UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 14
Issue 1 *Fall 2012*

Article 4

10-1-2012

Law, Dissonance, and Remote Computer Searches

Susan W. Brenner

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 14, ISSUE 1: FALL 2012

LAW, DISSONANCE, AND REMOTE COMPUTER SEARCHES

Susan W. Brenner*

This Article examines the conflict—the dissonance—that arises when law enforcement officers from one jurisdiction remotely search a computer that is physically located in another jurisdiction. It reviews the current status of remote computer searches in Europe, noting that such searches are legal under United Kingdom law but are, for most purposes, outlawed by German law. The Article then explains that, because U.S. state supreme courts have used their constitutions to impose search and seizure requirements that exceed those of the Fourth Amendment, similar dissonance has arisen between U.S. states. It uses this domestic dissonance to analyze the issues transnational searches are likely to create and to consider how those issues might be resolved.

I. INTRODUCTION

As authorities in Europe, the United States, and elsewhere have recognized for well over a decade,[1] cyberspace alters the process of law enforcement's searching for evidence of criminal activity in a very fundamental way: Crime ceases to be territorial as borders become irrelevant, which is advantageous for law-breakers and disadvantageous for law enforcers.[2]

---

* NCR Distinguished Professor of Law & Technology, University of Dayton School of Law, Dayton, Ohio USA.

[1] *See* COUNCIL OF EUROPE, EXPLANATORY REPORT TO THE EUROPEAN CONVENTION ON CYBERCRIME (ETS NO. 185) ¶¶ 131–37 (2001), *available at* http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm; HOLLIS STAMBAUGH ET AL., NAT'L INST. OF JUSTICE, STATE AND LOCAL LAW ENFORCEMENT NEEDS TO COMBAT ELECTRONIC CRIME 3–4 (2000).

[2] *See* COUNCIL OF EUROPE, *supra* note 1, at ¶¶ 131–34; *see also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1, 31–65 (2004).

A case from Kentucky illustrates this. In 2009, cybercriminals operating from outside the United States surreptitiously extracted $415,989 from an account at the First Federal Savings Bank in Shepherdsville, Kentucky.[3] The account belonged to Bullitt County and held funds the county used to pay its employees.[4]

On June 22, 2009, "someone started making unauthorized wire transfers of $10,000 or less from the county's payroll to accounts . . . around the country."[5] It was not until June 29 that bank employees "realized something was wrong," but by that time the money was gone.[6] Because no one in Bullitt County had any idea who was responsible for the transfers, county officials contacted the Federal Bureau of Investigation, which began investigating.[7]

The investigation showed the transfers originated in Ukraine.[8] The criminals used a Trojan Horse program "known as 'Zeus' " to harvest the county's funds.[9] They "somehow" installed the program on the county treasurer's computer.[10] Zeus "creates a direct connection" between the infected computer (the treasurer's computer) and the system used by the cybercriminals; this let them "log in to the victim's bank account using the victim's own [computer and] Internet connection . . . ."[11]

---

[3] The account of the crime is taken from the following sources: *$415,989 Taken from Bullitt Bank Account*, COURIER-JOURNAL, July 1, 2009, *available at* 2009 WLNR 15630449; Kelly House, *$415,989 Taken from Bullitt Bank Account*, COURIER-JOURNAL, July 2, 2009, at A1, *available at* 2009 WLNR 15629810; Brian Krebs, *PC Invader Costs Ky. County $415,000*, WASH. POST (July 2, 2009), http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html.

[4] *See, e.g.*, *Theft Used Stealthy Computer Code*, COURIER-JOURNAL, July 27, 2009, *available at* 2009 WLNR 15691911.

[5] Krebs, *supra* note 3.

[6] *Id.*

[7] *See, e.g.*, *Hackers Stole $415,000 from Bullitt County Coffers*, SPAMFIGHTER (July 21, 2009), http://www.spamfighter.com/News-12758-Hackers-Stole-$415000-from-Bullitt-County-Coffers.htm.

[8] *See, e.g.*, Krebs, *supra* note 3.

[9] *Id.*

[10] *Id.*

[11] *Id.*

The cyberthieves then used the Zeus Trojan to acquire the county treasurer's username and password and link her computer with the one they would use in the thefts.[12] Then they "logged into the county's bank account by tunneling through the treasurer's Internet connection."[13] Since they were using her Internet connection, the bank's system did not flag this as a problematic attempt to log into the account.[14] The thieves "created several fictitious employees of the county" and initiated "a batch of wire transfers" to them, extracting more than $400,000 from the county's account.[15] The cybercriminals arranged for U.S.-based intermediaries to wire most of the funds to accounts in Ukraine, at which point they disappeared.[16] The criminals who created and implemented the theft have not been, and most certainly will not be, apprehended and punished for their crimes.[17]

Unlike their traditional counterparts, cybercriminals can almost instantaneously extract funds from a bank in one country and deposit them into accounts in other countries before the bank realizes what has happened.[18] This vastly complicates law enforcement's task of finding the perpetrator and bringing him or her to justice.[19] The criminal's use of cyberspace effectively fractures the crime, which means relevant evidence is located

---

[12] *See id.* Kennan Bradley, the County Treasurer, later became one of the plaintiffs in a lawsuit the County filed against the bank. *See, e.g.*, Emily Hagedorn, *Bank: Bullitt Could Have Avoided Theft*, COURIER-JOURNAL, Aug. 27, 2009, *available at* 2009 WLNR 16811648; *see also* Complaint at ¶ 2, Bullitt Cnty. Fiscal Court v. First Fed. Savings Bank of Elizabethtown, Inc. (Aug. 5, 2009), *available at* http://www.courier-journal.com/blogs/bullitt/ffsbcomplaint.pdf.

[13] Complaint, *supra* note 12, at ¶ 2.

[14] *See id.* For more on how a Zeus Trojan Horse attack on a bank account works, see Elinor Mills, *Zeus Trojan Steals $1 Million from U.K. Bank Accounts*, CNET NEWS (Aug. 20, 2010), http://news.cnet.com/8301-27080_3-20013246-245.html.

[15] *See, e.g.*, Krebs, *supra* note 3.

[16] *See id.*

[17] In this and similar scams, U.S. law enforcement usually apprehends some or most of the U.S.-based intermediaries, or mules. *See, e.g.*, Krebs, *supra* note 3.

[18] For more on this, see Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 VA. J.L. & TECH 13, 18–19 (2004).

[19] *See, e.g.*, Brenner, *supra* note 2.

within various U.S. states or other nation-states.[20] Officers from the jurisdiction in which the victim was attacked therefore must conduct an investigation that differs from the parochial investigations with which police historically have dealt.[21]

In traditional investigations, officers focus on a physical crime scene because in the real world it is impossible to rob, assault, murder, rape, or otherwise victimize someone without being in physical proximity to them. This means the perpetrator is likely to leave physical evidence at the scene of the crime and to have been observed arriving at or leaving the crime scene.[22] Given the need for physical proximity between perpetrator and victim and the constraints involved in fleeing the crime scene and disposing of evidence or the proceeds of the crime, traditional investigations are almost always conducted within a specific jurisdiction, i.e., within a single nation-state or within a constituent state in a federal system.[23] That, in turn, means that the investigation will almost certainly be conducted pursuant to the law of a single jurisdiction.[24]

As the Bullitt County bank theft illustrates, and as is explained elsewhere, this is not true of cybercrime.[25] Physical proximity between perpetrator and victim is not required; the crime scene and the evidence it encompasses can, as in the Bullitt County case, be scattered across two or more nation-states, which means the investigation will implicate the laws and the law enforcement officers of more than one jurisdiction.[26]

This creates scenarios with which law enforcement officers are ill-equipped to deal.[27] As scholars have explained elsewhere, the methods that law enforcement has traditionally used, on the rare

---

[20] For more on this, see Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 416–81 (2007).

[21] For more on this, see Brenner, *supra* note 2.

[22] *See id.*

[23] *See id.*

[24] *See id.*

[25] *See id.*

[26] *See id.*

[27] *See id.*

occasions when transnational evidence gathering was necessary, are far too complicated and cumbersome to be effective in this context.[28] And in some instances, they may simply not be available; one country may not, for example, have a mutual legal assistance treaty with another.[29] This leaves the investigating officers with two equally unattractive options: end their investigation or possibly violate foreign law in their efforts to obtain evidence.[30]

This is precisely what happened in 1999, when the Federal Bureau of Investigation was investigating a series of intrusions that originated in Russia and targeted "the computer systems of businesses in the United States."[31] The attackers stole financial information from the victims' computers and tried to extort money by threatening to expose sensitive data to the public or damage the victims' computers.[32]

After one of the attackers identified himself as "Alexey Ivanov" and the FBI confirmed that he was in Russia, the Department of Justice sent a request through diplomatic channels to Russian authorities, asking them to detain Ivanov and question him about the attacks.[33] The Russians did not respond to the initial contact or to a repeated request.[34] Because the United States does

---

[28] *See, e.g.*, Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347 (2002).

[29] *See id.* at 354. A "mutual legal assistance legal treaty," or MLAT, is a "bilateral intergovernmental agreement that obliges foreign jurisdiction authorities to render assistance" in evidence gathering. Nicholas M. Mclean, Note, *Cross-National Patterns in FCPA Enforcement*, 121 YALE L.J. 1970, 1987 (2012).

[30] *See, e.g.*, Brenner & Schwerha, *supra* note 28 at 348–54.

[31] United States v. Gorshkov, No. 00-550, 2001 WL 1024026, at *1 (W.D. Wash. May 23, 2001).

[32] *See* Press Release, U.S. Dep't of Justice, Russian Computer Hacker Convicted by Jury (Oct. 10, 2001), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2001/gorshkovconvict.htm.

[33] *See* Ariana Eunjung Cha, *A Tempting Offer for Russian Pair*, WASH. POST (May 19, 2003), http://www.washingtonpost.com/ac2/wp-dyn/A7774-2003May18?language=printer.

[34] *See id.*

not have an extradition treaty with Russia, Russian authorities would not have been obliged to turn Ivanov over to the United States for prosecution had the United States made such a request.[35]

Because the U.S. agents had no authority to arrest Ivanov in Russia, they decided to use a "sting" to get him to the United States.[36] They lured both Ivanov and his partner in cybercrime, Vasiliy Gorshkov, to Seattle to interview with a phony company, "Invita."[37] The men arrived in Seattle in November 2000 and were met by an undercover agent, who took them to the "Invita" office.[38] There, agents posing as "Invita" employees asked the Russians to demonstrate their hacking skills, using Invita computers. The hackers did not know the FBI had installed loggers—programs that record what is typed on a keyboard—on the computers.[39] As Ivanov and Gorshkov demonstrated their skills, the loggers recorded what they typed, which included the usernames and passwords they used to access the tech.net.ru server—which was their *kontora*'s (i.e., their unofficial company's) server in Russia.[40] The server stored tools they needed for the hacking demonstration. After the demonstration was over, they were arrested.[41]

Without getting a search warrant, FBI agents retrieved the usernames and passwords the loggers recorded and used them to access the tech.net.ru server and download 250 gigabytes of data.[42] The agents did not let Russian authorities know what they were doing.[43] Gorshkov and Ivanov were subsequently indicted for

---

[35] *See id.*; *see also* James A. Wilson, *Extradition: The New Sword or the Mouse that Roared?*, THE ANTITRUST SOURCE, Apr. 2011, at 1, 4 (citing list of treaties in 18 U.S. Code § 3181).

[36] *See* Cha, *supra* note 33.

[37] *See id.*

[38] *See id.*

[39] *See id.*

[40] *See* Brendan I. Koerner, *From Russia with LØPHT*, LEGAL AFFAIRS, May–June 2002, *available at* http://www.legalaffairs.org/printerfriendly.msp?id=286.

[41] *See* Cha, *supra* note 33.

[42] *See* Koerner, *supra* note 40.

[43] *See, e.g.*, United States v. Gorshkov, No. 00-550, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (noting that the "search was done by FBI fiat").

violating federal cybercrime law, and prosecutors prepared to use evidence from the tech.net.ru server at their trials.[44]

Gorshkov moved to suppress the evidence, arguing that it was the product of a search that violated the Fourth Amendment because the agents did not obtain a warrant before accessing the Russian server.[45] The district court held that the search did not violate the Fourth Amendment because it did not apply.[46] The Supreme Court has made clear that the "Fourth Amendment does not apply to . . . search[es] and seizur[es] of a non-resident alien's property outside . . . the United States."[47] Gorshkov and Ivanov were non-resident aliens; and the judge found that the search of the Russian server took place entirely "in" Russia, not in the United States.[48]

Ivanov pled guilty to various cybercrime charges and Gorshkov went to trial and was convicted on similar charges, after which both were sentenced to prison.[49] That was the end of the prosecutions, but not the case: In 2002, Russia's Federal Security Service—a police agency—charged one of the Invita agents with hacking in violation of Russian law.[50] The charge was apparently a symbolic way to assert Russian sovereignty over persons and

---

[44] *See id.* at *1; *see also* United States v. Ivanov, 175 F. Supp. 2d 367, 368–70 (D. Conn. 2001).

[45] *See Gorshkov*, 2001 WL 1024026 at *1–2.

[46] *See id.* at *2–3.

[47] *See id.* at *3 (citing United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)).

[48] *See id.* at *3.

[49] *See* Press Release, U.S. Dep't of Justice, Russian Computer Hacker Sentenced to Three Years in Prison (Oct. 4, 2002), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2002/gorshkovSent.htm; Press Release, U.S. Dep't of Justice, Russian Hacker Sentenced to Prison (July 25, 2003), *available at* http://www.usdoj.gov/usao/nj/press/files/iv0725_r.htm.

[50] *See, e.g.*, Mike Brunker, *FBI Agent Charged with Hacking*, MSNBC (Aug. 15, 2002), http://www.msnbc.msn.com/id/3078784/. Article 272 of the Russian Criminal Code makes "illegal accessing of computer information" a crime. UGOLOVNYU KODEKS ROSSIISKOI FEDERATH [UK RF] [CRIMINAL CODE] art. 272 (Russ.).

things in the territory Russia controls.[51] In announcing the charge, a spokesperson explained that "[i]f the Russian hackers are sentenced on the basis of information obtained by the Americans through hacking, that will imply the future ability of U.S. secret services to use illegal methods in the collection of information in Russia and other countries."[52] The Federal Security Service sent the criminal complaint to the Department of Justice and asked that the agent be surrendered for prosecution in Russia; the United States has apparently never responded.[53]

Scholars have examined the likely law enforcement response to this evolving state of affairs: remote computer searches.[54] The analysis has focused on whether U.S. law enforcement's using Trojan Horse programs to remotely search U.S. citizens' computers would violate the Fourth Amendment's prohibition on "unreasonable" searches and seizures.[55] At least one author has concluded that it would not, as long as the officers conducted the searches in a manner that comported with the Fourth Amendment's requirements, i.e., as long as they either obtained a search warrant that authorized the remote investigation or relied on a valid exception to the warrant requirement, such as exigent circumstances.[56] If that assessment is correct, it means that U.S. officers can remotely—and surreptitiously—explore the contents of citizens' computers and then use whatever they find as evidence in a criminal prosecution even though the search dynamic involved

---

[51] *See, e.g., FSB Hopes to Bring to Court Case Against FBI Agents*, RUSS. & FSU NEWS BULL., Oct. 10, 2001, *available at* 2002 WLNR 14527663 (noting that "[t]he problem is a matter of principle").

[52] *See* Brunker, *supra* note 50.

[53] *See, e.g.*, Ariana Eunjung Cha, *Despite U.S. Efforts, Web Crimes Thrive*, WASH. POST (May 20, 2003), http://www.washingtonpost.com/ac2/wp-dyn/A12984-2003May19; *see also FSB Hopes to Bring to Court Case Against FBI Agents*, *supra* note 51.

[54] Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force*, 81 MISS. L. J. 1229 (2012). For a definition of remote computer searches, *see infra* Part II.B.

[55] *See* Brenner, *supra* note 54, at 1229–46.

[56] *See id.* at 1246–53.

differs wildly from the searches with which the drafters of the Fourth Amendment were concerned. [57]

That remote computer searches differ greatly from the type of searches the Framers had in mind should not, in and of itself, be a barrier to bringing remote computer searches within the compass of the Fourth Amendment. Indeed, the United States' experience with evolving communications technology and the Fourth Amendment demonstrates that this outcome is preferable to the alternative. For example, in 1928, the U.S. Supreme Court rejected Roy Olmstead's argument that officers violated the Fourth Amendment by tapping phone lines leading into his home and listening to conversations he had with his colleagues in crime.[58] The Court found that "[t]here was no searching" because "[t]here was no entry" into Olmstead's home.[59] In reaching this conclusion, it relied on the proposition that "[t]he Fourth Amendment is to be construed in the light of what was deemed a . . . search . . . when it was adopted."[60]

It was not until 1967 that the Court reversed itself and held that it is a Fourth Amendment search for officers surreptitiously to listen to or record citizens' telephone conversations.[61] In the intervening years, because wiretapping did not violate the Fourth Amendment, those who were the targets of such activity could not successfully move to have the evidence suppressed as the product of a Constitutional violation.[62] Given the empirical analogies between wiretapping and remotely searching a computer, it is likely that the Court will hold that the latter also constitutes a Fourth Amendment search.

Therefore, this Article assumes that, for Fourth Amendment purposes, remote computer searches will be treated like more traditional searches. This means the default rule in the United

---

[57] *See id.*

[58] *See* Olmstead v. United States, 277 U.S. 438 (1928).

[59] *See id.* at 464.

[60] *Id.* at 465 (quoting Carroll v. United States, 267 U.S. 132, 149 (1924)).

[61] *See* Katz v. United States, 389 U.S. 347, 353 (1967).

[62] *See, e.g.*, Goldman v. United States, 316 U.S. 129, 135 (1942) (holding that use of a "detectaphone" listening device did not violate the Fourth Amendment).

States will be that such searches are lawful, as noted above, as long as they are conducted in accordance with the Fourth Amendment's requirements. Analogous rules are likely to emerge elsewhere. The default rule may not be the only one that emerges in this context.

Part II examines the possibility that dissonances will emerge in the rules that govern remote computer searches in the United States. It articulates a scenario in which dissonance emerges between federal law and the law of certain states due to the fact that the latter imposed standards on remote computer searches that exceed those required by the Fourth Amendment in either of two ways. Part II continues by analyzing the legal issues that are likely to arise if and when this scenario eventuates. That is, it analyzes how courts would deal with situations in which, for example, officers from State A, which applies a "mere" Fourth Amendment standard, remotely search a computer located in State B, which applies a Fourth Amendment "plus" standard. The analysis focuses on various issues, including the issue of precisely "where" such a search should be deemed to be conducted, for the purposes of applying search and seizure law.

Part III then examines the possibility that similar dissonances will emerge in transnational searches. It notes that one level of dissonance already exists in the search and seizure laws of two European states (e.g., the United Kingdom and Germany), and analyzes the likelihood that the issues examined in Part II are also likely to manifest themselves at the international level.

The purpose of the generally theoretical analyses in Parts II and III is to illustrate how remote crime and remote computer searches challenge the territorially-based Westphalian governance structures that currently monopolize sovereign power around the globe. A subsidiary purpose is to illustrate the increasing untenability of this system, at least with regard to transnational cybercrime.

II. UNITED STATES: FEDERALISM AND DISSONANCE

The potential for dissonant rules governing remote searches by U.S. law enforcement arises from the nature of the U.S. federal system:

> America's federal system offers dual protection . . . under the federal and state constitutions. The Federal Constitution protects all citizens, and its protections must be enforced by the states. However, a state can offer greater protection to its citizens based on that state's constitution. A state court's interpretation of its constitution is not reviewable by the United States Supreme Court.[63]

Every U.S. state has its own constitution and "each of these constitutions includes . . . a 'cognate' or 'analog' to the Federal Fourth Amendment."[64] In the 1970's, some state supreme courts began to interpret their versions of the Fourth Amendment as providing more protection for privacy than the U.S. Constitution.[65] Over the ensuing decades, these states have increasingly departed from "the federal courts' narrow interpretation of the Fourth Amendment"[66] to provide "more expansive protection of privacy"[67] under their own constitutions, a trend one author suggests will only increase "with advances in technology."[68] The results are that (i) every search and seizure conducted in the United States or conducted by U.S. law enforcement officers and that targets a U.S. citizen must comply with the requirements of the Fourth Amendment; and (ii) searches and seizures conducted in discrete

---

[63] Paul H. Anderson & Julie A. Oseid, *A Decision Tree Takes Root in the Land of 10,000 Lakes: Minnesota's Approach to Protecting Individual Rights Under Both the United States and Minnesota Constitutions*, 70 ALB. L. REV. 865, 870 (2007); *see also* Cooper v. California, 386 U.S. 58, 62 (1967) (noting that states have the "power to impose higher standards on searches and seizures than required by the Federal Constitution if [they] choose to do so").

[64] Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 374 (2006).

[65] *See, e.g.*, Katharine Goodloe, *A Study in Unaccountability: Judicial Elections and Dependent State Constitutional Interpretations*, 35 N.Y.U. REV. L. & SOC. CHANGE 749, 751, 753–55 (2011) (tracing the rise of the "New Federalism movement," in which criminal defense attorneys began asking "state judges to find more protections under state constitutions than the United States Supreme Court found in similar provisions of the federal constitution").

[66] Brian Andrew Suslak, Note, *GPS Tracking, Police Intrusion, and the Diverging Paths of State and Federal Judiciaries*, 45 SUFFOLK U. L. REV. 193, 194 (2011).

[67] *Id.*

[68] *Id.* at 195.

states must comply with the Fourth Amendment and with any heightened requirements imposed by that state's law.[69]

With regard to remote computer searches, this Article assumes for the purposes of analysis[70] that (i) the U.S. Supreme Court has held that such searches are constitutional if they are conducted in accordance with the Fourth Amendment's requirements, (ii) twelve U.S. state supreme courts have held that such searches are lawful if they are conducted in accordance with the Fourth Amendment and with the heightened requirements imposed by their state analogs of the Fourth Amendment,[71] and (iii) sixteen other state supreme courts have held that remote computer searches are categorically unlawful under their state analogs of the Fourth Amendment.[72] The remaining twenty-two state supreme courts follow the U.S. Supreme Court's rule and apply the Fourth Amendment only to the conduct of remote computer searches.[73] Since U.S. state supreme courts cannot interpret their constitutions as providing less protection than the Fourth Amendment,[74] this exhausts the scenarios that can arise in this context.

---

[69] *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 283 n.7 (1990) (Brennan, J., dissenting) ("[T]he rule, accepted by every Court of Appeals to have considered the question, that the Fourth Amendment applies to searches conducted by the United States Government against United States citizens abroad."); *see also* U.S. v. Toscanino, 500 F.2d 267, 280–81 (2d Cir. 1974).

[70] The first two assumed categories—"Fourth Amendment-plus states" and "Fourth Amendment-trump states"—do not actually exist, because no state has so far adopted specific standards governing remote computer searches that exceed the requirements of the Fourth Amendment. Therefore, all of the U.S. states are, by default, Fourth Amendment-only states. *See infra* note 73 and accompanying text. That is, absent future legislative or judicial action, the law governing remote computer searches in the fifty states is limited to the Fourth Amendment.

[71] These states shall be referred to as "Fourth Amendment-plus" states.

[72] These states shall be referred to as "Fourth Amendment-trump" states.

[73] These states shall be referred to as "Fourth Amendment-only" states. Because the requirements imposed by these states are coterminous with those of the Fourth Amendment, they will not be separately considered in the analysis that follows.

[74] *See* U.S. CONST. art. VI, cl. 2 (Constitution and laws made pursuant to it are the "supreme Law of the Land" and state court judges are bound by it, the "Constitution or Laws . . . of [their State] to the Contrary notwithstanding.").

Part II.A reviews how the state courts that impose Fourth Amendment-plus standards deal with situations in which "outsiders"—federal agents and officers from another state—conduct searches that do not comport with the heightened requirements imposed by that state's supreme court. Part II.B then analyzes how the existing standards apply or do not apply to remote computer searches conducted pursuant to the standards in effect in the Fourth Amendment-plus and Fourth Amendment-trump states.

A. *Current U.S. Law*

The postulated existence of Fourth Amendment-plus and Fourth Amendment-trump states illustrates how dissonant rules could arise to complicate the application of the hypothesized rule concerning the Fourth Amendment's applicability to remote computer searches. The possibilities for and consequences of such dissonance are examined below. The discussion also considers the extent to which dissonance can become an issue in the residual scenario noted above, in which twenty-two states follow the federal rule and rely solely on the Fourth Amendment.[75] In the federal system and in these twenty-two states, the lawfulness of remote computer searches is a function of the extent to which they comport with the Fourth Amendment only.[76] This is true regardless of whether the searches are conducted by local law enforcement officers, federal agents, or officers from other states.

This proposition would prevent the remaining states from refusing to enforce the Fourth Amendment or enforcing a "Fourth Amendment light" standard by enforcing some, but not all, of the Fourth Amendment's requirements or by substituting a less-rigorous state rule. *See, e.g.*, Ruth A. Moyer, *Why and How a Lower Federal Court's Decision That a Search or Seizure Violated the Fourth Amendment Should Be Binding in a State Prosecution: Using "Good Sense" and Suppressing Unnecessary Formalism*, 36 VT. L. REV. 165, 178 (2011).

[75] *See supra* note 73 and accompanying text.

[76] *See supra* note 73 and accompanying text. *See also* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.5(c), at 176 (4th ed. 2004) ("[T]here is no constitutional requirement that evidence obtained in another jurisdiction be suppressed merely because the process of acquisition offended some local law . . . .").

Because the Fourth Amendment is a *de minimis* standard with which all U.S. law enforcement officers must comply,[77] rule dissonance should not become an issue in prosecutions brought in these states.[78] If officers from another state or federal agents use remote searches to obtain evidence from a computer in a Fourth Amendment-only state, but do not comply with the Fourth Amendment's requirements in doing so, the defendant(s) can, aside from anything else, have the evidence suppressed as having been obtained in violation of the Fourth Amendment.[79]

In the twelve states in which the state supreme court has held that remote computer searches are lawful if they satisfy a Fourth Amendment-plus standard, the states' own officers are bound to comply with that standard. If they conduct remote computer searches that satisfy only the Fourth Amendment's requirements, the evidence will be suppressed as having been obtained in violation of the state constitution.[80] The same may be true if federal agents conduct remote searches in a Fourth Amendment-plus state but comply only with the Fourth Amendment. Some courts have held that to be admissible in a prosecution in their state, evidence must have been obtained in a manner that comports with the requirements of their state constitution.[81] Other courts

---

[77] *See supra* text accompanying note 74.

[78] In Part II.B, the possibility is explored that dissonance might arise when officers from a scenario (ii) or (iii) state remotely search a computer located in a Fourth-Amendment-only state and then seek to use the evidence so obtained in a prosecution brought in the scenario (ii) or (iii) state.

[79] *See, e.g.*, Mapp v. Ohio, 367 U.S. 643, 654–55 (1961).

[80] *See, e.g.*, State v. Mollica, 524 A.2d 1303, 1305–06 (N.J. Super. Ct. App. Div. 1987), *appeal granted and cause remanded*, 554 A.2d 1315 (N.J. 1989).

[81] *Accord* State v. Torres, 262 P.3d 1006, 1021 (Haw. 2011) ("We next consider whether the searches of Petitioner's vehicle were valid under the Hawaii Constitution, notwithstanding the fact that they were lawful under the United States Constitution."); *see, e.g.*, State v. Cardenas-Alvarez, 25 P.3d 225, 232 (N.M. 2001); State v. Rodriguez, 854 P.2d 399, 404 (Or. 1993).

Courts that take this view tend to focus on the exclusionary rule's role in protecting the citizen's right to be free from "unreasonable" searches. *See, e.g.*, State v. Gutierrez, 863 P.2d 1052, 1067 (N.M. 1993); People v. Porter, 742 P.2d 922, 925 (Colo. 1987). This is the preferred approach among modern courts. *See, e.g.*, State v. Torres, 262 P.3d at 1014–16; *see also* LAFAVE, *supra* note 76

have held that "evidence seized by federal agents, acting . . . in conformity with federal standards, will be admissible in state courts, even though the actions of the federal agents may not have met a higher burden imposed by the state constitution."[82]

Finally, some have applied this same principle to evidence seized by officers from another state on the theory that the

---

(noting that there is a "general practice . . . of using the exclusionary rule for violations of state law").

The Hawaii Supreme Court found that the exclusionary rule serves three principles: "judicial integrity, protection of individual privacy, and deterrence of illegal police misconduct." *Torres*, 262 P.3d at 1018 (citing State v. Bridges, 925 P.2d 357, 365 (1996)); *see also* LAFAVE, *supra* note 76 ("The purposes for using the exclusionary rule for violations of state law . . . are . . . deterrence of the police; the imperative of judicial integrity; and assuring the people that the government will not profit from its lawless behavior."). The *Torres* court found the fact that evidence was obtained "in another jurisdiction" in violation of the state's constitutional rules on search and seizure should be given "substantial weight" in determining if use of the evidence would compromise the judicial integrity of the state's courts. *Torres*, 262 P.3d at 1019. It also found the question of whether the defendant's privacy rights were violated by such a search should not "be governed by the law and constitution" of a jurisdiction that guarantees citizens less privacy than Hawaii law. *Id.* at 1020. It additionally found that excluding evidence seized by Hawaii officers in another state would deter the state's officers from engaging in such conduct in the future. *Id.*

[82] Pena v. State, 61 S.W.3d 745, 754 (Tex. Ct. App. 2001); *see also* State v. Johnson, 879 P.2d 984, 988 (Wash. Ct. App. 1994) ("[E]vidence that is lawfully obtained by federal officers pursuant to federal law is admissible in proceedings in courts of this state even if the Washington State Constitution would have required exclusion of evidence obtained in a similar manner by state officials."). Courts that take this view tend to focus on the deterrence rationale for the exclusionary rule and often find that suppressing the evidence would serve no purpose with regard to deterring conduct by their state officers because "it is only the conduct of another jurisdiction's officials that is involved." *Mollica*, A.2d at 1328. *But see Torres*, 262 P.3d at 1020 (finding that applying state exclusionary rule "would deter any federal and state cooperation 'to evade state law' "). This is known as the "reverse silver platter doctrine." *See, e.g., id.* at 1014. One article suggests "more states will want to exclude such evidence now that the Supreme Court has continued to narrow the exclusionary rule . . . ." Robert M. Bloom & Hillary Massey, *Accounting for Federalism in State Courts: Exclusion of Evidence Obtained Lawfully By Federal Agents*, 79 U. COLO. L. REV. 381, 391 (2008).

"protections afforded by the constitution of a sovereign entity control the actions only of the agents of that sovereign entity."[83]

The states that apply their constitutions to only in-state law enforcement officers incorporate a qualifier into this principle: In searching for and seizing evidence, federal agents and law enforcement officers from another state must not have been acting in cooperation with officers from the state in which the search and seizure occurred.[84] The premise is that the state's heightened standards do not apply to either when they act on their own behalf because they are "officers from another jurisdiction" who are not bound by local law,[85] but that they do apply when federal agents or officers from another state act "as agents for the [local] police."[86] When such an agency relationship exists, the federal agents or officers from another state "are subject to the same constitutional standards applied to the [local] police," which means "evidence

---

[83] *Mollica*, 554 A.2d at 1324. The *Mollica* court explained:

> [B]ecause the constitution of a state has inherent jurisdictional limitations and can provide broader protections than found in the United States Constitution or the constitutions of other states, the application of the state constitution to the officers of another jurisdiction would disserve the principles of federalism and comity, without properly advancing legitimate state interests.

Id. at 1327. The courts in at least one state refer to this as the "silver platter doctrine." *See, e.g.*, State v. Ventress, No. 59369-2-I, 2011 WL 1237644, at *2 (Wash. App. Apr. 4, 2011). The Supreme Court held that "a search is a search by a federal official if he had a hand in it; it is not a search by a federal official if evidence secured by state authorities is turned over to the federal authorities on a silver platter." Lustig v. United States, 338 U.S. 74, 78–79 (1949). The Court abolished this doctrine as unconstitutional, holding that "evidence obtained by state officers during a search which, if conducted by federal officers, would have violated the defendant's immunity from unreasonable searches and seizures under the Fourth Amendment is inadmissible . . . in a federal criminal trial." Elkins v. United States, 364 U.S. 206, 223 (1960).

[84] *See, e.g.*, State v. Garcia-Navarro, 226 P.3d 407, 409 (Ariz. Ct. App. 2010); People v. Coleman, 439, 882 N.E.2d 1025, 1032 (Ill. 2008); *Pena*, 61 S.W.3d at 754–55.

[85] *Pena*, 61 S.W.3d at 754.

[86] *Id.* at 755.

seized by [them] while operating in such capacity is subject to exclusion if not seized according to those standards."[87]

The same principles should apply to the Fourth Amendment-trump states, i.e., states in which the state supreme court has declared that certain searches which do not violate the Fourth Amendment are categorically unlawful under the state's own constitution. It would be illogical for states to suppress evidence obtained in violation of a Fourth Amendment-plus standard but decline to suppress evidence obtained in violation of a Fourth Amendment-trump standard. Logically, a violation of the more stringent standard should trigger consequences that are at least as severe as those imposed for a violation of the lesser standard.

There are, so far, no instances in which a state supreme court has used its constitution to adopt a Fourth Amendment-trump standard, even though such a result does not appear to be inconsistent with the Fourth Amendment.[88] The Fourth

---

[87] *Id.* Courts and commentators have found that a state supreme court's interpretation of its own constitution as providing more protection than the Fourth Amendment has "no binding effect on federal law enforcement." State v. Schwartz, 689 N.W.2d 430, 445 (S.D. 2004). *See also* United States v. Clyburn, 24 F.3d 613, 616 (4th Cir. 1994) ("[T]he Fourth Amendment, not . . . state law, governs the admissibility of evidence obtained by state officers but ultimately used in a federal prosecution."); United States v. Wright, 16 F.3d 1429, 1434 (6th Cir. 1994) ("A state may impose a rule for searches and seizures that is more restrictive than the Fourth Amendment . . . . However, the state rule does not have to be applied in federal court."); United States v. Dudek, 530 F.2d 684, 689–90 (6th Cir. 1976) ("[E]vidence seized in actual or (as here possible) violation of state law may nonetheless be admitted in a federal prosecution where the violation concerned would not be such as to require suppression of evidence under federal constitutional law . . . ."). In other words, a federal court is not bound to suppress evidence obtained in violation of state law. *See, e.g.*, *id.* at 689–90; *see also* Kenneth J. Melilli, *Exclusion of Evidence in Federal Prosecutions on the Basis of State Law*, 22 GA. L. REV. 667, 668 (1988) ("[F]ederal courts have generally resisted excluding evidence from criminal prosecutions for violations of state law.").

[88] *But see* Sitz v. Dep't of State Police, 485 N.W.2d 135, 138–39 (Mich. Ct. App. 1992) ("[W]e believe compelling reason exists to interpret the Michigan Constitution as affording greater rights than those found in the federal constitution. . . . Such a substantial departure, if appropriate, should be effected by our Supreme Court, not by this Court."); State v. Opperman, 247 N.W.2d

Amendment-trump standard means the state supreme court used the state constitution to hold that (i) state officers are categorically barred from conducting certain types of searches even though the searches do not violate the Fourth Amendment, but (ii) this prohibition does not apply to federal agents, at least not when they are acting solely as federal agents.[89] The same principle should also apply to officers from other states, as long as they were not acting as agents of the local police.[90]

This Article addresses the so-far-hypothetical Fourth Amendment-trump standard in this analysis because it is a doctrinal and empirical possibility and because its hypothesized application promotes the analysis of how dissonant rules can complicate the process of conducting remote computer searches. Part II.B examines this issue in greater detail.

B. *Remote Searches and Dissonance*

Before this Article considers how dissonant rules can complicate remote computer searches, it is useful to define such

---

673, 675 (S.D. 1976) ("[T]he protection afforded by S.D. CONST., art. VI, § 11 warrant a higher standard of protection for the individual in this instance than the United States Supreme Court found necessary under the Fourth Amendment."). This may change as intrusive technologies increase in sophistication and/or the exclusionary rule plays a lesser role in the enforcement of the Fourth Amendment. *See, e.g.*, Bloom & Massey, *supra* note 82, at 391. As noted above, the states—and their courts—are constitutionally bound to enforce the Fourth Amendment, which is part of the "supreme Law of the Land." *See supra* text accompanying note 74. This means that the states cannot provide less protection for privacy than the Fourth Amendment requires, but, as noted earlier, it does not bar states from providing more protection. *See* Goodloe, *supra* note 65. Because a rule that categorically bars in-state officers from conducting certain types of searches presumably provides at least as much protection as the Fourth Amendment, Fourth Amendment-trump rules should pass constitutional muster.

[89] *See, e.g.*, State v. Cardenas-Alvarez, 25 P.3d 225, 232 (N.M. 2001) ("Our application of state constitutional standards to determine the admissibility in state court of evidence seized by federal agents will not affect any prosecution that might be brought against Defendant in federal court, or otherwise circumscribe federal activities within our borders.").

[90] *See supra* notes 83–86 and accompanying text.

searches. Literally, a remote computer search would involve law enforcement officers situated at Point A using the Internet to surreptitiously search the data on a computer located at Point B. In its simplest formulation, a remote computer search is one in which the searchers are in a physical location other than the location where the computer that is the target of their search is situated. In this formulation, the only requirement for a "remote" computer search is that the searchers and computer(s) being searched are not physically proximate when the search occurs.

This baseline formulation of a remote computer search implicates the Fourth Amendment as long as one assumes, as this Article does, that U.S. citizens and aliens in U.S. territory have a reasonable expectation of privacy in their hard drives.[91] The default rule postulated in Part I would therefore require officers who intend to conduct such a search to obtain a warrant or otherwise satisfy the requirements of the Fourth Amendment before they begin searching.[92] And as outlined in Part II.A, the officers might also have to comply with additional standards established by state supreme courts. But that should be the only complication they would confront with the baseline formulation because it does not necessarily implicate the problem of dissonance. Dissonance can arise only when Point A is in one sovereign state and Point B is in another.[93] Dissonance is an

---

[91] *See, e.g.*, Commonwealth v. Cormier, No. 09-1365, 2011 WL 3450643, at *4 (Mass. Super. Ct. June 27, 2011); Brackens v. State, 312 S.W.3d 831, 841 (Tex. Ct. App. 2009). Such an expectation of privacy does not exist if the hard drive's owner has knowingly exposed its contents to public view by installing and using file-sharing software that exposes at least some of its contents to other users. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008); United States v. Gabel, No. 10-60168, 2010 WL 3927697, at *5–7 (S.D. Fla. Sept. 16, 2010). *See also* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."). The Supreme Court has held that the Fourth Amendment applies to U.S. citizens and aliens who are in U.S-controlled territory. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 268–72 (1990).

[92] *See* Brenner, *supra* note 54, at 1229–46.

[93] *See supra* Part II.A.

implicit possibility in the baseline formulation of remote computer searches, but it is not inevitable.

To ensure dissonance can arise, the Article from this point forward uses a modified formulation of remote computer searches: The Article will assume that Point A, the place from which officers conduct a remote computer search, is in the territory of one sovereign state and that Point B, the place where the computer that is the target of the search is situated, is in the territory of another sovereign state. For these purposes, a "sovereign state" is a nation-state (e.g., Canada),[94] a sovereign entity that is a constituent of a federal nation-state (e.g., Virginia),[95] or a confederation of nation-states (e.g., the European Union).[96] The remainder of this Part only addresses dissonance in the constituent entities that comprise the United States: the fifty states plus the District of Columbia.[97] Part III examines dissonance among nation-states.

---

[94] *See, e.g.*, D. Carolina Núnez, *Inside the Border, Outside the Law: Undocumented Immigrants and the Fourth Amendment,* 85 S. CAL. L. REV. 85, 117 n.158 (2011) (describing a nation-state as "a unitary, self-contained actor with complete and exclusive jurisdiction over the people within its territory").

[95] *See, e.g.*, John Dinan, *Patterns of Subnational Constitutionalism in Federal Countries,* 39 RUTGERS L.J. 837, 839 (2008) (noting that federal states whose constituent states have their own constitutions include the United States, Argentina, German Federal Republic, Mexico, and Venezuela); *see also* U.S. CONST. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.").

[96] *See, e.g.*, Elisabetta Lanza, Development, *Core of State Sovereignty and Boundaries of European Union's Identity in the Lissabon-Urteil*, 11 GERMAN L.J. 399, 405 (2010) (noting that the European Union is a "confederation of states" rather than a "federal state").

[97] *See, e.g.*, Jo Anne Hagen, *An Overview of U.S. Import/Export Regulations—Part I, Exports*, COLO. LAW., July 2003, at 75, 75 (noting that the United States "is comprised of the fifty states ... all U.S. territories, dependencies, and possessions"). Dissonance among rules adopted by the United States and its constituent entities can also encompass the U.S.-controlled territories. *See generally* Christina Duffy Burnett, *Untied States: American Expansion and Territorial Deannexation,* 72 U. CHI. L. REV. 797, 805–13 (2005) (reviewing applicability of U.S. law to territories and "other places subject to U.S. sovereignty"). They are not incorporated into the analysis because the application of the Fourth Amendment and other principles of U.S.

Part II postulated three scenarios. The original scenarios and the analysis in Part II.A implicitly incorporated the baseline formulation of remote computer searches noted above, which encompasses but is not coextensive with the possibility of rule dissonance.[98] The analysis of the scenarios in this Part addresses that limitation of the original formulation by incorporating the modified formulation outlined above; i.e., it assumes the searchers and the target of the search are located in different states. This does not guarantee rule dissonance but it guarantees that rule dissonance is possible. The two Parts below analyze the possibilities for dissonance in searches that involve states with inconsistent standards. It is assumed, in analyzing all of these scenarios, that the law enforcement officers who conducted the remote computer search complied with the requirements of the Fourth Amendment.[99]

C. *State-to-State Dissonance*

This Part examines the dissonance that arises when officers from one state remotely search a computer in another state and then use the evidence obtained from that search to prosecute someone in their state. The scenarios fall into two categories: searches that involve Fourth Amendment-only and Fourth Amendment-plus states, and searches that involve Fourth Amendment-plus and Fourth Amendment-trump states.[100]

1. *Fourth Amendment-only and Fourth Amendment-plus States*

If officers in one Fourth Amendment-only state remotely search a computer in another of these states, no dissonance arises because these states all use the same, federal standard: Remote searches are constitutional if they are conducted in accordance with the Fourth Amendment.[101] This result holds regardless of

---

law is not as linear as it is for the U.S. states and the District of Columbia. *See, e.g.*, Ediberto Román, *The Citizenship Dialectic*, 20 GEO. IMMIGR. L.J. 557, 586–88 (2006).

[98] *See supra* Part II.A.

[99] *See supra* Part II.

[100] *See supra* Part II.

[101] *See supra* Part II.

whether the prosecution is brought in the state whose officers conducted the cross-border search or in one of the other Fourth Amendment-only states. In other words, the person who is the target of such a search, and a resulting prosecution, cannot move to suppress the evidence obtained in the remote search either on the grounds that it violated the Fourth Amendment or the law of either of the states involved. It also holds regardless of whether the local officers, officers from another Fourth Amendment-only state, or federal agents conduct the search.[102] Because these states apply the (for the Article's purposes) *de minimis* Fourth Amendment standard,[103] dissonance does not arise with regard either to the other twenty-one states that follow this rule or with regard to the federal system. This is true regardless of whether the evidence is to be used in a prosecution brought by the state in which the computer was searched, by another Fourth Amendment-only state, or by the federal system.

It is not true for prosecutions brought in a Fourth Amendment-plus state that are based at least in part on evidence obtained by remotely searching a computer in a Fourth Amendment-only state. Assume, for example, that Fourth Amendment-plus Ohio's officers remotely search a computer in Fourth Amendment-only Idaho.[104] The officers provide the evidence so obtained to an Ohio prosecutor who seeks to admit it into evidence in the Ohio prosecution of John Doe, an Ohio resident who downloaded child pornography from the computer in Idaho. In conducting the remote computer search, the Ohio officers complied with the requirements of the Fourth Amendment and, in so doing, complied with the requirements of the Idaho Constitution.[105] But they did not comply with the Ohio Constitution's additional requirements.

---

[102] *See supra* notes 77–79 and accompanying text.

[103] *Id.*

[104] The law attributed to Ohio in this and the subsequent scenarios in this section is purely hypothetical.

[105] Given the default rule hypothesized earlier, i.e., that remote searches are constitutional if they are conducted in accordance with the requirements of the Fourth Amendment, this Article will assume in the scenarios examined from this point forward that the officers who conducted the out-of-state search had a local

Assume John Doe moves to suppress the evidence the officers obtained by searching the State W computer on the grounds that the search violated the Ohio Constitution. Doe points out that he is an Ohio citizen and is therefore entitled to the protections of its constitution. Under Ohio law, if officers from that state conduct a search for evidence without complying with the Fourth Amendment and with the added requirements imposed by its constitution, the evidence must be suppressed.[106]

---

search warrant that authorized the search. *See supra* Part II. That is, the Article will assume the officers got a warrant that satisfied the Fourth Amendment before they conducted the remote search.

Because their actions were authorized by a judicially-issued search warrant, one might argue that the forum state, i.e., the state in which the prosecution in which the use of the extraterritorially-seized evidence is at issue, must honor the warrant, even though it was issued by a court in another state, under the Full Faith and Credit clause of the U.S. Constitution. *See* U.S. CONST. art. IV, § 1 (stating that each state must give full faith and credit to the "Acts, Records, and judicial Proceedings of every other State"). The theory is that a search warrant is the product of a "judicial proceeding" and therefore triggers the applicability of the clause. *See, e.g.*, John Bernard Corr, *Criminal Procedure and the Conflict of Laws,* 73 GEO. L.J. 1217, 1227–28 (1985).

While it is not clear whether a search warrant qualifies for enforcement under this theory, there is another objection to relying on the clause as the basis for enforcing out of state search warrants. The Supreme Court has held that "the Full Faith and Credit Clause does not require that sister States enforce a foreign penal judgment." Nelson v. George, 399 U.S. 224, 229 (1970).

The issue in *Nelson* was whether the clause obligated the California courts to honor a North Carolina detainer for a prisoner who was serving a sentence for a conviction in a California court. *See id.* at 225–27. Given the principle noted above, the Court held that California was "free to consider what effect, if any, it will give to" the North Carolina detainer. *See id.* at 229. The *Nelson* Court was applying what is known as the penal exception to the Full Faith and Credit clause. *See, e.g.*, City of Oakland v. Desert Outdoor Advertising, Inc., 267 P.3d 48, 50–53 (Nev. 2011). Because the exception has been relied on in state courts, the Article will assume that it applies in this context and nullifies the applicability of the Full Faith and Credit clause.

[106] If the computer the officers searched belongs to someone other than Doe, the Ohio prosecutor may be able to defeat Doe's motion to suppress by arguing that the officers' conduct did not result in a "search" either for Fourth Amendment purposes or for the purposes of applying the Ohio Constitution. If the computer belongs to someone else, Doe almost certainly would not have a Fourth Amendment expectation of privacy in it, and it should be assumed, for

This issue has not yet arisen. If and when it does, it is likely that the State X prosecutor will argue that, because the officers did not conduct the search "in" State X, they were not bound to comply with the requirements of the Ohio Constitution.[107] If the

---

the purposes of analysis, that the same principle applies in Ohio constitutional analysis. *See, e.g.*, United States v. Angevine, 281 F.3d 1130, 1134–35 (10th Cir. 2002); State v. M.A., 954 A.2d 503, 512 (N.J. Super. Ct. App. Div. 2008).

Nor would Doe have a reasonable expectation of privacy if he owned the computer but had installed file-sharing software on it that let others download child pornography from it. *See, e.g.*, United States v. Norman, 448 F. App'x. 895, 897 (11th Cir. 2011) (finding no Fourth Amendment expectation of privacy in computer shared with others); United States v. Ladeau, No. 09–40021–FDS, 2010 WL 1427523, at *4 (D. Mass. Apr. 7, 2010) (finding no Fourth Amendment expectation of privacy in computer shared with others).

For the purposes of analysis, it is assumed that the Idaho computer which the Ohio officers searched belonged solely to Doe, that it was a computer he used for business he transacted in Idaho, and that he was able to access it remotely from his home in Ohio. Those assumptions should suffice to establish the expectation of privacy required to trigger the protections of the Fourth Amendment and the higher protections imposed by Ohio's constitution.

[107] This argument raises questions about precisely where the search occurred. This argument assumes that the Ohio officers were in Ohio when they searched the computer in Idaho. *See supra* Part II.B (discussing the modified formulation of remote computer searches). Did the search therefore occur (i) "in" Ohio because that is where the target of the search was located, (ii) "in" Idaho because that is where the searchers were located, or (iii) in both? This issue does not arise with traditional, non-remote searches because the searchers and the target(s) of the search are necessarily physically proximate while the search takes place. With cyberspace, the search dynamic can be altered, so physical proximity is no longer inevitable.

This issue has yet to be resolved in the context of remote computer searches, but courts that confront it might apply the rule federal courts have applied to transborder wiretaps, i.e., that a communication is "intercepted" where the tapped phone is located and where the "listening post" is located. *See, e.g.*, United States v. Denman, 100 F.3d 399, 403–04 (5th Cir. 1996). If that proposition is applied to the Doe scenario, the "place" where the search occurred will not be dispositive because it occurred in State W and in State X.

There is another possible argument as to why Ohio need not—and perhaps cannot—apply its law to the search of the computer in Idaho: "The allocation of authority among the states is territorial." Douglas Laycock, *Equal Citizens of Equal and Territorial States: The Constitutional Foundations of Choice of Law*, 92 COLUM. L. REV. 249, 316 (1992). The U.S. Constitution creates one federal

computer the Ohio officers searched in Idaho belonged to an Idaho citizen, that argument might prevail because the heightened requirements of Ohio's constitution are presumably intended to protect Ohio citizens (only) and the defendant would not be an Ohio citizen.[108]

---

sovereign and fifty subordinate but fully viable state sovereigns. *See, e.g.*, *id.* at 315.

Those who drafted the Constitution believed that for sovereigns to be able to share territory, i.e., with a federal system the authority of which essentially assumed that of the states, the allocation of state and federal authority had to be "defined as carefully as could be, so that the respective powers of each sovereign were workably clear." *Id.* Part of defining the respective spheres of authority of the states was establishing clearly defined territorial boundaries for each, boundaries that defined the state's territory and, in so doing, defined the legitimate sphere within which it could make and enforce laws. *See, e.g.*, *id.* at 316–17 (citing U.S. CONST amend. XIV, § 1; U.S. CONST. art. IV, § 3, cl. 1). Perhaps the most important constitutional provision designed to ensure that the states respect each other's laws is the Full Faith and Credit clause. *See* U.S. CONST. art. IV § 1; *see also supra* note 105.

This brings us back to the Doe case: The Ohio prosecutor could argue that, under the above principles, he cannot apply Ohio law to a search that occurred on the territory of State W because one state does not have the ability to apply its search and seizure law to activity that takes place within the territory of another. *See, e.g.*, State v. Bridges, 925 P.2d 357, 367–69 (Haw. 1996), *overruled by* State v. Torres, 262 P.3d 1006, 1021 (Haw. 2011); *cf.* State v. Davis, 834 P.2d 1008, 1012–13 (Or. 1992).

In other words, the Ohio prosecutor would argue that Ohio would be unconstitutionally usurping the sovereign authority of Idaho by applying its search and seizure law to remote computer searches that target computers in the territory of Idaho. *See, e.g.*, Barry Latzer, *The New Judicial Federalism and Criminal Justice: Two Problems and a Response,* 22 RUTGERS L.J. 863, 870 (1991) ("If the prosecuting state were to impose its constitutional restrictions upon police . . . operating outside the boundaries of that state, would that give its constitution extraterritorial effect?"); *see also* Alan Howard, *Fundamental Rights Versus Fundamental Wrongs: What Does the U.S. Constitution Say About State Regulation of Out-Of-State Abortions*?, 51 ST. LOUIS U. L.J. 797, 811 n.31 (2007) ("[T]he proposition that a state may not project its laws into other states . . . is bedrock in our federal system . . . .").

[108] *See, e.g.*, State v. Garcia, 217 P.3d 1032, 1046 (N.M. 2009) ("[I]t is imperative that our state constitution . . . protect the rights of our citizens . . . .").

This scenario is a variation of the situation noted earlier in which courts have found that a state's heightened privacy guarantees must be applied when its

If the computer belongs to Doe,[109] he can argue that Ohio law should apply here because he is an Ohio citizen who is entitled to the heightened protections of its constitution, even with regard to out-of-state activity by Ohio officers who gathered evidence that would be used to prosecute him in Ohio.[110] Doe can argue that applying Ohio's constitutional requirements to the out-of-state activity by Ohio officers at issue here is consistent with the state supreme court's intention to put added constraints on the investigative tactics used by Ohio officers when they investigate

---

citizen is the target of a search that did not provide equivalent protection. *See supra* note 81 and accompanying text. And as discussed earlier, courts also often consider deterrence in determining whether to apply heightened guarantees; Doe is a not an Ohio citizen, so the Ohio court might not be inclined to apply its heightened privacy guarantees to him in order to deter its officers from violating that aspect of Ohio law. *See supra* note 81 and accompanying text.

In other words, Ohio has an interest in deterring its officers from violating its law when they are investigating Ohio citizens in Ohio, but has little, if any, interest in deterring them from violating its law when they conduct searches outside its territory that do not target its citizens. Ohio might apply its heightened privacy requirements to Doe in order to ensure the integrity of its judicial processes (assuming an Ohio court would find that the conduct of out of state searches that do not target Ohio citizens threatens to undermine such integrity). *See supra* note 81 and accompanying text.

[109] *See supra* note 106. This and other scenarios involving the search of a computer in one state that is "owned" by someone who resides in and is a citizen of another state, assume a cloud computing scenario, i.e., that Doe, in the scenario outlined above, owns storage space on a cloud computing system that is physically situated in another state.

It is further assumed that ownership of that space provides a Fourth Amendment expectation of privacy in it, as well as the privacy level(s) needed to trigger heightened state search and seizure laws. *See, e.g.*, Derek Constantine, Note and Comment, *Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, or Both?*, 28 GA. ST. U. L. REV. 499, 509 (2012) (noting that despite a "lack of clarity" in this area, "several recent decisions apply the Fourth Amendment to various networked . . . situations, showing courts' willingness to provide Fourth Amendment protection to cloud computing environments").

[110] The argument as formulated above implicitly assumes that the search occurred only in Idaho. The argument would be strengthened if the court found that it occurred both in Idaho and in Ohio.

Ohio citizens.[111] Doe can also argue that if the court does not apply Ohio's constitutional requirements to out-of-state investigative activity of Ohio officers, it would undermine the deterrence rationale inherent in those requirements and thereby weaken the state's exclusionary rule.[112] If, as noted above, the computer does not belong to Doe, it will be much more difficult for him to make these arguments successfully.[113]

Similar issues would arise if Richard Roe, an Idaho citizen, were prosecuted in Idaho based on evidence Idaho officers obtained by remotely searching a computer in Ohio. Assume that the Ohio computer belonged to Roe.[114] In conducting the search, the officers complied with the Fourth Amendment, which is all Idaho's constitution requires. But they did not comply with the heightened requirements the Ohio Constitution imposes on such searches. Roe moves to suppress the evidence as having been obtained in Ohio by methods that violate the Ohio Constitution. This scenario is essentially the converse of the Doe scenario: Doe, an Ohio citizen, was being prosecuted by Ohio authorities based on evidence Ohio officers searched for and seized from a computer in Idaho. In so doing, they complied only with Idaho's constitutional requirements, which provide less protection than those of Ohio's constitution. Doe's argument is arguably stronger than Roe's because Doe was being prosecuted in Ohio by Ohio authorities based in part on evidence they presumably obtained by violating Ohio's constitutional law. The only dissonant component of the prosecution was that the Ohio officers obtained the evidence by conducting an out-of-state search that violated the laws of their (and Doe's) state, but that complied with the law of the state in which the search took place and with the Fourth Amendment.

Roe, on the other hand, is an Idaho citizen who is being prosecuted by Idaho authorities based in part on evidence Idaho officers obtained by remotely searching a computer in Ohio. Their search of the Ohio computer complied with the Fourth Amendment

---

[111] *See supra* note 81 and accompanying text.

[112] *See supra* notes 81–82 and accompanying text.

[113] *See supra* note 106; *see also supra* note 108 and accompanying text.

[114] *See supra* notes 108–09 and accompanying text.

and therefore with the constitutional standards of Roe's own state, but it did not comply with the heightened requirements of Ohio's constitution. As such, it is difficult to see how Roe can successfully argue that the search violated his rights under the U.S. Constitution, Idaho's constitution, or Ohio's constitution.[115] Because the search of the computer complied with the Fourth Amendment and State W's constitutional requirements, Roe has no basis on which to suppress under the federal or Idaho constitutions. That leaves Ohio. Roe, of course, is not being prosecuted by Ohio, which means he would not be moving to suppress the use of the evidence in an Ohio court on the grounds that it had been obtained in violation of Ohio law. How, then, could an Ohio court apply its law to the search of the Ohio computer owned by Roe is so inclined?

The first step in analyzing this question is to examine the interests state courts consider in deciding whether to apply their heightened privacy guarantees to particular police conduct.[116] Because Roe is a not an Ohio citizen,[117] and because the search at issue was not conducted by Ohio officers, an Ohio court would presumably not apply the state's heightened privacy guarantees here, given the minimal potential effect that would have in deterring its officers from violating the Ohio Constitution.[118] And

---

[115] *See supra* notes 108–09 and accompanying text. To establish that Roe had a federal, Idaho, or Ohio constitutional right to privacy in the searched Ohio computer, this Article will assume he owns it. *See supra* note 106.

[116] *See supra* note 81 and accompanying text.

[117] Because Roe is not a citizen, and because the search at issue did not target him, personally, while he was "in" Ohio, it is difficult to see how he was "deprived" of the enhanced rights the Ohio Constitution confers on its citizens and others who are the targets of searches conducted in Ohio's territory. This, of course, assumes that the heightened protections of Ohio's constitution, and those of other Fourth Amendment-plus states, are only intended to apply (i) to their own citizens and/or (ii) to searches conducted "in" their states.

[118] States like Ohio (in this hypothetical) might have an interest in using civil or criminal liability to deter their officers from conducting or assisting in the conduct of searches that violate state law if they extend the heightened privacy guarantees their state constitution establishes to citizens of other states, as well as their own. As to why states might do this, some might essentially treat the greater privacy their state offers as a commodity to entice out-of-staters to store

because Ohio is not prosecuting Roe, applying the heightened requirements of its law to him would not promote the integrity of its judicial processes.[119]

But there might be circumstances that would prompt a Fourth Amendment-plus court to apply the state's heightened privacy guarantees to a version of this scenario. If the original scenario is modified so that Ohio officers assisted the Idaho officers who searched Roe's Ohio computer, Ohio might have an interest in seeing that its more rigorous law was applied so as to deter its officers from providing similar assistance in the future. If, alternatively, the scenario is modified so the Ohio computer is owned by an Ohio citizen who lets Roe use it, this would give Ohio more of a stake in the conduct at issue.[120] Ohio courts would presumably be more inclined to apply the state's heightened privacy guarantees if Ohio (or other Fourth Amendment-only state) officers, with the assistance of Ohio officers, searched a computer that was owned by an Ohio citizen and located in Ohio but (only) complied with the lesser requirements of Idaho law (and the Fourth Amendment).[121] Even though the prosecution in this hypothetical was brought in Idaho, an Ohio court might find that Ohio's interests in deterring its officers from engaging in activity that

---

data in and otherwise make use of the more security systems hosted in Ohio. *See generally* Daniel M. Laifer, Note, *Putting the Super Back in the Supervision of International Banking, Post-BCCI*, 60 FORDHAM L. REV. S467, S482 (1992) (noting that some countries used bank secrecy laws "to attract business").

If Ohio were to do this, it would probably want to ensure that its own officers were prohibited from engaging in conduct that subverted the availability of those guarantees to non-citizens, as well as citizens. *See generally* Treaty on Mutual Assistance in Criminal Matters Between the Swiss Confederation and the United States, U.S.-Switz., art. 3(1)(a), May 25, 1973, 27 U.S.T. 2019 (noting that Swiss authorities can refuse to assist officers from another country with a criminal investigation if doing so would "prejudice its sovereignty, security or similar essential interests"); *see also* James A. Kehoe, Recent Development, *Exporting Insider Trading Laws: The Enforcement of U.S. Insider Trading Laws Internationally*, 9 EMORY INT'L L. REV. 345, 364 (1995).

[119] *See supra* note 81 and accompanying text.

[120] It could also undermine Roe's claim to have had a cognizable private interest in the computer. *See supra* note 106.

[121] *See supra* Part II.B.

violated Ohio's law warranted applying Ohio law in this situation.[122]

These variations return to the question posed earlier: Because Roe is not being prosecuted in Ohio and therefore cannot file a motion to suppress in that state, how could one of Ohio's courts apply Ohio law to the conduct at issue? If Ohio law allowed individuals like Roe to file civil suits seeking redress for violations of Ohio law, and if Roe filed such a suit, an Ohio court would then be in a position to apply Ohio law to the variation of the original hypothetical in which Ohio officers assist with the search of Roe's Ohio computer.[123] The same should be true if Ohio made it a crime for its officers to violate Ohio constitutional law and if the officers involved in the search of Roe's computer were prosecuted under this law.[124]

Both options implicitly assume that some or all of the Fourth Amendment-plus states would be willing to extend the protections of their more rigorous law to non-citizens like Roe. This is not inconceivable: Fourth Amendment-plus states might find it is in their interest to extend their heightened privacy guarantees to citizens of other states, as well as their own, at least under certain circumstances. As to why they might do this, some or all of these states might essentially treat the greater privacy their law offers as a commodity to entice out-of-staters to store data in and otherwise make use of the higher security systems hosted on cloud computing systems located in their state.[125]

---

[122] *See supra* note 81 and accompanying text.

[123] *See, e.g.*, Dorwart v. Caraway, 58 P.3d 128, 131, 134–37 (Mont. 2002). *See generally* Binette v. Sabo, 710 A.2d 688, 693 (Conn. 1998) (creating cause of action for damages resulting from violation of search and seizure provisions of state constitution).

[124] *See generally* Commonwealth v. Stephens, 515 N.E.2d 606, 608–09 (Mass. App. Ct. 1987) (establishing that it is a crime to violate guarantees of state constitution); *see also supra* note 81.

[125] In other words, they would offer a digital version of bank secrecy. *See generally* Laifer, *supra* note 118 (noting that some countries used bank secrecy laws "to attract business").

States that adopted this approach would probably want to ensure that their law enforcement officers were effectively deterred from engaging in conduct that subverted the availability of this commoditized privacy to non-citizens, as well as citizens.[126] The civil or criminal liability postulated above would presumably be the only way they could do this, unless the state was prosecuting a non-citizen victim of such conduct, and their courts were in a position to grant a motion to suppress evidence obtained in violation of their Fourth Amendment-plus requirements.

The imposition of civil or criminal liability on officers by a Fourth Amendment-plus state like Ohio would promote the deterrence interests noted above, but it would not directly impact the out-of-state prosecution of a non-citizen like Roe, who is at least arguably the "victim" of the officers' malfeasance. In other words, the imposition of such liability would sanction the misconduct but would not give Roe any basis for having the fruits of that misconduct suppressed in his pending Idaho prosecution. Roe might be able to use the imposition of civil or criminal liability on the Ohio officers who participated in the search of the Ohio computer to gain some advantage in the prosecution Idaho has brought against him. Because the imposition of either type of liability would be predicated on a finding that the Ohio officers violated Ohio's search and seizure law, he could try to use that finding in a motion challenging the use of the evidence in his own state.

Roe might be able use the Ohio conviction or civil verdict to establish that the conduct of the officers violated Ohio law, and thereby preclude litigation of that issue in the Idaho prosecution.[127]

---

[126] *See* Kehoe, *supra* note 118. *See generally* Treaty on Mutual Assistance in Criminal Matters Between the Swiss Confederation and the United States, *supra* note 118, at art. 3(1)(a) (establishing that Swiss authorities can refuse to assist officers from another country with a criminal investigation if doing so would "prejudice its sovereignty, security or similar essential interests").

[127] This strategy can apply between civil and criminal proceedings. *See, e.g.*, People v. Trakhtenberg, No. 290336, 2011 WL 1902020, at *9 (Mich. Ct. App. May 19, 2011) ("Crossover estoppels, which involves the preclusion of an issue in a civil proceeding after a criminal proceeding and vice versa, is permissible." (quoting Barrow v. Pritchard, 597 N.W.2d 853, 856 (Mich. Ct. App.1999))).

But even if Roe were to succeed in doing this, there is certainly no guarantee, and perhaps no reason even to believe that the Idaho court would find the illegality of the Ohio officers' conduct a reason to grant Roe's motion to suppress evidence obtained by searching the Ohio computer.

2. *Fourth Amendment-plus and Fourth Amendment-trump States: Routine Dissonance*

The basic dynamic of rule dissonance should be the same for conflicts between Fourth Amendment-plus states and Fourth Amendment-trump states as it is for conflicts between Fourth Amendment-only states and Fourth Amendment-plus states.[128] The issue in both contexts is determining what, if any, significance a state's more rigorous search and seizure law has for evidence-gathering in and prosecution by a state with a lesser standard.

The primary difference between the scenarios examined in Part II.C.1 and those that involve conflicts between "plus" and "trump" states is that the standards involved in the latter all exceed the requirements of the Fourth Amendment. The conflicts between "plus" and "trump" states give rise to two types of dissonance: routine rule dissonance and a special case. This Part examines routine rule dissonance, while Part II.C.3 examines special case dissonance.

Because the Fourth Amendment's requirements are a constant in any analysis of search and seizure under U.S. law, they were implicitly subsumed into the analysis in Part II.C.1. That is, Fourth Amendment requirements were not a problematic element in the scenarios examined above; the problematic element was the

---

See generally 50 C.J.S. *Judgments* § 1218 (2012) ("In the context of a criminal case, collateral estoppel precludes relitigation of an issue decided, or necessarily determined, in the defendant's favor by a valid and final judgment.").

Assuming, as seems reasonable, that Idaho was not a party to the Ohio civil and/or criminal proceedings, Roe apparently could not use judgment in either of those cases or the findings of fact or conclusions of law issued as part of the judgment as collateral estoppel in the Idaho prosecution. *See, e.g.*, *Stephens*, 885 N.E.2d at 793–94. *But see* State v. Gonzalez, 380 A.2d 1128, 1131–32 (N.J. 1977).

[128] *See supra* Part II.C.1.

disconnect between the search and seizure laws of a state that follows the Fourth Amendment only and a state that adds additional requirements for searches and seizures that are conducted in its state (and, perhaps, involve its citizens).[129]

Therefore, insofar as the analysis of the hypotheticals in Part II.C.1 involved a conflict between "higher" and "lower" state standards, one should be able to extrapolate the results to conflicts between Fourth Amendment-plus states and Fourth Amendment-trump states. For the purposes of this analysis, it is assumed that a Fourth Amendment-plus standard is necessarily a less-demanding standard than a Fourth Amendment-trump standard. The latter, after all, categorically prohibits remote computer searches, while the former allows them as long as they comply with requirements that are somehow more rigorous than those imposed by the Fourth Amendment.

Part II.C.1 began the analysis by noting that no dissonance would arise when officers from one Fourth Amendment-only state conduct a remote search that targets a computer in another Fourth Amendment-only state because the states follow the same standard.[130] This could, but probably would not, be true of the Fourth Amendment-plus states: If the supreme courts of these states all adopted the same heightened requirements for the conduct of remote computer searches, then no dissonance would arise when officers from one of the twelve Fourth Amendment-plus states conducted a remote computer search in another of the states.[131]

If and when states adopt Fourth Amendment-plus standards that govern remote computer searches and other intrusions, it is likely that the standards will be idiosyncratic and provide varying degrees of protection. Therefore, to the extent that the standard of

---

[129] *See supra* Part II.C.1; *see also supra* note 117 and accompanying text.

[130] *See supra* Part II.C.1.

[131] State-to-federal dissonance would arise if a remote computer search was conducted "in" a Fourth Amendment-plus state by federal agents who (only) complied with the requirements of the Fourth Amendment. Judges in the state would presumably apply the analysis outlined in Part II.A to determine whether the evidence could be used in the local court.

one Fourth Amendment-plus state provides more protection than the standard adopted by other Fourth Amendment-plus states, dissonance of the type examined in Part II.C.1 is likely to arise. And because these scenarios, like the ones examined above, involve a conflict between "higher" and "lower" standards, the analysis in Part II.C.1 can be extrapolated to conflicts among Fourth Amendment-plus states.

While the Part II.C.1 analysis should generally be adequate to resolve dissonance between Fourth Amendment-plus and Fourth Amendment-trump states, the latter's rather draconian standard could give rise to an issue that does not arise in conflicts between Fourth Amendment-only and Fourth Amendment-plus states. While "only" and "plus" states both impose specific constitutional requirements on the conduct of remote computer searches, they do allow such searches to be conducted. That means the analysis focuses on mismatched standards, rather than on a conflict between a standard and an absolute prohibition. This difference could create special dissonance issues.

3. *Fourth Amendment-plus and Fourth Amendment-trump States: A Special Case?*

The conflict between a heightened standard and a prohibition might not be problematic, either conceptually or as applied, if the Fourth Amendment-trump states applied the prohibition to remote computer searches that were conducted by their own law enforcement officers, regardless of "where" the search occurred.[132] The officers from such a state—like Florida—would then be bound by their state's prohibition on remote computer searches regardless of whether the searches were conducted "in" State Y's territory or "in" the territory of another state.

This would limit, if not eliminate, the special dissonance that would arise if officers from a Fourth Amendment-trump state conducted a remote computer search of a computer in Fourth Amendment-plus Ohio. While this scenario is to some extent

[132] This, of course, is essentially the opposite of the approach the U.S. Supreme Court has taken with regard to the Fourth Amendment. *See supra* note 58 and accompanying text.

analogous to the conflicts examined in Part II.C.1, it differs in one notable respect: Here, the Florida officers are not simply searching a computer in another state without abiding by that state's more demanding laws; they are doing something they are categorically forbidden to do in their own state.

Why should that matter? How does that scenario differ from the "greater" or "lesser" dissonance examined in Part II.C.1? In a functional sense, and even in a conceptual sense, it probably does not; it is, after all, a conflict between a "greater" (prohibitory) and "lesser" ("only" or "plus") standard. Perhaps the differentiating factor here is that this scenario carries a hint of taint, a suggestion of hypocrisy. Florida has decided that remote computer searches are such a massive intrusion on individual privacy that it refuses to allow its officers to use them against its own citizens—but has no qualms about using them against citizens of other states.

In the scenarios analyzed in Part II.C.1, officers from an "only" state could conduct no-dissonance remote computer searches in a "plus" state if they complied with the latter's more rigorous search and seizure requirements (as well as with the Fourth Amendment).[133] Also, officers from a "plus" state could conduct a

---

[133] As to how they would go about doing this, assume the "only" state officers would simply, on an *ad hoc* basis, do their best to implement the "plus" state's heightened requirements. They presumably could not rely on a warrant issued by one of their own state judicial officers, because state court judges and magistrates can, at most, issue search warrants that are to be executed within the territory of the state they serve. *See* NEB. REV. STAT. § 29–812 (2006); *see also* ARK. CODE ANN. § 5-64-805(c) (2005); IND. CODE § 35-33-5-7(a) (2011); MO. ANN. STAT. § 542.286(1) (1974); Gattus v. State, 105 A.2d 661, 664 (Md. 1954) ("A search warrant cannot have extraterritorial effect.").

The "only" state officers might—if this were not unlawful—persuade one of their state magistrates to issue a warrant that authorized a remote search for and the seizure of evidence located in the "plus" state under conditions that would satisfy its law, on the theory that this would provide at least some "symbolic" legitimacy to the process. State judges and magistrates in most, if not all, states have the authority to issue warrants that authorize a search for evidence of a crime, the commission of which occurred partially in their state and partially in one or more other states. *See, e.g.*, ARK. CODE ANN. § 5-1-104(a) (2005); COLO. REV. STAT. ANN. § 18-1-201(1) (1971); GA. CODE ANN. § 17-2-1 (1968); WIS.

no-dissonance search in an "only" state if they complied with the Fourth Amendment and with the more rigorous requirements their state's law imposed on such searches.[134] It is therefore possible to eliminate dissonance in conflicts between "only" and "plus" states. The problem is that under existing law, officers are under no obligation to eliminate dissonance.[135] While the Supreme Court has noted that "ours is not a union of 50 wholly independent sovereigns," it has held that given the provisions of the Tenth Amendment, relations among the states are "purely a matter of comity."[136] In other words, like nation-states, U.S. states are sovereign enough that they do not have to apply each other's law.[137]

STAT. § 939.03(1) (2003); *see also* Waters-Pierce Oil Co. v. Texas, 212 U.S. 86, 109–11 (1909).

[134] As to why and how they might do this, *see supra* note 133 and accompanying text.

[135] In the scenarios above, neither group of officers is, arguably, required to comply with the "plus" state's more rigorous requirements because (i) state law only applies "in" a state's territory and (ii) it not clear where a remote search computer search occurs. *See supra* notes 107–108 and accompanying text. In the first scenario, then, the officers from the "only" state could argue that because they were in their state when they searched the computer in the "plus" state, the search occurred "in" their state, so they were only required to comply with the Fourth Amendment. *See supra* notes 107–108 and accompanying text. And in the second, the officers from the "plus" state could argue that because the computer they searched was in an "only" state, the search occurred "in" that state, which they were not required to comply with the more rigorous requirements of their own state's law. *See supra* notes 107–108 and accompanying text

[136] Nevada v. Hall, 440 U.S. 410, 425 (1979); *see* U.S. CONST. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States . . . ."). As one source notes, comity "is viewed not as a legal obligation but as a matter of mutual respect among sovereigns to consider each other's interests." Anthony J. Colangelo, *A Unified Approach to Extraterritoriality*, 97 VA. L. REV. 1019, 1036 n. 69 (2011); *see, e.g.*, Hilton v. Guyot, 159 U.S. 113, 163–64 (1895).

[137] *Hall*, 440 U.S. 410, 421–22; *see also* Donald Earl Childress III, *Comity as Conflict: Resituating International Comity as Conflict of Laws*, 44 U.C. DAVIS L. REV. 11, 17 (2010) (arguing that nation-states' law is "absolute" in their own territory).

The issues examined in Part II.C.1 and examined in this Part therefore go to the extent to which U.S. states are willing to respect the idiosyncratic laws of their counterparts, i.e., to comity. The Supreme Court has "presumed that the States" intend "to adopt policies of broad comity toward one another," but has made it clear that such policies are not something it can impose.[138] The no-dissonance searches hypothesized above that involve officers from an "only" state and from a "plus" state are examples of comity. The officers in these hypotheticals are under no legal obligation to apply the other state's law but do so out of a sense of comity (and, perhaps, to minimize objections to the use of the evidence they obtain in these searches).[139]

There does not appear to be a no-dissonance analog for Fourth Amendment-trump states. In the scenarios examined above, the officers from the "only" and "plus" states eliminated dissonance by applying the "plus" state's higher standards, even though they were at least arguably not required to do so.[140] It would be impossible for them to replicate this strategy for searches conducted in a "trump" state because the latter prohibits such searches.[141] Applying the "trump" state's law would mean they could not conduct the remote search, something their own states' laws allow. Dissonance would therefore be unavoidable (i) if officers from "only" and "plus" states remotely searched a computer in a "trump" state and (ii) if officers from a "trump" state remotely searched a computer in another state.[142]

If a "trump" state were to apply its prohibition on remote computer searches to other states, as well as its own, it would

---

[138] *Hall*, 440 U.S. at 425–26.

[139] *See supra* Part II.C.1.

[140] *See supra* note 135 and accompanying text.

[141] *See supra* Part II; *see also supra* note 135 and accompanying text.

[142] Dissonance would arise in the second scenario regardless of whether the state in which the search was conducted was an "only" state, a "plus" state or another "trump" state. As to the latter, if officers from one "trump" state conducted a remote computer search in another "trump" state, the search would violate the latter's prohibition on such searches.

eliminate the second category of dissonance noted above.[143] Its officers would then not be able to do what they cannot do in their own state, which would demonstrate that this "trump" state "respect[ed] the sovereignty" of other states.[144] The question is whether that would be reciprocated. The "trump" state would be surrendering its right to not apply its law outside the boundaries of its own territory—something, as discussed in Part II.C.1, states are not inclined to do. If other states did not adopt a reciprocal rule (i.e., did not agree to refrain from conducting remote computer searches in the "trump" state) the first category of dissonance would persist and would no doubt be a source of tension between this "trump" state and most, if not all, of the other states.

III. TRANSNATIONAL SEARCHES POTENTIAL FOR NATION-STATE DISSONANCE

As Part I explained, nation-state dissonance has occurred in at least one rather notorious instance: the Invita incident, in which Federal Bureau of Investigation agents remotely searched a computer server that was in Russia and that belonged to Russian citizens.[145] The Parts below survey the current and future prospects for remote computer searches in the United States and in Europe. Part III.A examines the prospects for remote searches in the United States and Part III.B examines the prospects for such searches in Europe.

A. *United States*

The FBI's search of the Russian computer generated controversy in the United States and elsewhere,[146] which may

---

[143] As noted above, a "trump" state could accomplish this by simply applying its law to remote computer searches conducted by its law enforcement officers, regardless of "where" the search occurred. *See supra* note 107 and accompanying text. This, as noted earlier, is essentially the opposite of the approach the U.S. Supreme Court has taken to the applicability of the Fourth Amendment. *See supra* note 48 and accompanying text.

[144] Nevada v. Hall, 440 U.S. 410, 425 (1979).

[145] *See supra* Part I.

[146] *See supra* Part I; *see, e.g.*, Robert Lemos, *FBI "Hack" Raises Global Security Concerns*, CNET NEWS (May 1, 2001, 12:05 PM), http://news.cnet.com

explain why U.S. law enforcement has not publicly pursued the use of remote computer searches. The FBI possesses and has used a remote data-gathering program for roughly the last decade.[147] Initially known as Magic Lantern, the program was renamed the Computer and Internet Protocol Address Verifier ("CIPAV").[148] The limited information that is available on the few known occasions in which CIPAV has been used indicate that it "is [used] only used after law enforcement officers have obtained a search warrant."[149] If that is true, it inferentially supports the proposition noted above: Remotely accessing a computer and extracting data from it is a "search" under the Fourth Amendment and must therefore be conducted in accordance with Fourth Amendment requirements.[150]

It appears the FBI is planning to become more aggressive in conducting remote computer searches. In May 2012, the FBI announced it had created a new unit, the purpose of which is to create new technologies that can more effectively intercept communications and, apparently, conduct remote computer searches.[151] Because the new unit is named the Domestic

---

/2100-1001-256811.html; *see also* Nicolai Seitz, *Transborder Search: A New Perspective in Law Enforcement?*, 7 YALE J. L. & TECH. 23, 33 (2004–05) ("[T]he permissibility of a transborder search . . . is currently the subject of controversial discussion.").

[147] *See, e.g.*, Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 400 (2010) (noting that the existence of Magic Lantern software was revealed in 2001).

[148] *See id.*; *see also* Nat Hentoff, *The FBI's Magic Lantern*, THE VILLAGE VOICE (May 2, 2002), http://www.villagevoice.com/2002-05-28/news/the-fbi-s-magic-lantern/1/.

[149] Soghoian, *supra* note 147 at 401; *see also* Benjamin Lawson, Note and Comment, *What Not to "Ware": As Congress Struggles against Spyware, the FBI Develops Its Own*, 35 RUTGERS COMPUTER & TECH. L.J. 77, 88–93 (2008).

[150] *See supra* notes 54–62 and accompanying text.

[151] *See, e.g.*, Declan McCullagh, *FBI Quietly Forms Secretive Net-surveillance Unit*, CNET NEWS (May 22, 2012), http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit/ (reporting that the president of a technology company that has worked with the Department of Justice said he "would expect that capabilities like CIPAV would be an example example" of what the new unit will do).

Communications Assistance Center, its involvement with remote computer searches will presumably not involve transnational searches.[152] If that is true, it also inferentially supports the proposition that U.S. law enforcement assumes remote searches must comply with the Fourth Amendment.[153]

The next Part examines the potential for dissonance to arise between nation-states, if and when their law enforcement agencies begin conducting transnational remote computer searches.

B. *Europe*

The following Parts will discuss the potential for dissonance between European Union ("E.U.")[154] member states.

1. *Presence of Remote Search Programs in European Countries*

In a press release issued at the end of 2008, the E.U. announced a new five-year plan to target cybercrime.[155] Among other things, it called for law enforcement officers in E.U. states to conduct "remote searches" of computers.[156] A few months earlier, the E.U. Council Presidency had distributed a note regarding a " '[c]omprehensive plan to combat cyber crime' to the representatives of each E.U. state."[157] It noted that there were

---

[152] *See id.*

[153] *See supra* notes 54–62 and accompanying text.

[154] The European Union is a unique economic and political partnership between 27 European countries that together cover much of the continent. *Basic Information on the European Union*, EUROPA, http://europa.eu/about-eu/basic-information/index_en.htm (last visited Nov. 24, 2012).

[155] *See* Press Release, Europa, Fight Against Cyber Crime: Cyber Patrols and Internet Investigation Teams to Reinforce the E.U. Strategy (Nov. 27, 2008), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827.

[156] *See id.*

[157] TONY BUNYAN, STATEWATCH, STATEWATCH ANALYSIS: E.U. AGREES RULES FOR REMOTE COMPUTER ACCESS BY POLICE FORCES—BUT FAILS, AS USUAL, TO MENTION—THE SECURITY AND INTELLIGENCE AGENCIES 2 (2009), *available at* http://www.statewatch.org/analyses/no-83-remote-computer-access.pdf. The Council of the European Union is the main decision-making body of the European Union. *See, e.g.*, Lesley Dingle & Bradley Miller, *A Summary of*

"projects already in existence" that required "common approaches," including "computer searches, which are a delicate issue because of their cross-border nature."[158] As one source noted, the reference to "projects already in existence" implied that agencies in at least some E.U. states were already conducting cross-border remote computer searches in their home countries and across borders in other states.[159]

The note became the basis of a proposal for formal Council Conclusions that initially called for "measures to facilitate remote computer searches," which would allow "investigators rapid access to data."[160] The final version of the Conclusions called for "facilitating remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country."[161]

Neither the initial press release nor the subsequent news stories explained what, precisely, these "remote searches" would involve, but there was a practical precedent for using such tactics. In 2006, a German attorney general sought a warrant from "the investigating judge of the federal court" that would authorize German police "to search a suspect's computer using an RFS [remote forensic tool]."[162] The application for the warrant sought

---

Recent Constitutional Reform in the United Kingdom, 33 INT'L J. LEGAL INFO. 71, 94 (2005).

[158] BUNYAN, *supra* note 157.

[159] *Id.*

[160] *Id.* (quoting COUNCIL OF THE EUROPEAN UNION, DRAFT COUNCIL CONCLUSIONS ON A CONCERTED WORK STRATEGY AND PRACTICAL MEASURES AGAINST CYBERCRIME, E.U. DOC. NO. 13567/08 (Sept. 26, 2008), *available at* http://register.consilium.europa.eu/pdf/en/08/st13/st13567.en08.pdf).

[161] COUNCIL OF THE EUROPEAN UNION, DRAFT COUNCIL CONCLUSIONS ON A CONCERTED WORK STRATEGY AND PRACTICAL MEASURES AGAINST CYBERCRIME, E.U. DOC. NO. 15569/08 at 5 (Nov. 11, 2008), *available at* http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf.

[162] *See, e.g.*, Wiebke Abel & Burkhard Schafer, *The German "Federal Trojan"—Challenges between Law and Technology*, TEUTAS LAW & TECH. (Mar. 2, 2009), http://www.teutas.it/societa-informazione/prova-elettronica/634-the-german-federal-trojan-challenges; *see also German Police Seeks Legal Permission for Online House Search*, SPAMFIGHTER (Mar. 14, 2007), http://www.spamfighter.com/News-7906-German-Police-Seeks-Legal-Permissio

permission to install the tool on the computer. Once installed, the tool would copy all data stored on the computer and then transfer it to the investigating authority for evaluation.[163]

When the judge declined to issue the warrant, the attorney general appealed to the federal court (the Bundesgerichtshof), which held that the warrant could not be issued because "no legal authorisation existed . . . under German law permitting the use of RFS tools . . . by law enforcement agencies."[164] Around the same time, another German state adopted legislation that authorized the use of remote computer searches (or remote forensic tools).[165] A complaint challenging the constitutionality of this legislation was filed with the German Federal Constitutional Court (the Bundesverfassungsgericht).[166] On February 27, 2008, the Federal Constitutional Court held that it violated the German Constitution and was consequently unlawful and unenforceable.[167]

---

n-for-Online-House-Search.htm.

[163] Abel & Schafer, *The German "Federal Trojan"*, *supra* note 162.

[164] *Id.*

[165] *Id.*; *see also German Police Seeks Legal Permission for Online House Search*, *supra* note 162.

[166] *See* Abel & Schafer, *The German "Federal Trojan"*, *supra* note 162.

[167] *See id.* The authors explain:

> The decision [of the German Federal Constitutional Court] was based on a "new" human right in the confidentiality and integrity of information technology systems, for the first time recognised explicitly by this court. The court . . . derived this right from the fundamental rights in personal dignity and personality rights under articles 2 I in connection with 1 I of the Constitution (Grundgesetz - GG). This right can only be restricted, and therefore the use of [remote] investigation tools by law enforcement agencies is only permissible, when significant higher-ranking fundamental values, such as the life and integrity of others, or liberty or common goods essential for human existence, are in danger. While this in principle leaves open the use of [such tools] to prevent an imminent terrorist attack, it could not be used to retrospectively investigate one, nor for general prevention of acts of terrorism in the absence of a specific, imminent and clearly identified threat . . . .

Id.

The remote forensic tools at issue in these cases apparently involved the use of Trojan Horse programs.[168] Trojan Horse programs seem to be at least one of the tools officers in Britain, another E.U. country, can use to carry out "intrusive surveillance" of certain suspects.[169] The Regulation of Investigatory Powers Act of 2000 ("RIPA") allows certain officials to authorize such surveillance.[170] An official cannot authorize intrusive surveillance unless he or she determines that it is necessary for any or all of the following reasons: (i) it is "in the interests of national security"; (ii) to prevent or detect "serious crime"; or (iii) it is "in the interests of the economic well-being of the United Kingdom."[171] Intrusive surveillance can be authorized even if it "includes conduct outside the United Kingdom."[172] According to the code of practice for conducting such surveillance, "[w]here action in another country is contemplated, the laws of the relevant country must also be considered."[173]

The RIPA defines intrusive surveillance as surveillance that is "carried out in relation to anything taking place on any residential premises" and "involves the presence of an individual on the premises . . . or is carried out by means of a surveillance device."[174]

---

[168] *See id.* (noting that either computer viruses or Trojan Horse programs could be used, but tend to emphasize the use of Trojan Horse programs). For more on the impact of the Federal Constitutional Court's ruling, see *infra* Part III.C.

[169] *See, e.g.*, Flora Graham, *Police "Encouraged" to Hack More*, BBC NEWS (Jan. 5, 2009), http://news.bbc.co.uk/2/hi/7812353.stm (reporting use of Trojan Horse programs).

[170] *See* Regulation of Investigatory Powers Act, 2000, c. 23 § 32(1) (Eng.) (defining the officials who can authorize searches as Secretary of State and senior authorizing officers). Intrusive surveillance is surveillance that concerns "anything taking place on any residential premises" and involves the use of "an individual on the premises" or "surveillance device." *Id.* § 26(3).

[171] *Id.* § 32(2) (referencing §32(3)).

[172] *Id.* at § 27(3).

[173] HOME OFFICE OF THE UNITED KINGDOM, COVERT SURVEILLANCE AND PROPERTY INTERFERENCE: REVISED CODE OF PRACTICE 10 (2010), *available at* http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert?view=Binary.

[174] Regulation of Investigatory Powers Act § 26(3).

Surveillance that is carried out "by means of a surveillance device" that is not "present on the premises" is not intrusive unless the device "provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises."[175]

In 2009, the BBC reported that the British Home Office "signed up to an E.U. strategy . . . that 'encourages' police . . . to remotely access personal computers" in order to combat cybercrime.[176] This is presumably the strategy outlined above.[177] The story noted that British police already had the ability to conduct such searches and were "carrying out a small number of these operations" each year.[178] It also noted that a spokesperson for the Home Office "said the E.U. agreement would not affect police behaviour and was not legally binding."[179]

It is unclear whether other members of the E.U. have also incorporated remote computer searches into their criminal procedure.[180] Some clearly have not, but an absence of evidence relating to such programs in other countries does not necessarily mean they do not exist.[181] Despite the lack of clear evidence, it seems likely that most E.U. countries have not been conducting such searches, and in many instances still are not using remote computer searches because the authority to conduct such searches currently does not exist under their national law.[182]

---

[175] *Id.* at § 26(5).

[176] Graham, *supra* note 169.

[177] *See supra* notes 169–173 and accompanying text.

[178] Graham, *supra* note 169.

[179] *See id.*

[180] *But see infra* Part III.C (discussing use of remote computer searches in one country).

[181] *See, e.g.*, Juan Carlos Ortiz Pradillo, *Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain*, 19 EURO J. OF CRIME, CRIM. L. & CRIM. JUST. 363, 377–81 (2011), *available at* https://ruidera.uclm.es/xmlui/bitstream/handle/10578/1662/fi_1318575944-ORTIZ%20PRADILLO%20the%20admissibility%20of%20remote%20searches%20in%20Spain%202011.pdf?sequence=1.

[182] *See supra* note 161 and accompanying text; *see infra* Part III.C.

2. *Potential for Dissonance in European Countries*

Notwithstanding the lack of data and present inability of other European countries to conduct remote computer searches, the potential for nation-to-nation rule dissonance with regard to the conduct of searches clearly exists as to the two countries examined above. As was shown, United Kingdom law allows British officers to conduct remote computer searches for any of the three purposes noted above.[183] German law does not allow such searches to be conducted to investigate crimes that have already been committed.[184] Because the Federal Constitutional Court derived this prohibition from its recognition of a new constitutional "right in the confidentiality and integrity of information technology systems,"[185] it is inferentially reasonable to assume that the court would apply the prohibition to law enforcement officers from other countries as well. In other words, it is reasonable to assume that under the Federal Constitutional Court's decision, Germany has in effect become a "trump" state—a state that outlaws remote investigative computer searches.[186]

If that assumption is correct, then it would seem to follow that if British officers conducted a remote computer search that targeted a computer located in Germany, there would, in effect, be dissonance between an "only" state and a "trump" state, with the resulting complications analyzed above.[187] A different type of rule

[183] *See supra* notes 169–173 and accompanying text.

[184] *See supra* notes 166–67 and accompanying text.

[185] *See supra* notes 166–67 and accompanying text.

[186] *See supra* Part II; *see also supra* note 167 and accompanying text. As noted earlier, the Federal Constitutional Court's ruling bars German officers from using remote computer searches to investigate crimes that have already been committed and also bars their use otherwise except insofar as certain "higher ranking fundamental values" are in peril. *See supra* note 167 and accompanying text. So while Germany has not yet adopted a categorical prohibition on the use of remote computer searches, it qualifies as a de facto "trump" state because the court's ruling bars the use of remote computer searches to investigate *ex post* criminal activity. *See supra* Part II.

[187] *See supra* Parts II.C.1–2. Britain might better be characterized as a "plus" state insofar as its requirements for the conduct of remote computer searches exceed those for the conduct of routine investigative searches. *See supra* Part II; *see also supra* notes 170–175 and accompanying text. If that characterization is

dissonance between an "only" state and a "trump" state could arise if the Federal Constitutional Court's ruling did not apply to German officers, so they could conduct remote computer searches targeting computers located in countries other than Germany.[188] That would presumably mean that German officers could conduct such searches of computers in Britain without complying with British law, which could also give rise to the other type of dissonance, and resulting complications, analyzed earlier.[189]

Given the number and diversity of nation-states in Europe, and the extent to which their citizens interact online and offline, it seems reasonable to believe that if and when European officers begin using remote computer searches, they will generate a notable quantum of rule dissonance.[190] Until recently, there was no reason to believe that such a development was in the offing, but, as Part III.C explains, that changed in spring 2012.

C. *Recent Developments in Remote Transnational Computer Searches*

In fall 2011, the Chaos Computer Club, described as "a German hacking organization,"[191] discovered that police from "at least five German states"[192] were using Trojan Horse software to

---

accurate, then there would be dissonance between a "plus" state and a "trump" state. *See supra* Parts II.C.1–2.

[188] Such an interpretation seems reasonable, given that the Federal Constitutional Court's decision was based on the recognition of a new right derived from the German Constitution. *See supra* notes 166–67 and accompanying text.

[189] *See supra* Parts II.C.1–2. Again, the dissonance might be better characterized as a conflict between a "plus" state and a "trump" state.

[190] The manifestation of that quantum of European-focused dissonance will only be exacerbated if and when federal or state law enforcement agencies from the United States begin to conduct remote computer searches that, at least on occasion, target computers that are in Europe and belong to European citizens. *See supra* notes 31–53 and accompanying text.

[191] *See, e.g.*, Nicholas Kulish, *Germans Condemn Police Use of Spyware*, N.Y. TIMES, Oct. 14, 2011, http://www.nytimes.com/2011/10/15/world/europe/uproar-in-germany-on-police-use-of-surveillance-software.html.

[192] John Leyden, *German States Defend Use of "Federal Trojan"*, THE REGISTER (Oct. 12, 2011), http://www.theregister.co.uk/2011/10/12/bundestroja

conduct remote computer searches.[193] The software let police remotely record "keystrokes, capture screenshots and activate cameras and microphones."[194] The software's use for investigative purposes therefore "exceeded the powers prescribed to the police by Germany's Federal Constitutional Court."[195] Officers in the five German states admitted using it to "monitor suspects' e-mails and phone calls over the Internet" and "captured tens of thousands of screenshots in cases involving theft, fraud, and illegal performance-enhancing drugs."[196]

---

ner/. The five identified states were Baden-Württemberg, Brandenburg, Schleswig-Holstein, Bavaria and Lower Saxony. *Id.* The German Federal police "denied using this specific Trojan." *Id.*; *see also* David Gordon Smith & Kristen Allen, *Electronic Surveillance Scandal Hits Germany*, SPIEGEL ONLINE (Oct. 10, 2011), http://www.spiegel.de/international/germany/the-world-from-berlin-electronic-surveillance-scandal-hits-germany-a-790944.html ("Interior Ministry denied that the software had been used by the Federal Criminal Police Office (BKA), which is similar to the American FBI.").

An interesting aspect of the Trojan Horse software used by the German states is that it "transmitted information via a server located in the US." Smith & Allen, *supra* note 192. That raises the possibility that the analysis of "where" a remote computer search could be a trichotomy, rather than a dichotomy. *See supra* note 107.

[193] *See, e.g.*, Kulish, *supra* note 191.

[194] *Id.*

[195] *Id. See also supra* Part III.B; *accord* Smith & Allen, *supra* note 192.

[196] Kulish, *supra* note 191. As to the origin of the Trojan Horse program(s) used by the German states:

> Documents . . . suggest that the German Customs Investigation Bureau purchased surveillance services from German software developer DigiTask valued at more than €2m. The same set of documents suggest that DigiTask develop a commercial Trojan intended for law enforcement called Skype Capture Unit.

Leyden, *supra* note 192; *see also* Daniel Schmitt, *Skype and the Bavarian Trojan in the Middle*, WIKILEAKS (Jan. 24, 2008), http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle. According to one source:

> German federal law allows the use of malware to eavesdrop on Skype conversations. But the [Chaos Computer Club] analysis suggests that the specific Trojan it wrote about is capable of a far wider range of functions than this—including establishing a backdoor on compromised machines and keystroke logging. The backdoor creates a means for third parties to hijack compromised machines, while the lack of encryption creates a mechanism for miscreants to plant false evidence.

These revelations brought "swift and strong" public condemnation, along with demands for an inquiry into the matter and legislation that would address the use of such tactics in searching and surveilling computers.[197] Experts, who were asked to comment on the German police's use of such tactics, said it would be increasingly necessary for governments to determine the extent to which they are willing to authorize remote computer searches.[198]

Then, in April 2012, the German government revealed that between 2008 and 2011, representatives from the FBI, the U.K.'s Serious Organised Crime Agency (SOCA), and France's secret service, the DCRI, were among those to have held meetings with German federal police about deploying "monitoring software" used to covertly infiltrate computers.[199]

The information the government released also suggested that German authorities were using other spyware in addition to the Trojan Horse program discovered by the Chaos Computer Club:

> German authorities had also acquired a license in early 2011 to test a similar Trojan technology called 'FinSpy,' manufactured by England-based firm Gamma Group. FinSpy enables clandestine access to a targeted computer, and was reportedly used for five months by Hosni Mubarak's Egyptian state security forces in 2010 to monitor personal Skype accounts and record voice and video conversations over the Internet.[200]

But what many found even more shocking was information a German Member of Parliament obtained from Secretary of State Ole Schroder:[201]

> [The] German federal police force, the Bundeskriminalamt (BKA), met to discuss the use of monitoring software with counterparts from the

---

Leyden, *supra* note 192.

[197] *See* Kulish, *supra* note 191.

[198] *Id.*

[199] *See* Ryan Gallagher, *U.S. and Other Western Nations Met with Germany over Shady Computer-Surveillance Tactics*, SLATE (Apr. 3, 2012), http://www.slate.com/blogs/future_tense/2012/04/03/bundestrojaner_finspy_u_s_officials_met_with_germany_to_discuss_computer_surveillance_.html.

[200] *Id.*

[201] *Id.*

> U.S., Britain, Israel, Luxemburg, Liechtenstein, the Netherlands, Belgium, France, Switzerland, and Austria. The meetings took place separately between Feb. 19, 2008, and Feb. 1, 2012 . . . . Both the FBI and Britain's SOCA are said to have discussed with the Germans the 'basic legal requirements' of using computer-monitoring software. The meeting with SOCA also covered the 'technical and tactical aspects' of deploying computer infiltration technology . . . . France's secret service and police from Switzerland, Austria, Luxemburg, and Liechtenstein were separately briefed by the BKA on its experiences using Trojan computer infiltration.[202]

Not surprisingly, no details have surfaced as to what was involved in the U.S., German, and British officers' discussions of the "basic legal requirements" involved in implementing remote computer searches. But given the challenges cyberspace creates for law enforcers, it is very likely that the officers focused on the issues examined in this Article: the rule dissonance that can result from transnational (or trans-state) computer searches and the complications that dissonance can create for officers and prosecutors. The goal was, almost certainly, to avoid the type of international friction that resulted from the FBI agents' essentially *ad hoc* action in the Invita case examined in Part I.

What is particularly interesting about this prolonged series of meetings is the secrecy with which they were conducted. One observer speculated that the accelerating use of cyberspace is creating a "shift in police tactics . . . that appears . . . to be taking place almost entirely behind closed doors and under cover of state secrecy."[203]

Unlike this author, some do not see the secrecy that apparently surrounds the use of remote computer searches as necessarily sinister.[204] The clandestine nature of the meetings noted above and, no doubt, other similar meetings is probably a function of pragmatic considerations. Law enforcement officers from various countries are grappling with the conflict that currently exists between the need to deploy "computer intrusion techniques that

---

[202] *Id.*

[203] *Id.*

[204] *See id.* (noting the need for "democratic scrutiny" of "highly intrusive [computer] surveillance technologies").

exist in a legal gray area" if they are to battle cybercrime effectively and the need to preserve individual privacy.[205]

IV. CONCLUSION

The meetings described in the previous Part were likely an attempt to address and resolve some of the issues examined above: the likelihood that remote computer searches will be categorically illegal in some U.S. states and nation-states, conditionally legal in others, and generally legal in still others.[206] It is likely that the meetings were to a great extent dedicated to identifying the dissonances that exist between the laws of the countries whose representatives were involved and attempting to identify ways in which avoid or minimize the impact the use of remote transnational computer searches could have on investigations and prosecutions. The need to avoid or minimize the presumptive or potential illegality of such searches advances the interests of law enforcement insofar as it addresses the issues noted above, i.e., the prosecution's ability to use the evidence obtained as the result of a remote transnational computer search. It also, at least to some extent, can reduce the type of international tension that arose in the Invita case, which was discussed in Part I.

Meetings such as these may be a modest first step toward reducing the rule dissonance among nation-states that can arise from remote transnational computer searches. Countries may, at some point, be able to take the next step and directly address these issues by adopting treaties that eliminate, or at least reduce the dissonance, associated with remote computer searches. In the interim, judges, lawyers, and law enforcement officers will probably have to rely on *ad hoc* tactics to minimize dissonance and its impact on particular cases and on relations among nation-states and subordinate states in federal systems like the United States.

---

[205] *Id.*; *accord.* Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659, 663–69 (2005) (discussing the challenges cybercrime creates for law enforcement); Brenner & Schwerha, *supra* note 28 at 347–54.

[206] *See supra* Parts III.A–B; *see also supra* Part II.