June 2, 2012

Law, Dissonance and Remote Computer Searches

Susan W. Brenner

Law, Dissonance and Remote Computer Searches

By

Susan W. Brenner[1]

[1]NCR Distinguished Professor of Law & Technology, University of Dayton School of Law, Dayton, Ohio USA. Email: susanwbrenner@yahoo.com

Table of Contents

I. Introduction

As authorities in Europe, the United States and elsewhere have recognized for well over a decade,[2] 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 come irrelevant, which is advantageous for law-breakers and disadvantageous for law enforcers.[3]

Unlike their traditional counterparts, a cybercriminal 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.[4] This vastly complicates law enforcement's task of finding the perpetrator and bringing him/her to justice; the criminal's use of cyberspace effectively fractures the crime into shards, which means relevant evidence is located in the territories of various nation-states.[5] Officers from the jurisdiction in which the victim was attacked therefore must conduct an investigation that differs from the parochial investigations with which police have historically dealt.[6]

As I have explained elsewhere, the methods law enforcement has traditionally used on the rare occasions when transnational evidence-gathering was necessary, are far too complicated and cumbersome to be effective in this context.[7] And in some instances, they may simply not be available, e.g., one country may not have a mutual legal assistance treaty with another.[8] This leaves the investigating officers with the Hobson's

---

[2]*See, e.g.*, Council of Europe, Convention on Cybercrime (ETS No. 185), Explanatory Report ¶¶ 131 – 137, http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm; Hollis Stambaugh, *et al.*, State and Local Law Enforcement Needs to Combat Electronic Crime, National Institute of Justice Research Brief 3-4 (2000).

[3]*See id. See also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security,* 10 B.U. J. Sci. & Tech. L. 1, 31-65 (2004).

[4]For more on this, *see, e.g.*, Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?,* 9 Va. J.L. & Tech 1, 6-7 (2004).

[5]For more on this, *see, e.g.*, Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare,* 97 J. Crim. L. & Criminology 379, 416 – 481 (2007).

[6]For more on this, see, e.g., Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security,* 10 B.U. J. Sci. & Tech. L. 1, 49-75 (2004).

[7]*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).

[8]*See id.* at 354-348. *See also infra* note 9. A mutual assistance legal treaty, or MLAT, is a "bilateral intergovernmental agreement that obliges foreign jurisdiction authorities to render assistance" in evidence gathering. Nicholas M. Mclean, *Cross-National Patterns in FCPA Enforcement,* 121 Yale L.J. 1970, 1987 (2012).

choice of ending their investigation or possibly violating foreign law in their efforts to obtain evidence.[9]

---

[9]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". United States v. Gorshkov, 2001 WL 1024026 *1 (W.D. Wash. 2002). 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. *See* U.S. Department of Justice, Russian Computer Hacker Convicted by Jury (October 10, 2001), http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm.

After one of the attackers identified himself as "Alexey Ivanov" and the FBI was able to confirm 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. *See* Ariana Eunjung Cha, *A Tempting Offer for Russian Pair*, Washington Post (May 19, 2003), http://www.washingtonpost.com/ac2/wp-dyn/A7774-2003May18?language=printer. The Russians did not respond to the initial contact or to a repeated request. *See id.* Since the United States does 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 U.S. made such a request. *See id. See also* James A. Wilson, *Extradition: The New Sword or the Mouse that Roared?*, 10-APR Antitrust Source 1, 4 (2011) (citing list of treaties in 18 U.S. Code § 3181).

Since 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. *See* Ariana Eunjung Cha, *A Tempting Offer for Russian Pair, supra.* They lured both Ivanov and his partner in cybercrime, Vasiliy Gorshkov, to Seattle to interview with a phony company: "Invita." *See id.* The men arrived in Seattle in November, 2000 and were met by an undercover agent, who took them to the "Invita" office. *See id.* There, agents posting 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. *See id.* 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 – their kontora's, or unofficial company's, server in Russia. *See* Brendan I. Koerner, *From Russia with LØPHT*, Legal Affairs (May-June 2002), http://www.legalaffairs.org/printerfriendly.msp?id=286. The server stored tools they needed for the hacking demonstration. After the demonstration was over, they were arrested. *See* Ariana Eunjung Cha, *A Tempting Offer for Russian Pair, supra*.

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. *See* Brendan I. Koerner, *From Russia with LØPHT, supra.* The agents did not let Russian authorities know what they were doing. *See id.* Gorshkov and Ivanov were subsequently indicted for violating federal cybercrime law and prosecutors prepared to use evidence from the tech.net.ru server at their trials. *See* United States v. Gorshkov, *supra*, at *1. *See also* United States v. Ivanov, 175 F.Supp. 2d 367, 368-270 (D. Conn. 2001).

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. *See* United States v. Gorshkov, *supra*, at *1 - *2. The district court held that the search did not violate the Fourth Amendment because it did not apply. *See id.* at *2 - *3. The Supreme Court has made it clear that the Fourth Amendment does not apply to searches and seizures "of a non-resident alien's property outside the United States." *See id.* at *3 (citing United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)). 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. *See id.*

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. *See* U.S. Department of Justice, Russian Computer Hacker Sentenced to Three Years in Prison (October 4, 2002),

Last year, I wrote an article in which I examined a likely law enforcement response to this evolving state of affairs: remote computer searches.[10] In it, I analyzed 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.[11]

I 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.[12] If I am correct in that assessment, 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 differs wildly from the searches with which the drafters of the Fourth Amendment were concerned. [13]

---

http://www.usdoj.gov/criminal/cybercrime/gorshkovSent.htm; U.S. Department of Justice, Russian Hacker Sentenced to Prison (July 25, 2003), http://www.usdoj.gov/usao/nj/press/files/iv0725_r.htm.

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. *See, e.g.*, *See, e.g.*, Mike Brunker, *FBI Agent Charged with Hacking*, MSNBC (August 15, 2002), http://www.msnbc.msn.com/id/3078784/. *See also* Federal Security Service of the Russian Federation, Government of the Russian Federation (2012), http://government.ru/eng/power/113/. Article 272 of the Russian Criminal Code makes "illegal accessing of computer information" a crime. Criminal Code of the Russian Federation, Article 272, http://legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview.

The charge was apparently symbolic -- a way to assert Russian sovereignty over persons and things in the territory Russia controls. In announcing it, 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'". *See* Mike Brunker, *FBI Agent Charted with Hacking*, *supra*. 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 U.S. has apparently never responded. *See, e.g.*, Ariana Eunjung Cha, *Despite U.S. Efforts, Web Crimes Thrive*, Washington 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*, Russia & FSU General News (October 20, 2002), 2002 WLNR 14527663.

[10]Susan W. Brenner, *Remote Computer Searches and The Use of Virtual Force*, 81 Mississippi Law Journal 1229 (2012). For a definition of remote computer searches, *see* § II(B), *infra.*

[11]*See* Susan W. Brenner, *Remote Computer Searches and the Use of Virtual Force*, *supra* note 10 at 1229-1246.

[12]*See id.* at 1246-1253.

[13]*See id.*

That, in and itself, should not 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: 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.[14] The Court found that "[t]here was no searching" because "[t]here was no entry" into Olmstead's home.[15] In reaching this conclusion, it relied on the proposition that the "`Fourth Amendment is to be construed in the light of what was deemed" a "search . . . when it was adopted.'"[16]

It was not until 1967 that the Court reversed itself held that it is a Fourth Amendment search for officers surreptitiously to listen to or record citizens' telephone conversations.[17] In the intervening years, since 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.[18] Given the empirical analogies between wiretapping and remotely searching a computer, I suspect the Court will hold that the latter also constitutes a Fourth Amendment search.

Therefore, for the purposes of this analysis I shall assume that for Fourth Amendment purposes, remote computer searches will be treated like more traditional searches. This means the default rule in the United 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. I suspect analogous rules will emerge elsewhere.

The default rule may not be the only one that emerges in this context. In the next section, I examine the possibility that dissonances will emerge in the rules that govern remote computer searches in the United States. In § III, I examine the possibility that similar dissonances will emerge in transnational searches.

II. United States: Federalism and Dissonance

The potential for the emergence of dissonant rules governing remote searches by U.S. law enforcement arises from the fact that the United States' federal system provides dual protection

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

[15]*See id.*

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

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

[18]*See, e.g.*, Goldman v. United States, 316 U.S. 129, 135 (1942).

> 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.[19]

Every U.S. state has its own constitution and "each of these constitutions includes . . . a `cognate' or `analog' to the Federal Fourth Amendment."[20] In the 1970s, some state supreme courts began to interpret their versions of the Fourth Amendment as providing more protection for privacy than the U.S. Constitution.[21] Over the ensuing decades, these states have increasingly departed from the federal courts' "narrow interpretation of the Fourth Amendment" to provide "more expansive protection of privacy" under their own constitutions, a trend one author suggests will only increase "with advances in technology."[22] The result is that (i) every search and/or seizure that is conducted in the United States or that is conducted by U.S. law enforcement officers and targets a U.S. citizen must comply with the requirements of the Fourth Amendment; and (ii) searches and/or seizures conducted in discrete states must comply with the Fourth Amendment and with any heightened requirements imposed by that state's law.[23]

And that brings us back to remote computer searches. For the purposes of analysis, we will assume 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 analogues of the Fourth Amendment [24]

---

[19]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. State of California, 386 U.S. 58, 62 (1967) (states have the "power to impose higher standards on searches and seizures than required by the Federal Constitution" if they choose to do so").

[20]Stephen H. 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).

[21]*See, e.g.*, Katharine Goodloe, *A Study in Unaccountability: Judicial Elections and Dependent State Constitutional Interpretations*, 753-755 (2011).

[22]Brian Andrew Suslak, *GPS Tracking, Police Intrusion, and the Diverging Paths of State and Federal Judiciaries*, 45 Suffolk U. L. Rev. 193, 194-195 (2011). I shall refer to these heightened requirements as "Fourth Amendment-plus" standards.

[23]*See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 283 n. 7 (1990) (Brennan, J., dissenting) (noting ""the 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, 280-281 (2d Cir. 974). *See also infra* note 27.

[24]I shall refer to these states as "Fourth Amendment-plus" states.

and (iii) sixteen other state supreme courts have held that remote computer searches are categorically unlawful under their state analogues of the Fourth Amendment.[25] 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.[26] Since U.S. state supreme courts cannot interpret their constitutions as providing *less* protection than the Fourth Amendment,[27] this exhausts the scenarios that can arise in this context.

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

A. Current U.S. Law

Scenarios (ii) and (iii) illustrate how dissonant rules can arise to complicate the application of our 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.[28]

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).[29] This is true regardless of whether the searches are conducted by local law enforcement officers, federal agents or officers from other states. Since the Fourth Amendment is a *de minimis* standard with which all U.S. law enforcement officers

[25]I shall refer to these states "Fourth Amendment-trump" states.

[26]I shall refer to these states as "Fourth Amendment-only states."

[27]*See* U.S. Constitution, art. VI, clause 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"). This proposition would prevent the remaining states from refusing to enforce the Fourth Amendment and/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).

[28]*See supra* § II.

[29]*See supra* § II. *See also* Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 1.5(c) (4th ed. 2011) ("there is no constitutional requirement that evidence obtained in another jurisdiction be suppressed merely because the process of acquisition offended some local law.

must comply,[30] rule dissonance should not become an issue in prosecutions brought in these states.[31] If officers from another state or federal agents use remote searches to obtain evidence from a computer in a Fourth-Amendment 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.[32]

In the twelve scenario (ii) 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 only satisfy the Fourth Amendment's requirements, the evidence will be suppressed as having been obtained in violation of the state constitution.[33]

The same may, or may not, be true if federal agents conduct remote searches in a scenario (ii) state but only comply 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.[34] Others have held that "evidence seized by federal agents, acting . . . in conformity with federal

---

[30]*See supra* note 27 & accompanying text.

[31]In § II(B), we will explore the possibility 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.

[32]*See, e.g.,* Mapp v. Ohio, 367 U.S. 643, 654-655 (1961).
[33]*See, e.g.,* State v. Mollica, 217 N.J.Super. 95, 99-100, 524 A.2d 1303, 1305-1306 (N.J. Super. – A.D. 1987), appeal granted and cause remanded, State v. Mollica, 114 N.J. 329, 554 A.2d 1315 (N.J. 1989).

[34]*See, e.g.,* State v. Cardenas-Alvarez, 130 N.M. 386, 393, 25 P.3d 225, 232 (N.M. 2001); State v. Rodriguez, 317 Or. 27, 36, 854 P.2d 399, 404 (Or. 1993). *Accord* State v. Torres, 125 Hawai'i 382, 397, 262 P.3d 1006, 1021 (Hawai'i 2011).

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, 116 N.M. 431, 446, 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, *supra,* 125 Hawai'i at 390-392, 262 P.3d at 1014-1016. *See also* Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 1.5(c) (4th ed. 2011).

The Hawai'i Supreme Court found that the exclusionary rule serves three principles: "judicial integrity, protection of individual privacy, and deterrence of illegal police misconduct." State v. Torres, *supra,* 125 Hawai'i at 394, 262 P.3d at 1018. *See also* Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 1.5(c) (4th ed. 2011). The *Torres* court found that the fact 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. State v. Torres, *supra,* 125 Hawai'i at 395, 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 Hawai'i law. State v. Torres, *supra,* 125 Hawai'i at 396, 262 P.3d at 1020. And it found that excluding evidence seized by Hawai'i officers in another state would deter the state's officers from engaging in such conduct in the future. State v. Torres, *supra,* 125 Hawai'i at 396, 262 P.3d at 1020.

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."[35] And some have applied this same principle to evidence seized by officers from another state on the theory that the "protections afforded by the constitution of a sovereign entity control the actions only of the agents of that sovereign entity." [36]

The states that only apply their constitutions to in-state law enforcement officers incorporate a qualifier into this principle: In searching for and seizing evidence, federal agents and/or 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.[37] 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,[38] but ado apply when federal agents or officers from another state act "as agents for the [local] state police". [39] When such an agency relationship exists, the federal

---

[35]Pena v. State, 61 S.W.3d 745, 754 (Tex. App. 2001). *See also* State v. Johnson, 75 Wash. App. 692, 699, 879 P.2d 984, 988 (Wash. App. 1994). 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." State v. Mollica, supra, 114 N.J. 329, 352, 554 A.2d 1315, 1328. *But see* State v. Torres, *supra,* 125 Hawai'i at 396, 262 P.3d at 1020 (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.,* State v. Torres, *supra,* 125 Hawai'i at 390, 262 P.3d at 1015. *See also infra* note 36 (silver platter doctrine).

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).

[36] State v. Mollica, *supra,* 114 N.J. at 347, 554 A.2d at 1324. This court explained that

> [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.

114 N.J. at 352, 554 A.2d at 1327. The courts in at least one state refer to this as the "silver platter doctrine." *See, e.g.,* State v. Ventress, 160 Wash. App. 1044, 2011 WL 1237644 *2 (Wash. App. 2011). In *Lustig v. United States,* 338 U.S. 74 (1949), the Supreme Court held that "evidence unlawfully obtained by state officers was admissible in federal court via a `silver platter.'" 338 U.S. at 78-79. In *Elkins v. United States,* 364 U.S. 206 (1960), 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." 364 U.S. at 223.

[37]*See, e.g.,* State v. Garcia-Navarro, 224 Ariz. 38, 40, 226 P.3d 407, 409 (Ariz. App. 2010); People v. Coleman, 227 Ill.2d 426, 439, 882 N.E.2d 1025, 1032 (Ill. 2008); Pena v. State, *supra* note 35, 61 S.W.3d at 754-755.

[38] Pena v. State, *supra* note 35, 61 S.W.3d at 754.

[39]*Id.* at 755.

agents or officers from another state "are subject to the constitutional standards applied to the local police," which means "evidence seized by [them] while operating in such capacity is subject to exclusion if not seized according to those standards."[40]

The same principles should apply to the scenario (iii) 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.

I have been unable to find any instance 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.[41] As I conceptualize a Fourth-Amendment-trump standard, it 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.[42] The same principle should also apply to officers from other states, as long as they were not acting as agents of the local police.[43]

---

[40]*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); United States v. Wright, 16 F.3d 1429, 1434 (6th Cir. 1994); United States v. Dudek, 530 F.2d 684, 689-690 (6th Cir. 1976). In other words, a federal court is not bound to suppress evidence obtained in violation of state law. *See, e.g.,* United States v. Dudek, *supra*, 530 F.3d at 689-690. *See also* Kenneth J. Melilli, *Exclusion of Evidence in State Prosecutions on the Basis of State Law,* 22 Ga. L. Rev. 667 (1988).

[41]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.,* Robert M. Bloom & Hillary Massey, *Accounting for Federalism in State Courts: supra* note 35 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* note 27 & accompanying text. This means 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 id.* Since 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.

[42]*See, e.g.,* State v. Cardenas-Alvarez, *supra* note 34, 130 N.M. at 393, 25 P.3d 232 ("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"). *But see supra* notes 39 & 40 & accompanying text.

[43]*See supra* notes 36 & 39 & accompanying text.

I include 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 our analysis of how dissonant rules can complicate the process of conducting remote computer searches. We take up that issue in the next section.

B. Remote Searches and Dissonance

Before we consider how dissonant rules can complicate remote computer searches, it is useful to define such searches. Literally, a remote computer search would involve law enforcement officers situated at Point A using the Internet to surreptitiously search the date on a computer located at Point B. So, 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 I do, that U.S. citizens and aliens in U.S. territory have a reasonable expectation of privacy in their hard drives.[44] The default rule postulated in § 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.[45] And as we saw in § 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.[46] Dissonance is an implicit possibility in the baseline formulation of remote computer searches, but is not inevitable.

To ensure dissonance *can* arise, we will from this point forward use a modified formulation of remote computer searches: We will assume that Point A, the place from

---

[44]*See, e.g.*, Commonwealth v. Cormier, 2011 WL 3450643 *4 (Mass. Super. 2011); Brackens v. State, 312 S.W.3d 831, 841 (Tex. App. 2009). Such an expectation of privacy does not exist if the hard drive's owner has "knowingly expose[d]" 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, 1204-1205 (10th Cir. 2008); United States v. Gabel, 2010 WL 3927697 (S.D. Fla. 2010). *See also* Katz v. United States, 389 U.S. 347, 351 (1967). *See also id.* at 361 (Harlan, J., concurring).

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, 268-272 (1990).

[45]*See* Susan W. Brenner, *Remote Computer Searches and the Use of Virtual Force*, *supra* note 10 at 1229-1246.

[46]*See supra* § II(A).

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 our purposes, a "sovereign state" is a nation-state,[47] a sovereign entity that is a constituent of a federal nation-state[48] or a confederation of nation-states.[49] Our only concern in the remainder of this section is with the constituent entities that comprise the United States: the fifty states plus the District of Columbia.[50] We will examine dissonance among nation-states in § III.

Section II postulated three scenarios. The original scenarios and the analysis in § 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.[51] The analysis of the scenarios in this section 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 sections below analyze the possibilities for dissonance in searches that involve states with inconsistent standards. We will assume, 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.[52]

---

[47]*See, e.g.*, D. Carolina Núnez, *Inside the Border, Outside the Law: Undocumented Immigrants and the Fourth Amendment*, 85 S. Cal. L. Rev. 85, (2011) nation-state is "is a unitary, self-contained actor with complete and exclusive jurisdiction over the people within its territory").

[48]*See, e.g.*, John Dinan, *Patterns of Subnational Constitutionalism in Federal Countries*, 39 Rutgers L.J. 837, 839 (2008) (federal states whose constituent states have their own constitutions include the United States, Argentina, German Federal Republic, Mexico, and Venezuela). *See also* U.S. Constitution amendment x.

[49]*See, e.g.*, Elisabetta Lanza, *Core of State Sovereignty and Boundaries of European Union's Identity in the Lissabon-Urteil*, 11 German L.J. 399, 405 (2010) (European Union is a "confederation of States" rather than a "Federal State").

[50]*See, e.g.*, Jo Anne Hagen, *An Overview of U.S. Import/Export Regulations – Part I, Exports*, 32-JUL Colo. Law. 75, 75 (2003) (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 supra* note 44, They are not incorporated into the analysis because the application of the Fourth Amendment and other principles of U.S. law is not as linear as it is for the U.S. states and the District of Columbia. *See, e.g.*, Ediberto Roman, *The Citizenship Dialectic*, 20 Geo. Immigr. L.J. 557, 586-588 (2006).

[51]*See supra* note 46 & accompanying text.

[52]*See supra* § II.

C. State-to-State Dissonance

This section 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.[53]

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, i.e., remote searches are constitutional if they are conducted in accordance with the Fourth Amendment.[54] This result holds regardless of 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 and/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.[55] Since these states apply the (for our purposes) *de minimis* Fourth Amendment standard,[56] 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 State X's officers remotely search a computer in Fourth Amendment-only State W. The officers provide the evidence so obtained to a State X prosecutor who seeks to admit it into evidence in the State X prosecution of John Doe, a State X resident who downloaded child pornography from the computer in State W. In conducting the remote computer search, the State X officers complied with the requirements of the Fourth Amendment

[53]*See supra* § II.

[54]*See id. See also* note 29 & accompanying text.

[55]*See supra* notes 30 - 32 & accompanying text.

[56]*See supra* note 30 & accompanying text.

and, in so doing, complied with the requirements of the State W constitution.[57] But they did not comply with the State X constitution's additional requirements.

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 State X constitution. Doe points out that he is a State X citizen and is therefore entitled to the protections of its constitution. Under State X 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.[58]

---

[57]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, we will assume, in the scenarios we examine from this point forward, that the officers who conducted the out-of-state search had a local search warrant that authorized the search. *See supra* § II. That is, we will assume the officers got a warrant that satisfied the Fourth Amendment before they conducted the remote search.

Since 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. Constitution Art. IV § 1 (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, 1227-1228 (1985).

While it is not clear if 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. 244, 299 (1970).

The issue in the *Nelson* case 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 225-227. 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., 367 P.3d 48, 50-53 (Nev. 2011). Since the exception has been relied on state courts, we will assume it applies in this contexts and nullifies the applicability of the full faith and credit clause.

[58]If the computer the officers searched belongs to someone other than Doe, the State X 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 State X constitution. If the computer belongs to someone else, Doe almost certainly would not have a Fourth Amendment expectation of privacy in it, and we will assume, for the purposes of analysis, that the same principle applies in State X constitutional analysis. *See, e.g.*, United States v. Angevine, 281 F.3d 1130, 1134-1135 (10th Cir. 2002); State v. M.A., 402 N.J. Super. 353, 368-369, 954 A.2d 503, 512 (N.J. Super. – A.D. 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 Fed. Appx. 895, 897 (11th Cir. 2011) (no Fourth Amendment expectation of privacy in computer shared with others); United States v. Ladeau, 2010 WL 1427523 *4 (D. Mass. 2010) (same).

For the purposes of analysis, we will assume that the State W computer which the State X officers searched belonged solely to Doe, that it was a computer he used for business he transacted in State W and that he

As far as I can determine, this issue has not yet arisen. If and when it does, I suspect 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 State X constitution.[59] If the computer the State X officers searched in State W belonged to a

---

was able to access it remotely from his home in State X. 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 State X's constitution.

[59]This argument raises questions about precisely where the search occurred. We are assuming that the State X officers were in State X when they searched the computer in State W. *See supra* § II(B) (modified formulation of remote computer searches). Did the search therefore occur (i) "in" State W because that is where the target of the search was located, (ii) "in" State X 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, 403-404 (5th Cir. 1996). If we apply that proposition to the Doe scenario, the "place" where the search occurred will not be dispositive, since it occurred in State W and in State X.

There is another possible argument as to why State X need not – and perhaps cannot -- apply its law to the search of the computer in State W: "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 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 defines 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 316-317 (citing U.S. Constitution amend. XIV, § 1; U.S. Constitution 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. Constitution Art. IV § 1. *See also supra* note 57.

This brings us back to the Doe case: The State X prosecutor could argue that, under the above principles, he cannot apply State X law to a search that occurred on the territory to 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, 83 Hawai'i 187, 196-199, 925 P.2d 357, 367-269 (Hawai'I 1996), overruled by State v. Torres, 125 Hawai'i 382, 397, 262 P.3d 1006, 1021 (Hawai'i 2011). *Cf.* State v. Davis, 313 Or. 246, 25, 834 P.2d 1008, 1012-1013 (Or. 1992).

In other words, the State X prosecutor would argue that State X would be unconstitutionally usurping the sovereign authority of State W by applying its search and seizure law to remote computer searches that target computers in the territory of State W. *See, e.g.*, Barry Latzer, *The New Judicial Federalism and Criminal Justice: Two Problems and a Response*, 22 Rutgers L.J. 836, 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 0f Out-Of-State*

State W citizen, that argument might prevail, because the heightened requirements of State X's constitution are presumably intended to protect State X citizens (only) and the defendant would not be a State X citizen.[60]

If the computer belongs to Doe,[61] he can argue that State X law should apply here because he is a State X citizen who is entitled to the heightened protections of its constitution, even with regard to out of state activity by State X officers who gathered evidence that would be used to prosecute him in State X.[62] Doe can argue that applying State X's constitutional requirements to the out-of-state activity by State X officers at issue here is consistent with the state supreme court's intention to put added constraints on the investigative tactics used by State X officers when they investigate State X citizens.[63]

Abortions?, *51 St. Louis U. L.J. 797*, 811 n. 31 (2007) ("the proposition that a state may not project its laws into other states . . . is bedrock in our federal system").

[60]*See, e.g.*, State v. Garcia, 147 N.M. 134, 148, 217 P.3d 1032, 1046 (N.M. 2009) ("it is imperative that our state constitution . . . protect the rights of our citizens"). *See also supra* note 58.

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 citizen is the target of a search that did not provide equivalent protection. *See supra* note 34. And as we saw earlier, courts also often consider deterrence in determining whether to apply heightened guarantees; Doe is a not a State X citizen, so the State X court might not be inclined to apply its heightened privacy guarantees to him in order to deter its officers from violating that aspect of State X law. *See id.*

In other words, State X has an interest in deterring its officers from violating its law when they are investigating State X citizens in State X, 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. State X *might* apply its heightened privacy requirements to Doe in order to ensure the integrity of its judicial processes (assuming a State X court would find that the conduct of out of state searches that do not target State X citizens threatens to undermine such integrity). *See id.*

[61]*See supra* note 58. In 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, I am assuming 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.

I am further assuming that his ownership of that space gives him 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, *Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, or Both?*, 28 Ga. St. U. L. Rev. 499, 509 (2012) (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").

[62]The argument as formulated above implicitly assumes that the search occurred only in State W. The argument would be strengthened if the court found that it occurred both in State X and in State X. *See supra* note 59.

[63]*See supra* note 34 & accompanying text.

He can also argue that if the court does not apply State X's constitutional requirements to out-of-state investigative activity of State X officers, it will undermine the deterrence rationale inherent in those requirements and thereby weaken the state's exclusionary rule.[64] (If, as noted above, the computer does not belong to Doe, it will be much more difficult for him to make these arguments successfully.[65])

Similar issues would arise if Richard Roe, a State W citizen, was prosecuted in State W based on evidence State W officers obtained by remotely searching a computer in State X. We will assume the State X computer belonged to Roe.[66] In conducting the search, the officers complied with the Fourth Amendment, which is all that State W's constitution requires. But they did not comply with the heightened requirements the State X constitution imposes on such searches. Roe moves to suppress the evidence as having been obtained in State X by methods that violate the State X constitution.

This scenario is essentially the converse of the Doe scenario: Doe, a State X citizen, was being prosecuted by State X authorities based on evidence State X officers searched for (and seized) from a computer in State W. In so doing, they complied (only) with State W's constitutional requirements, which provide less protection than those of State X's constitution. Doe's argument is arguably stronger than Roe's because Doe was being prosecuted in his own state (State X) by State X authorities based in part on evidence they (at least arguably) obtained by violating State X's constitutional law. The only dissonant component of the prosecution was that the State X 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 a State W citizen who is being prosecuted by State W authorities based in part on evidence State W officers obtained by remotely searching a computer in State X. Their search of the State X computer complied with the Fourth Amendment and therefore with the constitutional law of Roe's own state, but it did not comply with the heightened requirements of State X's constitution. Given all that, it is difficult to see how Roe can successfully argue that the search violated his rights under the U.S. constitution, State W's constitution or State X's constitution.[67]

Since the search of the computer complied with the Fourth Amendment, and with State W's constitutional requirements, Roe has no basis on which to suppress under the federal or State W constitutions. That leaves State X.

---

[64]*See supra* notes 34 and 35 & accompanying text.

[65]*See supra* note 58. *See also supra* note 60 & accompanying text.

[66]*See supra* note 61. *See supra* note 65 & accompanying text and note 58.

[67]*See supra* 60 & accompanying text. *See also supra* notes 63 - 64 & accompanying text. To establish that Roe had a federal, State W and/or State X constitutional right to privacy in the searched State X computer, we will assume he owns it. *See supra* note 58.

Roe, of course, is not being prosecuted by State X, which means he would not be moving to suppress the use of the evidence in State X court on the grounds that it had been obtained in violation of State X law. How, then, could a State X court apply its law to the search of the State X computer owned by Roe (assuming it was inclined to do so)?

The first step in analyzing this question is to consider the interests state courts consider in deciding whether to apply their heightened privacy guarantees to particular police conduct.[68] Since Roe is a not a State X citizen,[69] and since the search at issue was not conducted by State X officers, a State X court would presumably not apply the state's heightened privacy guarantees here, given the minimal (if any) effect that would have in deterring its officers from violating the State X constitution.[70] And since State X is not prosecuting Roe, applying the heightened requirements of its law to him would not promote the integrity of its judicial processes.[71]

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 we modify the original scenario, so that State X officers assisted the State W officers who searched Roe's State X computer, State X *might* have an interest in seeing that its more

---

[68]*See supra* note 34.

[69]Since Roe is not a citizen, and since the search at issue did not target him, personally, while he was "in" State X, it is difficult to see how he was "deprived" of the enhanced rights the State X constitution confers on its citizens and/or others who are the targets of searches conducted in State X's territory. This, of course, assumes that the heightened protections of State X's constitution, and that 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.

[70]*See id.*

States like State X might have an interest in using civil or criminal liability to deter their officers from conducting and/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 data in and otherwise make use of the more security systems hosted in State X. *See generally* Daniel M. Laifer, *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").

It State X 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* The Treaty on Mutual Assistance in Criminal Matters Between the Swiss Confederation and the United States, Article 3(1)(s), May 25, 1973, U.S.-Switz., 27 U.S.T. 2019 (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, *Exporting Insider Trading Laws: The Enforcement of U.S. Insider Trading Laws Internationally,* 9 Emory Int'l L. Rev. 345, 364 (1995).

[71]*See supra* note 34.

rigorous law was applied so as to deter its officers from providing similar assistance in the future. We return to this issue below.

If, alternatively, we modify our scenario so the State X computer is owned by a State X citizen who lets Roe use it, that would give State X more of a stake in the conduct at issue.[72] State X courts would presumably be more inclined to apply the state's heightened privacy guarantees if State W (or other Fourth Amendment-only state) officers, with the assistance of State X officers, searched a computer that was owned by a State X citizen and located in State X but (only) complied with the lesser requirements of State W law (and the Fourth Amendment).[73] Even though the prosecution in this hypothetical was brought in State W, a State X court might find that State X's interests in deterring its officers from engaging in activity that violated State X's law warranted applying State X law in this situation.[74]

That brings us back to the question posed earlier: Since Roe is not being prosecuted in State X and therefore cannot file a motion to suppress in that state, how could one of its courts apply State X to the conduct at issue?

If State X law allowed individuals like Roe to file civil suits seeking redress for violations of State X law, and if Roe filed such a suit, a State X court would then be in a position to apply State X law to the variation of the original hypothetical in which State X officers assist with the search of Roe's State X computer.[75] The same should be true if State X made it a crime for its officers to violate State X constitutional law and if the officers involved in the search of Roe's computer were prosecuted under this law.[76]

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 was 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

[72]It could also undermine Roe's claim to have had a cognizable private interest in the computer. *See supra* note 58.

[73]*See* § II(B), *supra.*

[74] *See supra* note 34.

[75]*See generally* Binette v. Sabo, 244 Conn. 23, 32, 710 A.2d 688, 693 (Conn. 1998) (creating cause of action for damages resulting from violation of search and seizure provisions of state constitution). *Accord* Dorwart v. Caraway, 58 P.3d 128, 131, 134-137 (Mont. 2002).

[76] *See generally* Com. v. Stephens, 25 Mass. App. Ct. 117, 120-121, 515 N.E.2d 606, 608-609 (Mass. App. 1987) (crime to violate guarantees of state constitution). *See also supra* note 9.

offers as a commodity to entice out-of-staters to store data in and otherwise make use of the more security systems hosted on cloud computing systems located in their state.[77]

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 commodified privacy to non-citizens, as well as citizens.[78] The civil and/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 and/or criminal liability on officers by a Fourth Amendment-plus state like State X 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 State W prosecution.

Roe *might* be able to use the imposition of civil or criminal liability on the State X officers who participated in the search of the State X computer to gain some advantage in the prosecution State W has brought against him. Since the imposition of either type of liability would be predicated on a finding that the State X officers violated State X'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 State X conviction or civil verdict to establish that the conduct of the officers violated State X law, and thereby preclude litigation of that issue in the State W prosecution.[79] But even if Roe were to succeed in doing this, there is no

---

[77]In other words, they would offer a digital version of bank secrecy. *See generally* Daniel M. Laifer, *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").

[78]*See generally* The Treaty on Mutual Assistance in Criminal Matters Between the Swiss Confederation and the United States, Article 3(1)(s), May 25, 1973, U.S.-Switz., 27 U.S.T. 2019 (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, *Exporting Insider Trading Laws: The Enforcement of U.S. Insider Trading Laws Internationally*, 9 Emory Int'l L. Rev. 345, 364 (1995).

[79]*See generally* 50 C.J.S. Judgments § 1218 ("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"). It can apply between civil and criminal proceedings. *See, e.g.*, People v. Trakhtenberg, 2011 WL 1902020 *9 (Mich. App. 2011) ("`[c]rossover estoppel, which involves the preclusion of an issue in a civil proceeding after a criminal proceeding and vice versa, is permissible'") (quoting *Barrow v. Pritchard*, 235 Mich. App. 478, 481, 597 N.W.2d 853, 856 (1999)).

If we assume, as seems reasonable, that State W was not a party to the State X civil and/or criminal proceedings, Roe apparently could not use judgment in either of those cases or the findings of fact or

certainly no guarantee, and perhaps no reason even to believe, that the State W court would find the illegality of the State X officers' conduct a reason to grant Roe's motion to suppress evidence obtained by searching the State X computer.

2. Fourth Amendment-"plus" and Fourth Amendment-"trump" States

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.[80] 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/or prosecution by a state with a lesser standard.

The primary difference between the scenarios we examined in § 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 sections below examine two aspects of dissonance between the search and seizure laws of these states: routine rule dissonance and a special case.

a. Routine Dissonance

Since 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 § II(C)(1). That is, Fourth Amendment requirements were not a problematic element in the scenarios examined above; the problematic element was the 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).[81]

Therefore, insofar as the analysis of the hypotheticals in § II(C)(1) involved a conflict between "higher" and "lower" state standards, it should be extrapolatable to conflicts between Fourth Amendment-plus states and Fourth Amendment-trump states. For the purposes of analysis, I shall assume that a Fourth Amendment-plus standard is necessarily a less-demanding standard than a Fourth Amendment-trump standard. The later, 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.

---

conclusions of law issued as part of the judgment as collateral estoppel in the State W prosecution. *See, e.g.*, Commonwealth v. Stephens, 451 Mass. 370, 379-380, 885 N.E.2d 785, 793-794 (Mass. 2008). *But see* State v. Gonzalez, 75 N.J. 181, 187-192, 380 A.2d 1128, 1131-1132 (N.J. 1977).

[80] *See supra* § II(C)(1). For more on this, *see infra* § II(C)(2)(a).

[81] *See supra* § II(C)(1). *See also supra* note 69.

I began the analysis in § II(C)(1) 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.[82] This could, but probably would not, be true of the Fourth Amendment-plus states: If these 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.[83]

Personally, I suspect that if and when states adopt Fourth Amendment-plus standards that govern remote computer searches and/or other intrusions, the standards will be idiosyncratic and provide varying degrees of protection. Therefore, to the extent that the standard of one Fourth Amendment-plus state provides more protection than the standard adopted by one or more other Fourth Amendment-plus state(s), dissonance of the type examined in § II(C)(1) is likely to arise. And since these scenarios, like the ones examined above, involve a conflict between "higher" and "lower" standards, the analysis in § II(C)(1) should be extrapolatable to conflicts among Fourth Amendment-plus states.

While the § 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 "trump" 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.

b. 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.[84] The officers from such a state – State Y, say – would then be bound by their state's prohibition on remote

[82]*See supra* § II(C)(1). *See also supra* notes 54 - 56 & accompanying text.

[83]*See supra* note 24 & accompanying text. 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 § II(A) to determine whether the evidence could be used in the local court.

[84]This, of course, essentially the opposite of the approach the U.S. Supreme Court has taken with regard to the Fourth Amendment. *See supra* note 9.

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 -- like State Y – conducted a remote computer search of a computer in Fourth Amendment-plus State X. While this scenario is to some extent analogous to the conflicts we examined in § II(C)(1), it differs in one notable respect: Here, the State Y 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"-"lesser" dissonance we examined in § 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, with it: State Y 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 we analyzed in § 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).[85] And officers from a "plus" state could conduct a 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.[86]

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

---

[85]As to why they might do this, *see infra* note 91 & accompanying text. As to how they would go about doing this, I 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. *See also* Ark. Code § 5-64-805(c); Ind. Code § 35-33-5-7(a); Mo. Stat. § 542.286(1). *See also* Gattus v. State, 204 Md. 589, 595, 105 A.2d 661, 664 (Md. 1954) ("A search warrant cannot have extraterritorial effect").

The "only" state officers might – if this was 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 § 5-1-104(a); Colo. Rev. Stat. § 18-1-201(1); Ga. Code Ann. § 17-2-1; Wis. Stat. § 939.03(1). *See also* Waters-Pierce Oil Co. v. State of Texas, 212 U.S. 86, 109-111 (1909).

[86]As to why and how they might do this, *see id.*

eliminate dissonance.[87] 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."[88] In other words, like nation-states, U.S. states are sovereign enough that they do not have to apply each other's law.[89]

The issues we examined in § II(C)(1) and are examining in this section 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 this is not something it can impose.[90]

The no-dissonance searches hypothesized above that involve officers from an "only" state and from a "plus" state are an example 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).[91]

There does not appear to be a no-dissonance analogue for Fourth Amendment-trump states. In the scenarios we 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.[92] It would be impossible for them to replicate this strategy for searches conducted in a "trump" state because the latter

---

[87]In the scenarios above, neither group of officers is, at least 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 59 - 60 & accompanying text, *supra.* In the first scenario, then, the officers from the "only" state could argue that since 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 id.* 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 id.*

[88]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, 163-164 (1895).

[89]Nevada v. Hall, *supra* note 88 at 421-422. *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) (nation-states' law is "absolute" in their own territory).

[90]Nevada v. Hall, 440 U.S. 410, 425-426 (1979).

[91]*See supra* § II(C)(1).

[92]*See supra* note 87.

prohibits such searches.[93] 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.[94]

If a "trump" state were to apply its prohibition on remote computer searches to other states, as well as its own, this would eliminate the second category of dissonance noted above.[95] 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.[96] The question is whether that would be reciprocated: The "trump" state would be surrendering its right to not to apply its law outside the boundaries of its own territory, something, as we saw in § 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.

The next section examines dissonance among nation-states.

III. Transnational Searches: Potential for Nation-State Dissonance

As noted earlier, nation-state dissonance has occurred in at least one, rather notorious instance: In 2000, agents of the Federal Bureau of Investigation remotely searched a computer server that was in Russia and belonged to Russian citizens.[97] They extracted data from the computer and downloaded it to their own, after which it was used to prosecute two Russian citizens for committing cybercrimes in the United States.[98] The Russians tried to suppress the seized data as having been obtained in violation of the Fourth Amendment, but lost, because the Supreme Court has held that the Fourth

---

[93]*See supra* § II. *See also supra* note 87.

[94]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.

[95]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 59 & 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 9.

[96]Nevada v. Hall, *supra* note 90 at 425.

[97]*See supra* note 9.

[98]*See id.*

Amendment does not apply to searches that are conducted outside U.S. territory and that do not impact on U.S. citizens.[99]

The sections below survey the current and future prospects for remote computer searches in the United States and in Europe. The first section examines the prospects for remote searches in the United States and the second 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,[100] which may explain why U.S. law enforcement, at least, has not publicly pursued the use of remote computer searches. The FBI has had, and used, a remote data-gathering program for roughly the last decade.[101] Initially known as Magic Lantern, the program was renamed the Computer and Internet Protocol Address Verifier, or CIPAV.[102]

The limited information that is available on the few known occasions in which CIPAV has been used indicate that it "is only used after law enforcement officers have obtained a search warrant."[103] If that is true, it inferentially supports the proposition noted above, i.e., that remotely accessing a computer and extracting data from it is a "search" under the Fourth Amendment and must therefore be conducted in accordance with its requirements.[104]

It appears the FBI is planning to become more aggressive in conducting remote computer searches: In May of 2012, the Bureau announced it had created a new unit, the purpose of which is to create new technologies that can more effectively intercept

---

[99]*See id.*

[100]*See, e.g.,* Robert Lemos, *FBI "Hack" Raises Global Security Concerns,* CNET (May 1, 2001), http://news.cnet.com/2100-1001-256811.html. *See also* Nicolai Seitz, *Transborder Search: A New Perspective in Law Enforcement?,* 7 Yale J. L. & Tech. 23, § II(A) (2004-2005) ("the permissibility of a transborder search . . . is currently the subject of controversial discussion").

[101]*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) (FBI revealed existence of Magic Lantern software in 2001).

[102]*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/.

[103]Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era, supra* note 101at 401. *See also* Benjamin Lawson, *What Not to "Ware": As Congress Struggles against Spyware, the FBI Develops Its Own,* 35 Rutgers Computer & Tech. L.J. 77, 88-93 (2008).

[104]*See supra* notes 11 - 12 & accompanying text.

communications and, apparently, conduct remote computer searches.[105] Since the new unit is named the Domestic Communications Assistance Center, its involvement with remote computer searches will presumably not involve transnational searches.[106] If that is true, it also inferentially support the proposition that U.S. law enforcement assumes remote searches must comply with the Fourth Amendment.[107]

The next section 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

In a press release issued at the end of 2008, the European Union[108] ("EU"} announced a new five-year plan to target cybercrime.[109] Among other things, it called for law enforcement officers in EU states to conduct "remote searches" of computers.[110]

A few months earlier, the EU Council Presidency had "circulated a Note on a: `Comprehensive plan to combat cyber crime'" to the representatives of each EU state.[111] It noted there were projects "already in existence" that required "`common approaches", including "`computer searches, which are a delicate issue because of their cross-border nature.'" As one source noted, the reference to "projects already in existence" implied

---

[105]*See, e.g.*, Declan McCullagh, *FBI Quietly Forms Secretive Net-surveillance Unit*, CNET (May 22, 2012), http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit/. 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'" of what the new unit will do. *Id.*

[106]*See id.*

[107]*See supra* note 104 & accompanying text.

[108]The European Union is "a unique economic and political partnership between 27 European countries that together cover much of the continent." About the European Union, Europa, http://europa.eu/about-eu/basic-information/index_en.htm.

[109]*See Fight against Cyber Crime: Cyber Patrols and Internet Investigation Teams to Reinforce the EU Strategy*, Press Release – Europa (November 27, 2008), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827/ .

[110] *See id.*

[111]Tony Bunyan, *EU Agrees Rules for Remote Computer Access by Police Forces – But Fails, as Usual, to Mention – the Security and Intelligence Agencies* 2, Statewatch Bulletin January-Marcy 2009), 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 Recent Constitutional Reform in the United Kingdom*, 33 Int'l J. Legal Info. 71, 94 (2005).

that agencies in at least some EU states were already conducting cross-border remote computer searches in their home countries and across borders in other states.[112]

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'".[113] 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".[114]

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]".[115] The application for the warrant sought permission to install the tool on the computer; once installed, it would "copy all data stored on the computer and . . . transfer it back to the investigating authority for evaluation."[116]

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 issue because "no legal authorisation existed . . . under German law permitting the use of RFS tools . . . by law enforcement agencies."[117] Around the same time, another German state adopted legislation that authorized the use of remote computer searches (or remote forensic tools).[118] A complaint challenging the constitutionality of this legislation was filed with the German Federal Constitutional Court (the

---

[112]*Id.*

[113]*Id.* (quoting (EU document number 13567/08).

[114]Draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, EU doc. No. 1559/08 at 5, Council of the European Union (November 11, 2008), http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf.

[115]*See, e.g.*, Wiebke Abel & Burkhard Schafer, *The German "Federal Trojan" – Challenges between Law and Technology*, Teutas Law & Technology (March 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 (March 14, 2007), http://www.spamfighter.com/News-7911-German-Police-Seeks-Legal-Permission-for-Online-House-Search.htm.

[116]Wiebke Abel & Burkhard Schafer, *The German "Federal Trojan", supra* note **Error! Bookmark not defined.**.

[117]*Id.*

[118]Wiebke Abel & Burkhard Schafer, *The German "Federal Trojan", supra* note **Error! Bookmark not defined.**. *See also German Police Seeks Legal Permission for Online House Search*, SpamFighter (March 14, 2007), http://www.spamfighter.com/News-7911-German-Police-Seeks-Legal-Permission-for-Online-House-Search.htm.

Bundesverfassungsgericht).[119] On February 27, 2008, the Federal Constitutional Court held that it violated the German Constitution and was consequently unlawful and unenforceable.[120]

The "remote forensic tools" at issue in these cases apparently involved the use of Trojan horse programs.[121] Trojan horse programs seem to be at least one of the tools officers in Britain, another EU country, can use to carry out "intrusive surveillance" of certain suspects.[122] The Regulation of Investigatory Powers Act of 2000 ("RIPA") allows certain officials to authorize such surveillance.[123]

An official cannot authorize intrusive surveillance unless he/she determines that it is necessary (i) "in the interests of national security"; (ii) to prevent or detect "serious crime"; or (iii) "in the interests of the economic well-being of the United Kingdom."[124] Intrusive surveillance can be authorized even if it "includes conduct outside the United Kingdom."[125] According to the code of practice for conducting such surveillance,

---

[119]*See* Wiebke Abel & Burkhard Schafer, *The German "Federal Trojan", supra* note 115.

[120]*See id.* As these authors explain, the German Federal Constitutional Court's decision 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.

[121]*See id.* The authors note 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* § III(C).

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

[123]*See* Regulation of Investigatory Powers Act 2000 c. 23 Pt. 22 § 32(1) ("Secretary of State and . . . senior authorising 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." Regulation of Investigatory Powers Act 2000 c. 23 Pt. 22 § 26(3).

[124]Regulation of Investigatory Powers Act 2000 c. 23 Pt. 22 § 32(2).

[125]Regulation of Investigatory Powers Act 2000 c. 23 Pt. 22 § 27(3).

"[w]here action in another country is contemplated, the laws of the relevant country must also be considered."[126]

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." [127] 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". [128]

In 2009, the BBC reported that the British Home Office "signed up to an EU strategy that `encourages' police . . . to remotely access personal computers."[129] This is presumably the strategy outlined above.[130] 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.[131] It also noted that a spokesperson for the Home Office "said the EU agreement would not affect police behaviour and was not legally binding."[132]

I cannot find any information as to whether other members of the EU have also incorporated remote computer searches into their criminal procedure.[133] Some clearly have not.[134] My suspicion, and it is just that, is that most EU countries have not been, 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.[135] We return to that issue in § III(C), *infra.*

---

[126]Home Office of the United Kingdom, Covert Surveillance and Property Interference: Revised Code of Practice 10 (2010), http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert?view=Binary.

[127]Regulation of Investigatory Powers Act 2000 c. 23 Pt. 22 § 26(3).

[128]Regulation of Investigatory Powers Act 2000 c. 23 Pt. 22 § 26(5).

[129]Flora Graham, *Police "Encouraged" to Hack More, supra* note 122.

[130]*See supra* notes 109 - 114 & accompanying text.

[131]Flora Graham, *Police "Encouraged" to Hack More, supra* note 122.

[132]*See id.*

[133]*But see infra* § III(C).

[134]*See, e.g.,* Juan Carlos Ortiz Pradillo, *Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain*, 19 Criminal Law and Criminal Justice 363, 377-381 (2011), https://ruidera.uclm.es/xmlui/bitstream/handle/10578/1662/fi_1318575944-ORTIZ%20PRADILLO%20the%20admissibility%20of%20remote%20searches%20in%20Spain%202011.pdf?sequence=1.

[135]*See* note 114 & accompanying text, *supra.*

Notwithstanding the lack of data on and/or 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 we saw, United Kingdom law allows British officers to conduct remote computer searches for any of the three purposes noted above.[136] German law does not allow such searches to be conducted to investigate crimes that have already been committed.[137]

German law clearly prohibits German officers from conducting remote searches in order to investigate such crimes. Since the Federal Constitutional Court derived this prohibition from its recognition of a new constitutional "right in the confidentiality and integrity of information technology systems,"[138] it is inferentially reasonable to assume 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, i.e., a state that outlaws remote investigative computer searches.[139]

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, we would, in effect, have dissonance between an "only" state and a "trump" state, with the resulting complications analyzed above.[140] A different type of rule 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 remote computer searches targeting computers located in countries other than Germany.[141] That would (presumably) mean German officers could conduct such searches of computers in Britain without complying

[136]*See supra* note 124 & accompanying text.

[137]*See supra* note 120 & accompanying text.

[138]*See id.*

[139]*See supra* § II. *See also supra* note 120 & 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 120. 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* § II.

[140]*See supra* §§ II(C)(1) & II(C)(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* § II. *See also supra* notes 123 - 128 & accompanying text. If that characterization is accurate, then we would have dissonance between a "plus" state and a "trump" state. *See supra* §§ II(C)(1) & II(C)(2).

[141]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* note 138 & accompanying text.

with British law, which could also give rise to the other type of dissonance, and resulting complications, analyzed earlier.[142]

Given the number and diversity of nation-states in Europe, and the extent to which their citizens interact on- and off-line, 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.[143] Until recently, there was no reason to believe that such a development was in the offing, but, as the next explains, that changed in the spring of 2012.

IV. Conclusion

In the fall of 2011, the Chaos Computer Club, described as "a German hacking organization,"[144] discovered that police from "at least five German states"[145] were using Trojan Horse software to conduct remote computer searches.[146] It let police remotely record "keystrokes, capture screenshots and activate cameras and microphones."[147]

---

[142]*See supra* §§ II(C)(1) & II(C)(2). Again, the dissonance might be better characterized as a conflict between a "plus" state and a "trump" state. *See supra* note 140.

[143]The manifestation of that quantum of European-focused dissonance will only be exacerbated if and when federal and/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, e.g., supra* note 9.

[144] *See, e.g.*, Nicholas Kulish, *Germans Condemn Police Use of Spyware*, New York Times (October 14, 2011), http://www.nytimes.com/2011/10/15/world/europe/uproar-in-germany-on-police-use-of-surveillance-software.html.

[145]John Leyden, *German States Defend Use of "Federal Trojan,"* The Register (October 12, 2011), http://www.theregister.co.uk/2011/10/12/bundestrojaner/. 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 (October 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." David Gordon Smith & Kristen Allen, *Electronic Surveillance Scandal Hits Germany, supra.* That raises the possibility that the analysis of "where" a remote computer search could be a trichotomy, rather than a dichotomy. *See supra* note 59.

[146]*See, e.g.*, Nicholas Kulish, *Germans Condemn Police Use of Spyware, supra* note 144.

[147]Nicholas Kulish, *Germans Condemn Police Use of Spyware, supra* note 144.

The software's use for investigative purposes therefore "exceeded the powers prescribed to the police by Germany's Federal Constitutional Court."[148] 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." [149]

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.[150] Experts who were asked to comment on the German police's use of such tactics said it "will increasingly be necessary" for government "across the globe" to determine the extent to which they are willing to authorize remote computer searches.[151]

Then, in April of 2012, the German government revealed that

> between 2008-2011, 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.[152]

---

[148]*Id. See also supra* § III(B). *Accord* David Gordon Smith & Kristen Allen, *Electronic Surveillance Scandal Hits Germany, supra* note 145.

[149]*Id.* As to the origin of the Trojan Horse program(s) used by the German states, *see, e.g.*, John Leyden, *German States Defend Use of "Federal Trojan," supra* note 145:

> 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.

See also Daniel Schmitt, *Skype and the Bavarian Trojan in the Middle*, Wikileaks (January 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.

John Leyden, *German States Defend Use of "Federal Trojan," supra* note 145. *But see supra* note 148 & accompanying text (German states' use of the Trojan Horse program violated German law).

[150]*See id.*

[151]*See id.*

[152]*See* Ryan Gallagher, *U.S. and Other Western Nations Met with Germany over Shady Computer-Surveillance Tactics,* Slate (April 3, 2012),

The information the government released also revealed that in addition to using the Trojan Horse program discovered by the Chaos Computer Club – the Bundestrojaner – 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.[153]

But what many found even more shocking was information a German Member of Parliament obtained from Secretary of State Ole Schroder.[154] In a letter to the Member of Parliament, Shroder explained that the

> German federal police force, the Bundeskriminalamt (BKA), met to discuss the use of monitoring software with counterparts from the 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.[155]

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 very likely that they focused on the issues examined in this article, i.e. the rule dissonance that can result from transnational (or trans-state) computer searches and the complications that dissonance can create for officers and prosecutors.

---

http://www.slate.com/blogs/future_tense/2012/04/03/bundestrojaner_finspy_u_s_officials_met_with_germany_to_discuss_computer_surveillance_.html.

[153]*Id.*

[154]*See id.*

[155]*Id.*

What is particularly interesting about this prolonged series of meetings is the secrecy with which they were conducted. One observer speculated that our 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.'[156] Unlike this author, I do not see the secrecy as necessarily sinister.[157]

I ascribe the clandestine nature of the meetings to pragmatic considerations, i.e., to the fact that law enforcement officers from many nations are grappling with the ever-increasing need to deploy "computer intrusion techniques that exist in a legal gray area" if they are to battle cybercrime effectively.[158] More precisely, I think the meetings were an attempt to address, and perhaps resolve, some, if not all, of the issues we examined above, i.e., the likelihood that remote computer searches will be categorically illegal in some countries, conditionally legal in others and generally legal in still others.[159] I suspect 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 on investigations and prosecutions.

Meetings like these might be a modest first step toward reducing rule dissonance among nation-states. Countries may, at some point, be able to address these issues by adopting treaties that eliminate, or at least reduce the rule 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.

---

[156]*See id.*

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

[158]*Id.* As to the challenges cybercrime creates for law enforcement, *see, e.g.*, Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. Marshall J. Computer & Info. L. 659, 663-669 (2005). *See also* Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, *supra* note 7 at 347-354.

[159]*See supra* § III(A)-(B). *See also supra* § II.