").

Supreme Court's state action doctrine is incoherent.[164] Much of the claimed incoherence is attributable to the development of the doctrine in cases involving race discrimination.[165] The Court loosened the doctrine from the 1940s through the 1960s, so as to combat acts of discrimination that, though committed by private parties, were essentially supported or even required by the States.[166] The looser interpretation of the state action requirement also prevented government actors from evading constitutional limits on their conduct by transferring certain functions to private parties.[167] More recently, outside of the racial context, the

---

[164] See Chemerinsky, 80 Nw U L Rev at 504–05 (cited in note 163) (commenting on how scholars have shown the "incoherence" of the state action problem); Black, 81 Harv L Rev at 95 (cited in note 163) ("conceptual disaster area"); Choper, 1979 Wash U L Q at 757 (cited in note 163) (noting the "confounding" nature of the state action doctrine).

[165] See Glennon and Nowak, 1976 S Ct Rev at 222–24 (cited in note 163) (arguing that racial discrimination cases sounded "[t]he death knell for formal state action theories").

[166] See, for example, *Evans v Newton*, 382 US 296, 301–02 (1966) (holding that where a city's maintenance of land as a trustee was an integral part of its activities, the land became a public facility and could not be operated on a segregated basis even when control of it passed into private hands); *Burton v Wilmington Parking Authority*, 365 US 715, 725 (1961) (holding that exclusion of a black restaurant patron violated the Equal Protection Clause, where a state agency leased space in a publicly owned and financed building to the restaurant owner); *Terry v Adams*, 345 US 461, 469–70 (1953) (plurality opinion) (finding that a private political organization's exclusion of blacks from its primaries violated the Fifteenth Amendment where, in practice, the outcome of the organization's election always determined the outcome of the county's Democratic primary); *Shelley v Kraemer*, 334 US 1, 20 (1948) (holding that a state's judicial enforcement of a racially restrictive covenant violated the Equal Protection Clause). For discussions of the racial context in which the state action doctrine developed, see, for example, David A. Strauss, *State Action After the Civil Rights Era*, 10 Const Commen 409, 411–14 (1993) (discussing the state action doctrine in the civil rights era); Madry, 59 Mo L Rev at 507–10 (cited in note 163) (considering the development of the state action doctrine in cases where blacks were excluded from voting in Democratic primaries and subsequent findings of state action in private conduct); Choper, 1979 Wash U L Q at 758–59 (cited in note 163) (commenting that until the Civil Rights Act of 1964, most litigation over the state action doctrine dealt with private racial discrimination).

[167] The loosening of the state action requirement in cases where the Court perceives the government to be attempting to evade constitutional strictures by shifting functions to private parties is well illustrated by the Court's response to Texas's attempts to exclude blacks from primary elections. After the Supreme Court struck down an outright prohibition on blacks' participation in Democratic party primary elections in Texas, see *Nixon v Herndon*, 273 US 536 (1927), the state passed a law permitting political parties, through their executive committees, to decide who would be permitted to vote in party elections. In a challenge to the Texas Democratic Party's decision to exclude black voters from a primary, the Court found state action on the ground that the state statute had vested power in the executive committee that the committee did not otherwise possess under state law, making party executive committees "organs of the State itself, the repositories of official power." *Nixon v Condon*, 286 US 73, 88 (1932). The state then transferred all questions of party political membership to the parties themselves; the Texas Democratic Party limited its membership—and thus the participants in its primaries—to white citizens. The Court again found state action, in view of the extensive regulatory structure governing the primary process in Texas. *Smith v Allwright*, 321 US 649, 663–64 (1944). See also *Terry*, 345

Supreme Court has strictly defined what qualifies as governmental conduct for constitutional purposes.[168] Even taking these doctrinal shifts into account, some critics advocate that the Court adopt a broader conception of what qualifies as government action;[169] and some even advocate that the Supreme Court jettison the doctrine altogether.[170] I do not attempt to enter this debate here. As I illustrate below, even under the Supreme Court's strict application of the state action doctrine, there is a powerful argument that U.S. participation in an arrangement effectively "authorizing" searches by foreign officials affecting data located in the United States makes those searches attributable to the United States for constitutional purposes.

Modern state action cases essentially acknowledge a unitary, but highly fact-specific, model of state action, as set forth in *Lugar v Edmonson Oil Co.*[171] That model first requires a showing of a constitutional deprivation "caused by the exercise of some right or privilege created by the State or by a rule of conduct imposed by the State or by a person for whom the State is responsible."[172] Where the government authorizes particular conduct by statute or treaty, this first part of the Court's model is satisfied. Second, the third party claimed to have given rise to the depriva-

---

US at 469–70 (holding that even without state control, a private organization's primaries could satisfy the state action requirement when they were "an integral part . . . of the elective process that determines who shall rule and govern").

168 See, for example, *American Manufacturers Mutual Insurance Co v Sullivan*, 526 US 40, 49–58 (1999) (rejecting an argument that a private insurer is a state actor when it withholds payment for disputed medical expenses, as permitted under state law); *Blum v Yaretsky*, 457 US 991, 1002–12 (1982) (rejecting a claim that involuntary discharge or transfer of nursing home patients violates the Due Process Clause; holding that nursing homes' decisions do not constitute state action merely because the state regulates them); *Rendell-Baker v Kohn*, 457 US 830, 837–43 (1982) (holding that state is not responsible for a private school's discharge of a teacher); *Jackson v Metropolitan Edison Co*, 419 US 345, 351–59 (1974) (rejecting the claim that privately owned and operated utility is a state actor and that termination of service without notice and an opportunity to be heard violated the Due Process Clause).

169 See, for example, Larry Alexander, *The Public/Private Distinction and Constitutional Limits on Private Power*, 10 Const Commen 361, 371–77 (1993) (advocating the adoption of a three-step analysis of private actions by comparing them to analogous state actions in order to determine whether or not they are constitutional).

170 See, for example, Chemerinsky, 80 Nw U L Rev at 506 (cited in note 163) (arguing that "limiting the Constitution's protections of individual rights to state action is anachronistic, harmful to the most important personal liberties, completely unnecessary, and even detrimental to the very goals that it originally intended to accomplish"). But see Richard S. Kay, *The State Action Doctrine, The Public-Private Distinction, and the Independence of Constitutional Law*, 10 Const Commen 329, 337–41 (1993) (defending the state action doctrine as preserving the distinction between constitutional law and ordinary law).

171 457 US 922 (1982).

172 Id at 937.

tion "must be a person who may fairly be said to be a state actor."[173] Where the party responsible for the deprivation is not a state or federal official, a showing that the conduct is chargeable to the government can be made in one of two ways: by demonstrating that the nongovernmental actor is essentially supplanting the state in the performance of a public function that traditionally has been exclusively reserved to the sovereign;[174] or by demonstrating particular facts and circumstances that give rise to the conclusion that the government has jointly participated in[175] or compelled[176] the conduct in question.

It might be thought that conducting a search for law enforcement purposes is clearly a function traditionally reserved to the sovereign, and that U.S. involvement in a treaty arrangement under which such a search would occur makes the search attributable to the state. Under the Court's doctrine, however, the public function exception is extremely narrow: it applies only to circumstances in which a private party supplants the government in performing a function that is "traditionally the exclusive prerogative of the State."[177] That foreign conduct under a cross-border search arrangement would not supplant U.S. conduct is clear; the United States would not even receive the results of the tests in most cases. Nor, in light of the existence of private detectives, would the investigative function likely be found exclusive under the Court's doctrine.

We turn, then, to the second method of demonstrating that conduct is chargeable to the government: by showing circumstances that give rise to the conclusion that the government has participated in or compelled the conduct in question. Although this requirement from *Lugar* might suggest that an arrangement

---

173 Id.

174 Id at 938. For cases discussing and applying the public function test, see *Jackson*, 419 US 345 (discussing whether furnishing utility services is a public function); *Terry*, 345 US 461 (considering whether elections are a public function); *Marsh v Alabama*, 326 US 501 (1946) (examining whether a town operated and owned by a private corporation qualified as a public function).

175 *Lugar*, 457 US at 937, 941.

176 See *Blum*, 457 US at 1004 ("[A] State normally can be held responsible for a private decision only when it has exercised coercive power or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the State."); *Adickes v S.H. Kress & Co*, 398 US 144, 170 (1970) (holding the state responsible for discriminatory acts of private parties when the State, by law, compelled the act).

177 *Jackson*, 419 US at 353. Compare *Rendell-Baker*, 457 US at 842 (holding that providing education is not traditionally an exclusive public function), with *Terry*, 345 US at 469–70 (conducting elections is a public function); *Marsh*, 326 US at 507 (finding state action where a private company performed all municipal functions in a town).

under which the United States authorizes searches of computers within U.S. territory (without directly participating in or compelling the searches) will not give rise to a finding of state action, the underlying case law is actually more nuanced. By way of illustration, it is useful to examine two cases in which the Court has considered claims that the government's "authorization" of certain conduct makes the conduct attributable to the United States.

The first is one of the cases on which *Lugar* relied for its synthesis of the state action doctrine.[178] *Flagg Brothers v Brooks*[179] involved the claims of two property owners who had placed certain goods with a storage company. A New York self-help statute authorized storage companies to sell goods when a property owner failed to pay a fee.[180] The statute did not require the company to provide property owners with an opportunity to be heard prior to the sale of the property.[181] Although the Court did not address the matter,[182] we can assume that if the state itself had custody of the goods, it could not sell them in the manner the statute permitted: if it did, it would violate the Due Process Clause. When a dispute arose over the payment of fees and the storage company threatened to sell the goods, the property owners sued, claiming that the private storage company's threatened sale violated the Due Process Clause of the Fourteenth Amendment.[183] Although the state would not be involved in the sale, the property owners argued, among other things, that the state was nevertheless responsible for the sale, because it had passed a statute "authorizing" the private conduct.[184] Without the authorizing statute, the storage company could not have sold the goods without the risk that the property owners would sue the

---

178 457 US at 938–39.

179 436 US 149 (1978). For commentary on *Flagg Brothers*, see Thomas D. Rowe Jr., *The Emerging Threshold Approach to State Action Determinations: Trying to Make Sense of* Flagg Brothers, Inc. v. Brooks, 69 Georgetown L J 745, 759–62 (1981) (arguing that the *Flagg Brothers* state action doctrine makes sense if limited to nonordinary cases and if the compulsion criterion is only a possible route to finding state action rather than a requirement); Paul Brest, *State Action and Liberal Theory: A Casenote on* Flagg Brothers v. Brooks, 130 U Pa L Rev 1296 (1982) (critiquing the Court's state action doctrine and how it addresses concerns over preventing abuses of power and protecting individual autonomy).

180 *Flagg Brothers*, 436 US at 151 n 1.

181 Id.

182 Id at 155 n 4.

183 The property owners also claimed that the sale would violate the Equal Protection Clause of the Fourteenth Amendment. Id at 153.

184 *Flagg Brothers*, 436 US at 164.

storage company under a conversion theory; the statute essentially immunized the storage company from such a claim. Since the storage company could not have sold the property without fear that its actions would later be found to violate the law, the property owners claimed that the statutory authorization was sufficient to make the sale attributable to the State.[185]

The Court rejected the property owners' claim, concluding that authorization of private conduct, without more, does not make the subsequent private conduct attributable to the government.[186] Although the statute in question adjusted traditional rules governing property arrangements, announcing circumstances in which New York courts would not interfere with private conduct, the statute still left to the storage company the choice whether to avail itself of the statutory self-help remedy.[187] The government, the Court reasoned, could not be held responsible for the choice.[188]

At first glance, it would seem that *Flagg Brothers* decisively settles the question under consideration here—whether government action "authorizing" certain conduct, in the sense of removing legal barriers that would otherwise deter someone from engaging in it, makes the conduct attributable to the government. Based on *Flagg Brothers*, one would conclude that the government is free to permit whatever conduct it chooses; it is only responsible for conduct it compels.

A second case involving government authorization of private conduct, however, complicates the matter. In *Skinner v Railway Labor Executives' Association*,[189] the Court considered a constitutional challenge to federal regulations authorizing private railroad companies to require their employees to submit to blood or urine tests under certain circumstances.[190] The regulations preempted any state law provisions and collective bargaining agreements that would have barred the testing.[191] Under the regulations, the Federal Railroad Administration would have the right to receive test results if the private company performed the test.[192] Employees claimed that the regulations needed to be scru-

---

185 Id at 156.

186 Id at 164–65.

187 Id at 165.

188 See *Flagg Brothers*, 436 US at 165.

189 489 US 602 (1989).

190 Id at 611–12. Some of the federal regulations made testing mandatory. I am concerned here only with the permissive regulations.

191 Id at 615.

192 Id.

tinized under the Fourth Amendment, because tests the railroad would conduct under the regulations were attributable to the state.[193]

The Court agreed with the employees that there was state action.[194] On the surface, it appears that the Court, testing for state participation or compulsion, found more than mere "authorization" of the private railroads' conduct.[195] The Court classified the government's action as "encouragement" of, "endorsement" of, and "participation" in the conduct.[196] The finding of encouragement, endorsement, and participation, however, was based principally—if not solely—on two factors: the fact that the regulations preempted contrary state law and collective bargaining provisions and the fact that the federal government could receive test results if it chose.[197] As to the first factor, preemption of contrary state law and collective bargaining agreements is nothing more than "authorization."[198] Although the result is accomplished by the federal government, rather than a state, a federal regulation with preemptive force is no different from a state law clarifying a legal regime to indicate what conduct is permissible. As to the second factor, it is difficult to see how the possibility that the government may receive a result of a test that may (or may not) occur influences one way or the other the railroad company's decision whether to conduct the test. The decision to perform a test in a specific case—or even to formulate company guidelines under which such tests will be performed—remains a private choice.

Flagg Brothers and *Skinner*, thus, seem to compel precisely opposite conclusions with respect to the question whether government authorization of private conduct makes that conduct attributable to the government. *Flagg Brothers* states that mere authorization is insufficient;[199] *Skinner* purports to find "participation" and "encouragement" in questionable circumstances, when the government conduct looks much like mere authorization.[200] Upon closer analysis, however, there is a plausible basis upon which the cases can be reconciled, one that would place an

---

193 See *Skinner*, 489 US at 612–13.
194 See id at 614–16.
195 See id at 615–16.
196 Id.
197 See *Skinner*, 489 US at 615.
198 Id.
199 436 US at 164.
200 489 US at 615–16.

arrangement governing cross-border searches by foreign officials on the *Skinner* side of the state action line.

The *Lugar* test—implicitly followed in *Skinner* and carried forward in more recent cases—oversimplifies the state action model with respect to authorization-type cases. In attempting to draw a clear line between "authorization" on the one hand and "participation" or "compulsion" on the other, the *Lugar* test fails to capture the distinction between two different kinds of authorization cases. The distinction is well illustrated by *Flagg Brothers* and *Skinner* themselves.

The Supreme Court's instinct in *Flagg Brothers* is that, when the state merely adjusts common law property or tort rules, any private conduct that follows is not attributable to the state.[201] The new rule may give parties certainty about their rights; it may shift an immunity from one party to another; or it may establish a default rule around which the parties can contract. Although the policy underlying the statute may reflect an accommodation of or choice between conflicting interests, any benefit that flows to the state—for example, having fewer disputes in its courts—is quite attenuated. In other words, to the extent that the state itself is in a better position than if it had merely left the common law regime intact, any benefit the state receives bears only a distant relationship to the underlying policy choice the state made. The new rule may change the position of the parties with respect to one another, but the state's posture is essentially "neutral," in the sense that no power or benefit flows directly to the state from the state's choice of policy.

---

[201] See, for example, *Flagg Brothers*, 436 US at 160–61, 161 n 9, 165–66 (holding that resolving disputes between debtors and creditors is not traditionally an exclusive state function and commenting that the state's statutory refusal to act is no different than a statute of limitations, saying that the state will not provide a remedy after a given period of time). The Court's instinct is consistent with a conceptual point scholars frequently make in discussing the Court's state action doctrine—that all private action takes place against the backdrop of state "permission," see Alexander, 10 Const Commen at 362–63 (cited in note 169)—and is also consistent with some scholars' normative view that this fact alone cannot make the private conduct attributable to the government. See, for example, Harry H. Wellington, *The Constitution, The Labor Union, and "Governmental Action,"* 70 Yale L J 345, 356–57 (1961) (arguing that federal preemption of state regulations cannot be the sole basis for finding state action; otherwise "all private action taken under the authority of federal legislation that occupies a field by that token alone becomes governmental action," requiring the government to outlaw private behavior in which the government could not itself constitutionally engage); Kenneth L. Karst and Harold W. Horowitz, Reitman v. Mulkey: *A Telophase of Substantive Equal Protection*, 1967 S Ct Rev 39, 52 ("[I]t would be foolish to say that the state has unconstitutionally become a partner in . . . private practices [merely] because it permits them . . . .").

In a case like *Skinner*, the situation is quite different. The regulations authorizing blood and urine testing by railroad companies preempted contrary state law and collective bargaining agreements.[202] This fact alone may not be significant: as in *Flagg Brothers*, the regulations authorizing railroad testing, without more, might simply reflect a choice between various policy interests (in promoting railroad safety or protecting employee privacy, for example). But there is more at work here. The government has the right to receive the test results when a railroad company performs the test.[203] Although it is not correct to say that the government "participates" in the underlying private conduct, or that it compels or even encourages the test, the government has still done something significant. It has chosen between conflicting policy interests, just as the state government did in *Flagg Brothers*. But in the course of doing so, it has bargained for an important and direct benefit—the right to the results of the tests. Unlike in *Flagg Brothers*, we cannot view the government as "neutral" in making its policy choice.

This analysis suggests a more nuanced view of the significance of "authorization" under the state action doctrine. When the government authorizes certain conduct—whether private conduct or that of foreign officials—it cannot always be assumed that there is no state action, on the theory that the government is simply adjusting background permissions and prohibitions on the underlying conduct. State action may be present even where a typical agency relationship is lacking in a particular case. Recognizing that there are certain core functions that the government performs—among them, investigation and prosecution—it is possible to distinguish between an "authorization" like that in *Flagg Brothers*, where the government merely adjusts rules affecting private individuals, and an "authorization" like that in *Skinner*, where the government adjusts those rules but gives itself a benefit or power, in connection with particular public functions it performs, in the process. Outside of the agency context, where the government achieves a benefit or increases its power in exchange for authorizing conduct—be it private or that of a foreign sovereign—that conduct is attributable to the government. The government is in no sense neutral in the policy choice it makes.

This is precisely what happens when the government negotiates with another sovereign and, as part of the bargain struck,

---

202 See *Skinner*, 489 US at 615.

203 See id.

selectively removes legal obstacles that would otherwise bar that state from affecting property or persons that federal or state law protects. A treaty permitting remote cross-border searches would have three important effects: it would remove any diplomatic objection the United States might have against foreign law enforcement activity conducted within its borders; it would displace the federal and state anti-hacking and privacy statutes; and it would preempt state law, such as trespass doctrines, that might otherwise protect the data in question. It would do so in exchange for a very important benefit: the United States' reciprocal power to search communications located in foreign countries. When the U.S. bargains for its own right to conduct remote searches abroad, and essentially exchanges existing legal protections of U.S. property and persons for that right, the foreign conduct that follows is attributable to the United States for constitutional purposes. Under this theory, it would not matter that the United States does not compel or participate in a foreign search in a particular instance.

As this discussion suggests, although a consent-based regime governing remote cross-border searches might resolve problems of international law, it has the potential to create problems under domestic law. Under state action principles, foreign conduct authorized by an international agreement will be attributable to the United States. To the extent that the United States seeks to participate in consensual cross-border search arrangements, then, it must take into account the limitations that the Fourth Amendment imposes upon government conduct.[204]

---

[204] It is beyond the scope of this Article to consider in detail what limitations the Fourth Amendment would impose on foreign officials by virtue of U.S. involvement in empowering searches of data in the United States. Generally speaking, when a state action analysis makes conduct attributable to U.S. officials, that conduct is subject to the same limitations that would apply if U.S. officials engaged in it. The constitutional requirements for a search or seizure by U.S. officials of data protected by the Fourth Amendment are highly fact dependent. At a minimum, if a person has a reasonable expectation of privacy in the data, U.S. officials could search that data, in the absence of any exigent circumstances, only with a warrant issued by a neutral and detached magistrate based on probable cause to believe that the data reflects evidence of a crime. See, for example, *Berger v New York*, 388 US 41, 54–55 (1967) (measuring a state eavesdropping statute against Fourth Amendment requirements). As previously noted, if officials believe that data might otherwise be lost, the Fourth Amendment might permit them to freeze the data, so long as they still have individual suspicion rising to the level of probable cause. See note 91.

One of the major problems in applying Fourth Amendment requirements to searches by foreign officials is determining whether the warrant requirement applies. As previously discussed, in some cases in which searches occurring abroad are attributable to U.S. officials, courts have applied only the Fourth Amendment's reasonableness require-

CONCLUSION

As computer crime becomes more widespread, states will increasingly face difficulties in retrieving evidence stored in electronic form. Potential solutions to these difficulties present complicated legal issues, requiring us to address how the rise of online activities cutting across international borders affects state power to protect data stored within its territory.

In developing a legal framework for evaluating these issues, we have drawn upon the two sides of an important scholarly debate about whether states can and should regulate online activities. Analyzing cross-border search claims in light of the poles in this debate helps to refine our understanding of how concepts of territorial sovereignty apply in the internet context. This analysis, I have argued, points away from a broad conclusion that territorially-based regulation of internet activities is always problematic. Likewise, it points away from the conclusion that even if it is permissible to apply territorially based privacy or property protections against private conduct, such regulations are no barrier to the conduct of a foreign state that seeks to advance its own regulatory interests.

To the extent that states seek to claim a unilateral power to conduct cross-border searches, such claims may be problematic under international law. There are strong arguments that the customary international law prohibition on performing law enforcement functions in the territory of another sovereign applies even when law enforcement officials do not enter the territory of another state. This 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. In addition, because the customary international law prohibition on conducting law enforcement functions arguably does not apply when a nation acts in self-defense,[205] there may be extreme circumstances in which a cross-border search is permissible despite the breach of sovereignty. To take one example, a cross-border search or other enforcement action might be permissible—and, indeed, appropri-

---

ment. See note 152. Those situations are slightly different from the cross-border search situation, because the foreign officials and the searched property are both located abroad. When a foreign official conducts a cross-border search, the data is located in the United States. As in the reverse situation, when a U.S. official conducts a cross-border search, it is difficult to assign an exclusive location to the search. Id.

[205] See note 41.

ate—if foreign computers were being used in a state-sponsored or terrorist attack that threatened the nation's communications infrastructure.

To the extent that states seek to adopt multilateral and bilateral arrangements setting forth circumstances under which states can conduct cross-border searches, domestic law may impose some limitations. In the case of the United States, I argued, the Constitution limits government officials from permitting foreign searches on terms lower than those the Fourth Amendment requires in exchange for a U.S. power to conduct searches abroad. Customary international law and domestic law impose valid legal obstacles on foreign cross-border searches, and the removal of those legal obstacles should make the subsequent foreign conduct attributable to the United States. This is not to say that the requirements of the Fourth Amendment would apply to every foreign search conducted under such a treaty, regardless of whether the person whose privacy interest was affected has any substantial connection to the United States. Nor am I suggesting that the U.S. could not develop principles consistent with the Fourth Amendment under which cross-border searches could occur. I have simply argued that the U.S. needs to take Fourth Amendment principles into account in formulating its policies.