Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the *Microsoft Ireland* Case the "Next Frontier"?

—

Collecte transfrontalière de preuves dans les enquêtes pénales transnationales: l'affaire *Microsoft Ireland* dessine-t-elle la "prochaine frontière"?

ROBERT J. CURRIE

Abstract

A recent and prominent American appeals court case has revived a controversial international law question: can a state compel a person on its territory to obtain and produce material that the person owns or controls, but which is stored on the territory of a foreign state? The case involved, *United States v Microsoft*, features electronic data stored offshore that was sought in the context of a criminal prosecution. It highlights the current legal complexity surrounding the cross-border gathering of electronic evidence, which has produced friction and divergent state practice. The author here contends that the problems involved are best understood — and potentially resolved — via an examination through the

Résumé

Un arrêt récent d'une importante instance d'appel américaine a relancé une question de droit international controversée: un État peut-il obliger à une personne sur son territoire d'obtenir et de produire du matériel qui lui appartient ou qu'il contrôle, mais qui est stocké sur le territoire d'un État étranger? L'affaire en question, *États-Unis c Microsoft*, traite de données électroniques stockées à l'étranger et recherchées dans le cadre d'une poursuite pénale. Elle souligne la complexité juridique actuelle entourant la collecte transfrontalière de preuves électroniques, ce qui a généré des frictions et une pratique divergente entre les États. L'auteur affirme que les problèmes impliqués sont mieux compris — et

Robert J. Currie, Schulich School of Law, Dalhousie University, Halifax, Canada. This article originated as a presentation made at the annual conference of the International Society for the Reform of Criminal Law in Edinburgh, Scotland, in June 2015, though it has been significantly updated. I am grateful for the questions and feedback I received at the conference and particularly to Justice Tom Cromwell, Justice Elizabeth Bennett, Director of Public Prosecutions Claire Loftus, Professor Neil Boister, and Jeffrey Johnston. Thanks are also due to Chris Ram, David Fraser, Al Gidari and the anonymous peer reviewers for this article, and to Greg Melchin (JD, Dalhousie University, 2016) for excellent research assistance.

Vol. 54 [2016], doi:10.1017/cyl.2017.7

lens of the public international law of jurisdiction and, specifically, the prohibition of extraterritorial enforcement jurisdiction. An analysis of state practice reveals that unsanctioned cross-border evidence gathering is viewed by states as an intrusion on territorial sovereignty, engaging the prohibition, and that this view properly extends to the kind of state activity dealt with in the *Microsoft Ireland* case.

potentiellement résolus — selon l'optique du droit international public de la compétence, et plus particulièrement de l'interdiction de l'exercice de la compétence d'exécution à l'étranger. Une analyse de la pratique des États révèle que la collecte transfrontalière non-autorisée de données est perçue par les États comme une atteinte à leur souveraineté territoriale ainsi qu'une contravention à l'interdiction d'exécution extraterritoriale. Cette analyse se prête bien à l'évaluation du genre d'activités étatiques traitées dans l'affaire *Microsoft Ireland*.

Keywords: Transnational crime; cybercrime; cross-border electronic evidence; extraterritorial jurisdiction; enforcement jurisdiction.

Mots-clés: Crime transnational; cybercriminalité; preuves électroniques transfrontalières; compétence extraterritoriale; compétence d'exécution.

Introduction

There are schools of thought in international law regarding where the methodological emphasis should lie. These vary from practitioner to practitioner and sometimes from issue to issue. The members of one such school are sometimes colloquially called "jurisdictionalists" because they tend to the view that, despite the temptation to analyze international law problems as "realists" or "diplomats," or to take into account the various political aspects of any given matter, many legal issues between states are best approached from the standpoint of jurisdiction — specifically, those international law rules that govern how, when, and where states may exert their sovereign power. So doing, it is argued, allows one to identify problems in the most legally sound manner and provides the best platform from which to propose solutions, even though the solutions themselves may very well involve realism, *realpolitik*, or diplomacy. It also acknowledges that the rules around jurisdiction arise from the nature of state sovereignty and are, in fact, a primary manner in which states channel their sovereign power *vis-à-vis* other states.

To analyze otherwise is to put the cart before the horse; it is simply more efficient to begin with jurisdiction than to attack the problem from the standpoint of, say, what is most advantageous to a particular party to the problem or to focus on the subject matter of the issue. Beginning with jurisdiction draws a frame around the picture, which can then be filled in by using the other colours on our palette. While many might disagree on the primacy of this particular tool bag in a broad sense, the jurisdictionalist point of view is at its most powerful when examining legal issues that arise in the context of

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

transnational criminal law.[1] State sovereignty concerns are at their stickiest and most intense when the criminal law is engaged, and, thus, jurisdiction becomes a most useful lens for analysis when looking at how states cooperate — or fail to cooperate — in the suppression of transnational crime.

In my view, the current furor around the *Microsoft Ireland* case[2] wending its way through the US courts bears the hallmarks of a discussion that has fallen into the traps that jurisdictionalists seek to avoid. The case has been fervently discussed and blogged upon in many interested communities, but it can be summarized quite simply.[3] In a criminal investigation US federal prosecutors identified a user's email account held by Microsoft and wished to obtain both the account's content and any metadata associated with it. A New York magistrate issued a warrant directing Microsoft to produce the content (including emails) and associated metadata.[4] While it produced the metadata, which was stored in the United States, Microsoft moved to quash the warrant on the basis that the rest of the data was stored in Ireland and, thus, beyond the jurisdictional reach of the US government. The motion to quash was dismissed by the magistrate, and Microsoft voluntarily placed itself in contempt of the order for the warrant in order to advance the case to the Second Circuit Court of Appeals.[5] A number of *amici* filed briefs in the Second Circuit, which heard oral argument in September 2015 and rendered its decision in July 2016 (discussed below). The issue, simply put, is whether it

[1] The emerging field of "transnational criminal law" examines the body of public international law, primarily treaty based, under which states cooperate in the suppression of criminal activity that transcends borders and engages mutual interests. See generally Neil Boister & Robert J Currie, *Routledge Handbook of Transnational Criminal Law* (London: Routledge, 2015); Neil Boister, *An Introduction to Transnational Criminal Law* (Oxford: Oxford University Press, 2012). As this article is focused on investigation and enforcement, I am using the term in the broader sense of cross-border crime that engages the interests of more than one state, which I have called elsewhere "transnational crimes of domestic concern." Robert J Currie & Joseph Rikhof, *International and Transnational Criminal Law*, 2d ed (Toronto: Irwin, 2013) at 22.

[2] *Microsoft Corporation v United States of America*, 829 F3d 197 (2d Circ 2016), rehearing *en banc* denied, No 14-2985, 2017 WL 362765 (2d Cir, 24 January 2017) [*Microsoft Ireland* case].

[3] One of the *amici* in the case, Electronic Frontier Foundation (EFF), has put up a page on its website that conveniently provides pdf copies of all of the relevant documents and pleadings in the case. See EFF, online: <https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland>. All citations to these documents herein will be sourced to this site.

[4] What species of "warrant," "subpoena," or other criminal procedure device this order amounts to is actually at issue in the case. It appears to be analogous to the Canadian production order (see *Criminal Code*, RSC 1985, c C-46, s 487.014) where at the Crown's instance a court will issue an order directing a private party to produce evidence. What is pertinent for this article, as discussed below, is that the "warrant" amounts to an exercise of compulsory state power and is thus an exercise of enforcement jurisdiction.

[5] *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, 2014 WL 1661004, 13 Mag 2814 (US Dist Ct) (25 April 2014).

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

is lawful for a government to compel an individual within its territory to produce data that is stored on the territory of another state, even if the individual in question has the technical ability to retrieve and produce the data.

The *Microsoft Ireland* case is significant in part because it appears to be the first case on this particular issue that has approached a major appellate court in a common law jurisdiction, or at least the first where the international law aspects of the question have been explicitly raised.[6] Parenthetically, it may not be the last, as Google is embroiled in a similar dispute before the federal courts in a different district.[7] On a broader view, however, this development is a very current splash in an already roiled pond. It is a specific example of the challenges posed by the increasing amount of digital evidence that must be gathered in transnational crime cases[8] and of the way that these challenges are fraying the fabric of traditional models of cooperative evidence gathering used by states. Traditionally, the bar on extraterritorial enforcement jurisdiction (explained in more detail below) has meant that states that resorted to gathering evidence beyond their territories did so at their own legal peril, and, in recent decades, mutual legal assistance treaty (MLAT) practice has developed to serve this need.[9] However, gathering digital evidence (whether it is in servers located in known locations in other states or in "the cloud") presents both opportunities and challenges — opportunities because of the relative ease with which evidence can be obtained via computer, but challenges because of state reluctance to allow foreign enforcement authorities to pierce territorial borders, even where those borders are straddled by cyberspace.

Part of the reason why the *Microsoft Ireland* case, in particular, is clouding the waters of this discussion is that a great deal of the conversation revolves around American law, particularly American procedural and constitutional law and the manner in which that state's law interacts with international law (the presumption against extraterritoriality when interpreting statutes, the

[6] The case of *eBay Canada Ltd v Canada (National Minister of Revenue)*, 2007 FC 930, aff'd 2008 FCA 348 [*eBay* case], before the Federal Court and Federal Court of Appeal of Canada dealt with essentially the same issue, but it appears the international law aspects were not brought to the attention of the courts.

[7] *In re Search Warrant no 16-690-M-01 to Google; In re Search Warrant no 16-690-M to Google*, Decision of Judge Thomas J Reuter (Dist Ct Eastern District for Pennsylvania, 3 February 2017) [*Google Warrant* case]. See Ricci Dipshan, "The Cloud Conundrum: Explaining Divergent Google, Microsoft Search Warrant Rulings," *LAW.COM* (15 February 2017), online: <http://www.law.com/sites/almstaff/2017/02/15/the-cloud-conundrum-explaining-divergent-google-microsoft-search-warrant-rulings/?slreturn=20170122201302>.

[8] Indeed, it is sometimes the presence of potentially relevant evidence in a state outside the investigating state that makes a case "transnational" in nature. See Ellen S Podgor, "Cybercrime: National, Transnational or International?" (2004) 50 Wayne L Rev 97.

[9] That is, the conclusion of mutual legal assistance treaties (MLATs), under which states agree to collect and send evidence to each other, on a reciprocal basis, for use in criminal proceedings. See section II below.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

"*Charming Betsy*" doctrine, and so forth).[10] The result of this has been that the international law issues at the heart of the case are not always clearly understood — for example, the clear distinction between extraterritorial prescriptive and enforcement jurisdiction (described below) is sometimes lost. Many of the commentators who do go into the international law issues nonetheless give them short shrift, often referring away the issue as "the MLAT problem" and using it as a springboard for proposals involving a new and/or different approach to how law enforcement operates in this area. While all of that will definitely play a role in the resolution of the case itself, the goal here is to analyze the problem from a strictly international law point of view, with domestic laws and practices utilized simply as examples of state practice rather than assuming any normative role on their own. This is a more modest goal than attempting to figure out how to resolve the problem, but it may be that generating a solid international law understanding of the issues will help in the generation of solid solutions.

Extricating the discussion from the morass of US law and law enforcement policy concerns that surround it is useful, in my view, for two reasons. First, as explored below, the precise legal issue at play in the *Microsoft Ireland* case is not a new one, but it is one that is assuming increasing importance between states engaged in transnational criminal cooperation, and a picture of the international scene could be of some use. In the end, despite the frustration with the nature of the international legal system that moves commentators to demand we "do something different," international law is ultimately a consent-based system, and a positivist approach provides the clarity needed for the formulation of solid legal alternatives. Second, the time is right for a more internationally focused, and thus less United States focused, examination of these issues, particularly as they involve the storage of data. It has been correctly observed that in terms of where international user data is located, "at the moment, US-based providers dominate much of the global market and US law and practice therefore impacts on a significant percentage of international internet users."[11] However, the legacy of the Edward Snowden/Wikileaks disclosures regarding US surveillance practices appears to be a shift away from the US market as the default location for the data centre market,[12] as demonstrated by the "data sovereignty" movement seen

[10] Some solid examples of writing of this sort: Orin Kerr, "The Surprising Implications of the Microsoft/Ireland Warrant Case," *Washington Post* (29 November 2016), online: <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/?utm_term=.8cd07e1ec5a9>; Jennifer Daskal, "The Un-Territoriality of Data" (2015–16) 125 Yale LJ 326.

[11] Kate Westmoreland & Gail Kent, "Foreign Law Enforcement Access to User Data: A Survival Guide and Call For Action" (2015) 13:2 Can J L & Technology 225.

[12] As is well known, in October 2015, the Court of Justice for the European Commission issued a decision invalidating the US–EU *Safe Harbour Agreement Regarding Data Transfer and Protection*. See Case C-362/14, *Maximillian Schrems v Data Protection*

in some states[13] and by the relocation of data centres by Internet companies themselves to jurisdictions where there is greater legal protection for privacy and where, at least for the moment, there is a shield of territorial sovereignty to be wielded (a feature of the *Microsoft Ireland* case itself).[14]

The remainder of this article will proceed in four parts. The second part will briefly review the fundamental international jurisdictional principles that form the backdrop for any discussion of cross-border evidence gathering, particularly the bar on extraterritorial enforcement jurisdiction and the tools that have been crafted to allow for criminal cooperation between states. The third part will examine the specific jurisdictional challenges to cross-border electronic evidence gathering in transnational crime cases,[15] in particular, the seizure of cross-border electronic evidence by police, and assess the overall "lay of the land" in terms of international law norms. The fourth part will look

Commissioner (6 October 2015), online: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=61478>, which one blogger accurately referred to as "Snowden aftershocks." Alysa Zeltzer Hutnik & Crystal N Skelton, "Snowden Aftershocks: High Court Invalidates US-EU Safe Harbor," online: <http://www.adlawaccess.com/2015/10/articles/snowden-aftershocks-high-court-invalidates-u-s-eu-safe-harbor/#page=1>. And see David S Kris, *Statement before the Committee on the Judiciary, US House of Representatives, Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests* (25 February 2016), online: <http://judiciary.house.gov/_cache/files/95e3c0d6-2da2-40f3-a91a-a4849ff240b8/david-kris-testimony.pdf>.

[13] See generally C Kuner et al, "Internet Balkanization Gathers Pace: Is Privacy the Real Driver?" (2015) 5:1 International Data Privacy Law 1; P de Filippi & S McCarthy, "Cloud Computing: Centralization and Data Sovereignty" (2012) 3:2 Eur J L & Technology. Brazil has been especially keen on this point. See Tim Ridout, "Brazil's Internet Constitution: The Struggle Continues," *Fletcher Forum* (25 March 2014), online: <http://www.fletcherforum.org/2014/03/25/ridout/>. Russia's new "data localization" laws came into force on 1 September 2015 and the Russian telecommunications regulator recently issued an order blocking public access to the LinkedIn social network on the basis that it was in violation of the law. Maria Tsvetkova & Andrew Osborn, "Russia Starts Blocking LinkedIn Website after Court Ruling," *Reuters Technology News* (17 November 2016), online: <http://www.reuters.com/article/us-russia-linkedin-idUSKBN13C0RN>.

[14] See Mark Wilson, "Twitter Moves Non-US Accounts to Ireland, and Away from the NSA," *Slashdot* (18 April 2015), online: <http://yro.slashdot.org/story/15/04/18/0633204/twitter-moves-non-us-accounts-to-ireland-and-away-from-the-nsa>.

[15] I should note that I am intentionally avoiding any substantial discussion of "cybercrime" in this article. It is not necessarily irrelevant, as on some definitions of "cybercrime" any criminal case that has electronic evidence involved would be a cybercrime case. However, the focus here is more generally on situations where there is electronic evidence that appears to require a transnational enforcement effort of some sort, whether a given case would involve "cybercrime" or not. The recent study by the United Nations Office and Drugs and Crime's (UNODC) inter-governmental panel of experts highlighted "the increasing involvement of electronic evidence in *all* crime types and not just those falling within the term 'cybercrime.'" UNODC, *Comprehensive Study on Cybercrime: Draft 2013* (New York: United Nations, 2013) at 188.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

at the specific problem raised by the *Microsoft Ireland* case — that of courts or prosecutorial authorities ordering private parties to produce digital evidence that is located in a foreign state — and will attempt to ascertain whether it is indeed a problem of extraterritorial enforcement jurisdiction or a different species of problem altogether. The fifth part will offer the quite unstartling conclusion that the problems associated with the issue in the *Microsoft Ireland* case specifically, and with cross-border evidence gathering more generally, are jurisdictional in nature, and jurisdictional problems are best resolved by treaties or other forms of cooperative arrangement. It will also comment on the utility of proposals to stretch the boundaries of the otherwise "hard law" prohibition against extraterritorial evidence gathering, proposals suited to a world in which electronic evidence is becoming central.

Jurisdictional Fundamentals

"Jurisdiction," in the international law sense used here, is "the term that describes the limits of legal competence of a State … to make, apply and enforce rules of conduct upon persons."[16] In international law, the jurisdiction of states is generally considered to be an aspect of state sovereignty, and the rules surrounding the exercise of jurisdiction by states are meant to manage potentially conflicting sovereign interests. States being territorial entities, conflict is less likely when states exercise jurisdiction entirely within their own territories. Thus, it is situations where a state's exercise of jurisdiction somehow extends beyond its territory — usually referred to as extraterritorial jurisdiction — that the international law of jurisdiction is designed to address. As has been noted,

> [t]he international law regarding the exercise of jurisdiction by states can be expressed simply: one state's exercise of sovereign power cannot infringe upon the sovereignty of another state or states. This is easy enough to assert, but nebulous and nuanced in application because judging where the line is crossed is a complex exercise. ... [T]he rules differ as between [prescriptive] and enforcement jurisdiction … The central point of conflict will be situations of *concurrent jurisdiction*; that is, where two or more states have some legal claim to exercise jurisdiction over a particular matter.[17]

The *Lotus* case tells us that states being sovereign entities, they are free to exercise jurisdiction in any way they choose, barring a rule to the contrary.[18] There being no *ab initio* prohibition on the exercise of jurisdiction,

[16] Vaughan Lowe & C Staker, "Jurisdiction" in Malcolm D Evans, ed, *International Law*, 3d ed (Oxford: Oxford University Press, 2010) 313.

[17] Steve Coughlan et al, *Law beyond Borders: Extraterritorial Jurisdiction in an Age of Globalization* (Toronto: Irwin Law, 2014) at 35–36 [emphasis in original].

[18] *Case of the SS Lotus (France v Turkey)*, 1927 PCIJ (Ser A) No 10, 31 [*Lotus*].

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

the international law rules are essentially designed to manage and head off potential conflict or, as it has been phrased, "to safeguard the international community against overreaching by individual [state]s."[19]

The key distinction is the one named in the excerpt quoted above between prescriptive jurisdiction (the ability of states to make laws pertaining to people, places, and things) and enforcement jurisdiction (the ability of states to apply or enforce those laws). Extraterritorial law-making by states tends to be considered lawful when it extends along one of the familiar traditional principles of jurisdiction: nationality, passive personality, protective, and universal. This generally permissive approach is in stark contrast to the rules surrounding the exercise of enforcement jurisdiction. The latter can for present purposes be understood as the ability of a state to enforce its criminal law not just through the prosecution in court of individuals but also through the ability of police to exercise the powers (often compulsory) required for the investigation of crimes, what the Supreme Court of Canada has labeled "investigative jurisdiction" — search and seizure, witness/accused questioning, arrest, and so on.[20] Enforcement jurisdiction is strictly territorially bounded; in the oft-quoted words of the *Lotus* case, a state

> may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.[21]

Accordingly, the police of State A cannot go across the border into neighbouring State B and arrest an individual, nor can they exercise other police powers, at least without the consent of State B.

The ban on extraterritorial enforcement jurisdiction is fairly straightforward and tends to be viewed restrictively and enforced strictly by states. It is important to appreciate the contours of how the rule works and how it interacts with the rules about prescriptive jurisdiction, all of which can be illustrated by simple, but true-to-life, examples:

- X commits murder in Canada and flees to the United States. Canada can exercise prescriptive jurisdiction over the crime, but cannot exercise enforcement jurisdiction over the person.
- Z, an American, commits murder in Oregon and flees to British Columbia. Canada can detain or arrest the person (on the basis of a request from the United States), but has no jurisdiction over the crime.

[19] Hannah L Buxbaum, "Transnational Regulatory Litigation" (2006) 46 Va J Intl L 251 at 304.

[20] *R v Hape*, 2007 SCC 26, para 58.

[21] *Lotus*, *supra* note 18 at 18–19.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

- Y, a Canadian, commits a terrorist crime in France and returns to Canada. Canada has extraterritorial prescriptive jurisdiction over the crime (on the basis of nationality), but can only exercise enforcement jurisdiction over the person because he is in Canada.
- The same scenario as immediately above involving Y and his return from France to Canada, but, in their investigation, Canadian police wish to gather forensic evidence and interview witnesses, all of which would occur on French soil. They are prohibited from this exercise of extraterritorial enforcement jurisdiction, even though Canada has jurisdiction over the crime and the person.

The latter point is a particularly important one because it is sometimes argued (as, indeed, the US government argued in *Microsoft Ireland*) that if a court has both "subject matter" and "personal" jurisdiction then it may issue whatever orders it wishes involving the case. This terminology is largely lifted from private international law and does not reflect the strictness of the international law prohibition on extraterritorial enforcement jurisdiction. To wit, a state may have jurisdiction over both the crime and the person, but this does not give it the ability lawfully to gather the evidence on its own because that evidence is in the territory of another state.

States tend to be quite chauvinistic about their domestic criminal laws and, thus, guard their sovereignty closely in this arena.[22] In fact, the international law of jurisdiction is generally understood to have evolved from state practice around conflicts of criminal law.[23] Conflicts between states over the exercise of criminal jurisdiction are by no means ordinary, but they do occur, and the investigation of any transnational criminal matter is meant to be shaped by sensitivity to the prohibition on extraterritorial enforcement jurisdiction. After all, enforcement activity on a state's territory that is not sanctioned or even known about by that state undermines the entire rule of law in that state and, in particular, any human rights protections. It is important not to understate the

[22] This is a point often made in international law literature, but a recent report based on a survey of cybercrime and international law experts from an array of countries provides a contemporary explanation: "It is worth noting here the strength of feeling among the international lawyers present in the workshop organized for this project as to the sensitivity of states to a breach of territorial integrity for the purpose of criminal law or security investigations. This feeling is based upon the dual observation that a state's first responsibility is traditionally understood to be ensuring public order and the fact that the enforcement of criminal law is explicitly connected to the coercive power of the state, ie its monopoly of violence that is the marker of its internal claim to sovereignty." Bert-Jaap Koops & Morag Goodwin, *Cyberspace, the Cloud and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law* (Tilburg: Tilburg Institute for Law, Technology and Society, 2014) at 61.

[23] Hugh M Kindred, et al, eds, *International Law: Chiefly as Interpreted and Applied in Canada*, 8th ed (Toronto: Emond Montgomery, 2014) at 252.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

dangers presented by jurisdictional conflict since, as one experienced commentator has noted,

> [s]tates and intergovernmental organizations act with caution, deliberation and consensus because the consequences of precipitous unilateral actions can be dire. The First World War started, in part, because one State insisted on the right to conduct a criminal investigation into the murder of one of its officials on the sovereign territory of another.[24]

Less calamitously, breaches of the rule against extraterritorial enforcement jurisdiction can create legal and diplomatic complications between states, create havens for criminals in situations where extradition is interfered with, and, perhaps most seriously, can compromise the level of trust that is required for states to cooperate in the suppression of transnational crime. In the Canadian experience, such breaches have led to both extradition[25] and mutual legal assistance requests[26] being denied by courts as well as the corrosion of relationships between Canadian and US police forces.[27]

Over the past century and a half, the increasing need to combat transnational crime has moved states to craft tools to allow them to provide mutual cooperation in crime suppression while, at the same time, respecting the jurisdictional rules and the sovereign interests they protect. Extradition, then, is properly understood as a formal (indeed, treaty-based) agreement by a state to exercise enforcement jurisdiction on its own territory (by way of arrest, detention, and rendition) on behalf of its partner/requesting states on a reciprocal basis. Similarly, under mutual legal assistance treaties, states are obliged to exercise various other forms of enforcement jurisdiction (typically investigation-type activities) on their territories, again on the request of treaty partners. The treaties themselves have a dual function:

[24] Chris D Ram, "The Globalization of Crime as a Jurisdictional Challenge" (paper delivered at the 2011 Annual Conference of the Canadian Council on International Law, Ottawa, 2011) at 1 [copy on file with author].

[25] See *USA v Licht*, 2002 BCSC 1151, where an extradition was stayed because the US Drug Enforcement Agency (DEA) had been operating a sting operation on Canadian territory without the permission of Canadian authorities.

[26] *United States of America v Orphanou* (2004), 19 CR (6th) 291 (Ont SCJ), where an MLAT request was denied because a US police officer who was permitted to attend the execution of an MLAT-based search warrant absconded with evidence.

[27] In early 2013, there were media reports of a dispute between the Canadian Royal Canadian Mounted Police (RCMP) and the US DEA, due to the Canadian police operating a confidential informant on US soil without the permission of American authorities. See John Nicol & Dave Seglins, "L.A. Cocaine Bust Threatens Canada-US Police Relations," *CBC News Canada* (12 February 2013), online: <http://www.cbc.ca/news/canada/story/2013/02/11/canada-us-police-relations.html>.

they create the legal obligation between the states, and they provide (via implementation) a basis in domestic law for the enforcement activities that the requested state carries out.[28]

INTERPOL, while predominantly an information-sharing network among national police forces, serves a similar function with its Red Notices, under which states can arrest and detain individuals who are outside the territory of the state that wants them. More recently, there has been a growth in the use of more direct policing cooperation, utilizing such mechanisms as posting liaison officers in foreign states, joint investigation teams, and "shiprider" agreements[29] on bilateral, multilateral, and regional bases.[30] These are employed with varying degrees of formality, but they have taken on extra layers of formality and obligation as they are used by regional organizations such as EUROPOL and form a significant part of the undergirding of the more recent transnational criminal law suppression conventions.[31] Importantly, all of this activity is done with an eye to guarding the sovereignty of all states involved, particularly the state that is the locus of the investigation: "[I]t is traditional to apply limiting conditions so as to ensure that investigative activities in state B conducted by or on behalf of state A will comply with state B's laws, norms, and traditions."[32]

By way of illustration, Canadian practice bears this out on both sides of the coin; in *R v Hape*, for example, Royal Canadian Mounted Police officers were engaged in a cooperative investigation with police in Turks and Caicos, but were bound strictly by the laws of that territory and under the authority of local police, pursuant to an agreement that was in place.[33]

[28] On extradition and mutual legal assistance generally, see Currie & Rikhof, *supra* note 1, ch 9.

[29] These are agreements, usually for narcotics interdiction, under which enforcement officials from one state will ride aboard an enforcement ship or aircraft from another state, in order to provide permission for the enforcement ship to cross into the first state's territorial waters or airspace to pursue traffickers' vessels. See JE Kramek, "Bilateral Maritime Counter Drug and Immigrant Interdiction Agreements: Is This the World of the Future?" (2000) 31 U Miami Inter-American L Rev 121; William Gilmore, *Agreement Concerning Co-operation in Suppressing Illicit Maritime and Air Trafficking in Narcotic Drugs and Psychotropic Substances in the Caribbean Area* (London: UK Foreign & Commonwealth Office, 2003).

[30] See generally Saskia Hufnagel & Carole McCartney, "Police Cooperation against Transnational Criminals" in Boister & Currie, *supra* note 1, 107; Saskia Hufnagel, Clive Harfield & Simon Bronitt, eds, *Cross-Border Law Enforcement: Regional Law Enforcement Cooperation — European, Australian and Asia Pacific Perspectives* (New York: Routledge, 2012); Andrew Goldsmith & James Sheptycki, eds, *Crafting Transnational Policing* (Oxford: Hart, 2007).

[31] See Boister, *supra* note 1, ch 13.

[32] Koops & Goodwin, *supra* note 22, citing PJP Tak, "Bottlenecks in International Police and Judicial Cooperation in the EU" (2000) 8 Eur J Crime, Crim L & Crim Justice 343 at 344.

[33] See note 20 above.

Under the terms of the Canada–United States *Framework Agreement on Integrated Cross-Border Maritime Law Enforcement Operations*, each state's enforcement officers are assimilated to those of the partner state and, when operating in the partner state, possess only those powers that the partner state's officers can exercise.[34]

Cross-Border Electronic Evidence Gathering

applying the prohibition on extraterritorial enforcement to electronic evidence

The foregoing section was a fairly conventional account of the international law of jurisdiction but was necessary to underpin the discussion here — in no small part because it is important to understand that the rules that exist evolved during times when investigation and prosecution of crimes occurred in the physical (or, as some prefer it, "kinetic") world. The remainder of this article is about the uneasy interaction between these rules, the presence and nature of digitized information, and shifting state interests and abilities in criminal investigation.

As communication technologies have come to play a more and more ubiquitous role in crime, as in life, there has been a corresponding increase in the preoccupation with how law enforcement can effectively and efficiently gather electronic data for use as evidence.[35] Due to the form it takes and how it exists within the international communications infrastructure, electronic evidence has a naturally "transnational" nature, and it is increasingly clear that traditional, territorially bound jurisdictional norms such as those described above obstruct investigation more than was even the case with traditional, kinetic evidence. Yet, the early prediction of cyberspace as some kind of "separate place" that could have its own independent legal regime died on the vine. As will be seen, states do treat the Internet and the overall international communications infrastructure as a territorially bounded place, and technology continues to develop in such a way that allows them to do so.[36] The goal of this section is to review the international law norms regarding enforcement jurisdiction as they apply to cross-border electronic evidence gathering, and it could properly be quite short, as study after study over the last decade or more have indicated that states

[34] *Framework Agreement on Integrated Cross-Border Maritime Law Enforcement Operations*, 26 May 2009, Can TS 25 (2012).

[35] Not to mention its use in court. A recent book on the subject to which I have contributed is already in its third edition. Stephen Mason, ed, *Electronic Evidence*, 3d ed (New York: LexisNexis, 2012).

[36] Bert-Jaap Koops & Susan Brenner, *Cybercrime and Jurisdiction: A Global Survey* (The Hague: TMC Asser Press, 2006); Teresa Scassa & Robert J Currie. "New First Principles? Assessing the Internet's Challenges to Jurisdiction" (2011) 42 Georgetown J Intl L 1017.

view cross-border intrusion by law enforcement authorities as a breach of sovereignty and a violation of the bar on extraterritorial enforcement jurisdiction.[37] Unpacking this picture provides a more nuanced, but still firm, view on this point.

Electronic evidence, in the form of digitized material, presents enforcement challenges for a number of reasons, but most importantly because it is ephemeral and subject to easy movement and manipulation by computers. Accordingly, the question of enforcement jurisdiction regarding electronic evidence very quickly becomes one about "jurisdiction over the Internet" since Internet-based access to the data is really the heart of the matter. If a police officer seizes a computer, a server, a compact disc, or a thumb drive full of data in a foreign state and then drives across the border to her own state, that is essentially the same kind of enforcement jurisdiction as an unlawful search and seizure in traditional terms and can be understood and dealt with in the same way. However, if a police officer who is in a foreign state causes data to be electronically compelled and sent across borders or, more pressingly, if police officers operating computers in their own state obtain data that is stored in a foreign state, the problem becomes more complex. Data can be transient and fast moving; its actual geographical location can be uncertain; and real-time monitoring and gathering may be needed or even required to successfully take an investigative step. The data may be openly obtainable by a website fully accessible to anyone via the Internet, it may be protected by law but not security measures, or it may be secured and require electronic intrusion of some sort ("hacking") to obtain. Whatever the territorial or geographical aspects of a particular matter, the Internet — and its use by criminals — is the locus of the problem.

Perhaps the single greatest dashed hope regarding the Internet was that it would prove to be a place *sui generis*, apart from the kinetic world, free from regulation by state laws[38] or, alternatively, that it would function as some sort of *res communis* space, subject to cooperative and collective regulation under international law.[39] None of these Latin hopes ever took shape.

[37] Gail Kent, *Sharing Investigation-Specific Data with Law Enforcement: An International Approach*, Stanford Public Law Working Paper (14 February 2014), online: <https://ssrn.com/abstract=2472413>; Koops & Goodwin, *supra* note 22; Nicolai Seitz, "Transborder Search: A New Perspective in Law Enforcement?" (2004–05) 7 Yale J L & Technology 23; UNODC, *supra* note 15.

[38] Most famously in John Parry Barlow, "A Declaration of the Independence of Cyberspace," EFF, online: <https://homes.eff.org/~barlow/Declaration-Final.html>. See also David R. Johnson & David Post, "Law & Borders: The Rise of Law in Cyberspace" (1996) 48 Stan L Rev 1367.

[39] See, eg, Daniel C Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces" (1998) 4 Mich Telecommunications & Technology L Rev 69.

From reasonably early times, states could and did treat the Internet as a territorially bounded place.[40] Jurisdiction was asserted and assumed over as broad a range of state interests as could be imagined, from crime to private law torts, to commerce, to speech, to culture.[41] As Bert-Jaap Koops and Susan Brenner comment in the preface to their edited collection of studies on jurisdiction over cybercrime, "territoriality still turns out to be a prime factor; apparently, cyberspace is not considered so a-territorial after all."[42]

To be sure, the Internet has caused notable and significant stresses and stretching effects upon the jurisdictional rules. As Teresa Scassa and I explored in an earlier article,[43] the assertion of prescriptive jurisdiction by states over Internet-based activities has led to a rise in the use of the "qualified territoriality" or "extended territoriality" principle — the assertion of jurisdiction based on the impact of a matter upon the territory of a state, even if the whole matter was not contained within that state's territory.[44] This principle has proven useful in allowing states and regulatory authorities to deal with the fact that Internet-based matters do not correspond easily to Westphalian concepts. As Justice Gerard La Forest famously said regarding crimes, they may occur "both here and there."[45] Yet this is a simple stretching of the territorial principle to deal with the practical realities that globalization has wrought and one that fits well (if slightly fuzzily at its margins) within the traditional law of jurisdiction.

State practice regarding enforcement jurisdiction has also remained more conservative in regard to electronic evidence and generally reflects a territorial understanding of how the law will treat the gathering of data by law enforcement — a view buttressed in no small part by the fact that technological developments increasingly make it possible to tell where data is present or stored.[46] A recent piece on cybercrime sums up the prevailing attitude of states:

[40] See Milton L Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010) at 3.

[41] See generally Jack Goldsmith, "Unilateral Regulation of the Internet: A Modest Defense" (2003) 11 EJIL 135; Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge: Cambridge University Press, 2007).

[42] Koops & Brenner, *supra* note 36 at 6.

[43] Scassa & Currie, *supra* note 36.

[44] See also Coughlan et al, *supra* note 17, ch 4.

[45] *Libman v The Queen*, [1985] 2 SCR 178, para 63.

[46] Dan Jerker B Svantesson, "How Does the Accuracy of Geo-Location Technologies Affect the Law?" (2007) 2 Masaryk U J L & Tech 11. Of course, as discussed below, this cannot always be accomplished rapidly and in real-time accordance with the needs of a criminal investigation.

International law is clear that, while offences may be given extraterritorial application to protect essential interests, any form of extraterritorial investigation or enforcement requires the consent of any country on whose territory it takes place. This includes any kind of investigative measures … and without consent, foreign investigative measures would be fully subject to local criminal laws. Foreign intrusions would also usually be regarded as an infringement of sovereignty calling for some sort of retaliatory action.[47]

This statement captures the findings of numerous studies that have been done on the subject in the last fifteen years. Indeed, expressions by states of the dual concern of maintaining state sovereignty over territory while coming up with an effective approach to deal with the problem can be tracked back to the 1980s.[48] The case most frequently cited to prove the point is that of *Gorshkov/Ivanov*,[49] two Russian cybercriminals who hacked numerous websites and stole large amounts of information, including credit card numbers. The two were lured to California by the Federal Bureau of Investigation (FBI) under the guise of a job interview at a technology company, and during the "interview," FBI agents monitored Gorshkov's access to his computer back in Russia. Obtaining his login and password information, the agents accessed his computer and downloaded its entire contents in order to collect evidence with which to prosecute. Russia protested this action as a violation of its territorial sovereignty and charged the FBI agents with hacking, the Russian Federal Security Service explicitly invoking territorial sovereignty as part of its overall objection.[50]

This same view was quite evident in the negotiations leading to the Council of Europe's *Convention on Cybercrime*, concluded in 2001.[51] It was clear that potential states parties to the treaty were keenly aware that the inherently cross-border nature of data meant that territorial borders were essentially getting in the way of effective investigation, but the official *Explanatory Report* also reflects that a territorial understanding of enforcement jurisdiction was still the dominant point of view and that consensus on solutions was difficult to achieve.[52] The only compromise reached was

[47] Chris Ram, "Cybercrime" in Boister & Currie, *supra* note 1, 390.

[48] Cybercrime Convention Committee (T-CY), *Transborder Access and Jurisdiction: What Are the Options?*, Doc no T-CY (2012) 3 (6 December 2012) at 6 [T-CY, *Transborder Access and Jurisdiction*].

[49] See Susan Brenner & Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) 4 J High Tech L 1 at 21–23; Seitz, *supra* note 37.

[50] "Russians Accuse FBI of Hacking," *The Register* (16 October 2002), online: http://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent>.

[51] *Convention on Cybercrime*, ETS 185 (2001).

[52] Council of Europe, *Explanatory Report to the Convention on Cybercrime* (23 November 2001), online: <https://rm.coe.int/16800cce5b>. See also Henrik WK Kaspersen, "Jurisdiction in the Cybercrime Convention" in Koops & Brenner, *supra* note 36, 9 at 19–21.

embodied in Article 32 of the convention, which permitted cross-border access to data by law enforcement authorities in either of two situations: (1) the data is "publicly available (open source)" and, thus, obtainable by anyone on the Internet or (2) the investigating state obtains the lawful and voluntary consent of a person who is legally entitled to disclose the data. Even this fairly mild compromise was controversial, as Slovakia has stated that notwithstanding the article it considers that its domestic courts must still approve any request for data,[53] while Russia highlighted the article as part of its reasons for not ratifying the convention.[54]

These examples illustrate that states are sensitive and conservative about any cross-border electronic traffic by foreign investigators and that they wish to maintain the ability to object publicly to actual events or even potential intrusion. There are understandable policy reasons for this. The integrity of territorial sovereignty and control is always key in any discussion of inter-state interaction, and, as noted above, the criminal law is where states are at their most guarded. More specifically, a state may have dual criminality concerns and be leery of the potential for being unwittingly implicated in a prosecution of conduct that it does not view as criminal. It may wish to retain the capacity to refuse to cooperate or allow its territory to be used for enforcement activity where it would view the foreign prosecution (or some aspect of it) as contrary to its *ordre public* — for example, the pursuit of a political dissident under the guise of a criminal prosecution or the suppression of forms of speech that the target state views as being legitimate, to say nothing of the varied views among states on what constitutes terrorism. A permissive or unguarded position on cross-border data gathering deprives a state of this sovereign capacity and allows the investigating state "to circumvent such principles."[55] Many states are also sensitive to the potential for depriving individuals of human rights protections in the form of procedural standards and would prefer that their own judiciaries or other authorities approve any evidence gathering on their territories. As the Transborder Group of the Cybercrime Convention Committee notes,

[53] See Koops & Goodwin, *supra* note 22 at 57, n 220.

[54] See Boris Vasiliev, "Sovereignty, International Cooperation and Cyber Security: A Treaty Dialogue" (2013), online: <http://cyfy.org/speaker/boris-vasiliev/>. The Council of Europe's T-CY appears to disagree. See T-CY, *Guidance Note no 3: Transborder Access to Data (Article 32)*, online: <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)7REV_GN3_transborder_V12adopted.pdf> [T-CY, *Guidance Note no 3*]. Nonetheless, the overall lack of consensus has been consistent. See *Deliberations at the First Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, Held in Vienna from 17 to 21 January 2011: Summary by the Rapporteur*, UN Doc UNODC/CCPCJ/EG.4/2017/2 (21 February 2017), para 27.

[55] T-CY, *Transborder Access and Jurisdiction*, *supra* note 48 at 12.

[e]veryone agrees that transborder access must protect individuals by setting conditions and safeguards on computer and network searches by law enforcement entities. However, States diverge in their views of what safeguards and protections should apply. Well-known examples include differences on the scope of freedom of expression or the requirements on police to obtain an order authorizing a search. The people in a particular State normally expect, at a minimum, the protections afforded to them by this State; they do not expect to be searched according to the standards of a State they do not live in and may never have been in. In turn, the State has an obligation to respect individuals' rights and freedoms incorporated into its domestic law.[56]

This issue has been studied a great deal, and the observation has been consistently made that, regardless of the investigational utility or the desirability of not imposing state borders on cyberspace for the purposes of enforcement jurisdiction, it is the overall view of states that this is what is required.[57] This has continued to be the case well after the early twenty-first-century examples described above. One of the most recent studies, by Bert-Jaap Koops and Morag Goodwin, sums things up nicely:

[T]he most solid view on what international law permits is that accessing data that are, or later turn out to be, stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state and thus constitutes a wrongful act (where the action is attributable to the state), except where sovereign consent has formally been given.[58]

In its large-scale cybercrime study released in 2013, the United Nations Office on Drugs and Crimes's inter-governmental expert group reached a similar conclusion, producing data that indicated that two-thirds of responding states view cross-border access to computer systems or data to be impermissible and (outside limited exceptional situations) requiring access to formal channels.[59] Even more recently, the United States and the United Kingdom — two powerful, technologically advanced states whose relationship of mutual trust is well known — began talks towards a treaty

[56] *Ibid* [footnotes omitted]. "Everyone" in this report would refer to the Council of Europe states, since it is beyond question that not all states agree on the value of protecting the rights of individuals.

[57] An early and frequently cited description of this view is in Jack Goldsmith, "The Internet and the Legitimacy of Remote Cross-Border Searches" (2001) U Chicago Legal Forum 103, though Goldsmith himself takes a more progressivist view.

[58] Koops & Goodwin, *supra* note 22 at 61. See also Kent, *supra* note 37; Kent & Westmoreland, *supra* note 11; Susan W Brenner, "Law, Dissonance, and Remote Computer Searches" (2012) 14 North Carolina J Law & Tech 43.

[59] UNODC, *supra* note 15 at 220.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

that would allow reciprocal direct access to both stored data and traffic data. The proposed treaty is explicitly intended to address the need for an alternative to MLAT procedures.[60] The norm, then, seems to be a hard one.

VARIATIONS IN STATE PRACTICE

It is important to return to methodology at this point. Since the prohibition on extraterritorial enforcement jurisdiction is properly viewed as a customary international law norm, then the foregoing represents primarily the *opinio juris* quotient. States have fairly evenly expressed the view that cross-border electronic data gathering by investigative officials is an unlawful exercise of enforcement jurisdiction. However, in the complex and fast-moving world of transnational crime cases involving data, state practice is not always consistent with this view of the norms. Viewed collectively, at least, there is a certain dissonance between what states say and what they do.

When using treaty-making and legal modeling as examples of state practice, then, additional support for the prohibitive norm is observable. Aside from Article 32 of the *Convention on Cybercrime* and the other state practices mentioned above, the *Arab Convention on Combatting Information Technology Offences* contains rules regarding transborder access that can allow one to infer that acting otherwise would breach the prohibitive norm, and similar deductions can be made from the *Common Market for Eastern and Southern Africa Cybersecurity Draft Model Bill*.[61] Moreover, the mere existence — let alone the increasing prominence — of MLATs is also at least indirect evidence of the norm.

Drilling down to the level of domestic laws and investigative activities that form state practice, however, reveals a more nuanced picture than the public attitudes of states would suggest. While not all of the data assembled on the issue necessarily tracks the formal legal positions of states, the observers who have been surveyed have noted that there is an uncertain, but significant, amount of unilateral cross-border electronic evidence gathering, or other enforcement activity, by police and security personnel.[62] Some of this is simply done unilaterally by the police officers involved, while, in other situations, it is accomplished by way of direct inter-police cooperation, but

[60] Ellen Nakashima & Andrea Peterson, "The British Want to Come to America—with Wiretap Orders and Search Warrants," *Washington Post* (4 February 2016), online: <https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html>.

[61] As cited in UNODC, *supra* note 15 at 198.

[62] Koops & Goodwin, *supra* note 22 at 55–56; UNODC, *supra* note 15, ss 7.4, 7.5; T-CY, *Transborder Access and Jurisdiction*, *supra* note 48, ch 4.

without the sanction of either judicial authorities or other government apparatus of the territorial state. It is not always documented.[63]

On other occasions, the authorities of the territorial state are notified after the fact. Two Dutch cases are instructive. In the first, *Bredolab*, Dutch law enforcement determined that a foreign-located botnet had infected millions of computers worldwide, including a number of servers located in the Netherlands. The authorities took over the botnet and sent messages to every infected computer.[64] In the second, *Descartes*, Dutch authorities were investigating a TOR server containing child pornography that they suspected was located in the United States, and they notified American authorities about the server. When it was discovered that the server was actively posting newly made images, Dutch police copied the images for use in possible prosecutions, destroyed the images on the server, and blocked access to the server. The decision was made not to seek MLAT-based assistance because of time pressure, but the US authorities were later notified and provided with copies of the images seized; there was no objection from the United States.[65]

Moreover, despite the overall tilt towards viewing such actions as sovereignty violations, a surprising number of states have laws that allow or even compel them. The controversial British *Data Retention and Investigatory Powers Act* of 2014 contained broad extraterritorial powers to compel data, including people and companies located outside the United Kingdom being compelled to disclose data relating to conduct outside the United Kingdom — by way of warrants served on them outside the United Kingdom.[66] It has even renewed this approach in more recent proposed amendments.[67] A study by the Cybercrime Convention Committee revealed that the laws of a number of Council of Europe states allow unilateral transborder access in various scenarios, including Belgium, Norway, Portugal, Serbia, and Romania.[68] There are similar laws in Singapore,[69]

[63] T-CY, *Transborder Access and Jurisdiction*, *supra* note 48.

[64] As cited in *ibid* at 35.

[65] As cited in Koops & Goodwin, *supra* note 22 at 56; T-CY, *Transborder Access and Jurisdiction*, *supra* note 48.

[66] *Data Retention and Investigatory Powers Act*, 2014, c 27. A letter to the UK government from one group of academics said that the law "introduces powers that are not only completely novel in the United Kingdom, they are some of the first of their kind globally." Jemima Kiss "Academics: UK 'Drip' Law Changes Are 'Serious Expansion of Surveillance,'" *The Guardian* (15 July 2014), online: <http://www.theguardian.com/technology/2014/jul/15/academics-uk-data-law-surveillance-bill-rushed-parliament>.

[67] See *Investigatory Powers Act*, 2016, c 25.

[68] T-CY, *Transborder Access and Jurisdiction*, *supra* note 48 at 32–42.

[69] Koops & Brenner, *supra* note 36 at 3.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

Australia,[70] and, at the time of writing, similar draft legislation in Ireland.[71] The US Department of Justice and the FBI have introduced amendments to *Federal Rule of Criminal Procedure 41*, which were recently adopted by the US Supreme Court,[72] authorizing search warrants that permit remote accessing of data in other states where the location of the data is not known.[73] Interestingly, the Department of Justice responded to concerns about potential sovereignty violation by pointing out that US law already permits such actions where the location of the data is known.[74]

It is clear that the various imperatives that make cybercrime investigation difficult are presenting challenges to the more conservative traditional stance among states regarding extraterritorial enforcement, and, indeed, the theme of all of the literature on the topic tends to be along the lines of "we cannot do it that way any more, we need new tools." The need for these new tools is made all the more acute by the fact that even knowing where the data is at any given moment can be difficult, due to big data companies using more fluid data storage techniques.[75] Yet the tension between

[70] Christopher Hooper, Ben Martini & Kim-Kwang Raymond Choo, "Cloud Computing and Its Implications for Cybercrime Investigations in Australia" (2013) 29 Computer Law & Security Rev 152.

[71] In the Criminal Justice (Offences Relating to Information Systems) Bill, 2016, no 16, police are authorized, during the execution of a search warrant, to operate or cause to be operated a computer at the site of the search so as to access "any other computer, whether at the place being searched or at any other place, which is lawfully accessible by means of that computer" (s 7(9)). Admittedly this is ambiguous since much turns on how the word "lawfully" is interpreted, and it is not clear whether cross-border access was intended — yet it is reasonable to conclude that police would expect to be able to use this authority to access, for example, social media accounts, the data for which might be stored outside Ireland's territory.

[72] United States, *Federal Rules of Criminal Procedure*, r 41, proposed changes as adopted by the United States Supreme Court (28 April 2016), online: <https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf>. See Zach Lerner, "A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure" (2016) 18 Yale JL & Tech 26.

[73] For a good write-up, see Jon Kelly, "Unwarranted Amendments: Criminal Procedure Rule 41 Alteration Goes Too Far," *UCLA Law Review* (7 May 2015), online: <http://uclawreview.org/2015/05/07/unwarranted-amendments-criminal-procedure-rule-41-alteration-goes-too-far/#_ftn26>.

[74] *Ibid.*

[75] While detailed examination is beyond the scope of this article, it is important to acknowledge that the technological "back end" of data storage is evolving rapidly. *Microsoft Ireland* arose in the technologically straightforward context of a single company (or parent-subsidiary structure) with offices and storage facilities in different states. This could get more complicated where a similar company had data stored in one state, but backup servers in another. Even that context would be somewhat different for a company that had, for example, contracted with a third party cloud storage provider, which would introduce questions around where the cloud provider had stored the client's data, particularly if the cloud provider has storage farms in more than one state. Kerr, *supra* note 10, notes that Google's current methods of

investigational needs and the protection of sovereignty contributes to a sense of disarray that pervades the landscape. MLAT procedures, designed to deal with exactly this issue, are felt to be too blocky and time-consuming to be effective for investigation purposes — to the point that the US government has made the curious argument in the *Microsoft* case that it must be allowed to subvert these procedures because they are inconvenient.[76] Yet what is increasingly referred to as "the MLAT problem" is a real practical concern for law enforcement, and even the ramped-up cooperation regime in the European *Convention on Cybercrime* is not perceived to have helped matters much.[77]

An alternative approach that initially met with some success was for police to make requests of Internet service providers, cloud storage services, and other data holders for voluntary disclosure of data, particularly in cases involving child sexual abuse and child pornography. While this is apparently lawful under Article 32 of the *Convention on Cybercrime*, it is deeply controversial both within and without the Council of Europe states, with many states and commentators taking the view that it is objectionable.[78] Nonetheless, it was and is a fairly popular practice,[79] and many of the "big data" companies have been content to comply with such requests, particularly in investigations regarding child sexual abuse or child pornography. However, this practice has begun to tail off of late, both because national courts such as the Supreme Court of Canada have blocked the practice[80]

dealing with data are quite dynamic, meaning that it can be difficult to pinpoint with accuracy where any particular set of data might be at any instant. None of this, in my view, changes the analysis here, in that the data is always somewhere and international law rules are simply what they are, but any solutions will need to accommodate this complexity.

[76] *Microsoft Ireland*, *supra* note 2.

[77] Kent, *supra* note 37 at 6. A recent European privacy law conference hosted a session entitled "Creative Solutions to the MLAT Problem," online: <http://www.internetjurisdiction.net/ij-project-to-talk-about-reforming-mutual-legal-assistance-at-major-european-privacy-conference/>.

[78] Koops & Goodwin, *supra* note 22 at 58. In 2014, the Council of Europe's commissioner for human rights expressed the view that this practice was "effectively unregulated and close to arbitrary." Council of Europe's Commissioner for Human Rights, *The Rule of Law on the Internet and in the Wider Digital World* (2014) at 104.

[79] See *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc A/HRC/32/38 (11 May 2016), para 59.

[80] In *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212, the Supreme Court of Canada ruled that the previous practice of police making "law enforcement requests" to Internet service providers for voluntary disclosure of information (under the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5) amounted to a "search" under s 8 of the *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, and thus required a warrant. Prior to this, it appears that foreign law enforcement was free to make the "law enforcement requests" of Canadian data companies. See *United States of America v Viscomi*, 2015 ONCA 484, 126 OR (3d) 427, leave to appeal denied [2015] SCCA No 397.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

and because the ripple effects of the Wikileaks revelations have made companies more insistent on domestic search warrants or production orders based on MLAT requests.[81]

What is the methodological result of this situation? In short, it appears that despite overall state insistence that unauthorized cross-border evidence gathering breaches the bar on extraterritorial enforcement jurisdiction, when it comes to electronic data, state practice does not match up evenly with the *opinio juris*. Whether and how the traditional norm applies to the newer practices is, at best, uncertain. Such a state of uncertainty creates the potential for conflict — for example, the approach of "better to seek forgiveness than permission" illustrated in the Dutch cases mentioned above may respond to law enforcement exigencies, but the reaction from a sovereignty protection point of view would not always be positive, and, of course, the purity of the objectives would not mitigate a claim of state responsibility for the investigating state. Moreover, what is clear is that the lack of unity on the legality of the practice means that due process and human rights concerns are often being neglected.

The *Microsoft Ireland* Issue

Framing the problem

Having assessed how well or poorly the traditional norm covers active police cross-border data gathering, the next step is to examine the more indirect method that is raised by the *Microsoft Ireland* case. The methodological question, then, is this: can State A order Individual X to produce data that X controls, but that is stored in State B? Or, in the context of the case itself, can the US government order Microsoft to produce data that is stored in Ireland for use by the state in a criminal investigation? For the present purposes, this legal question will be referred to hereafter as the "*Microsoft Ireland* issue."

It is first worth noting that this discrete legal issue becoming the subject of attention is a display of the adage "everything old is new again." The question of whether it is a breach of international law for the courts of one state to compel private parties to disclose documents located in another state is one that well predates the popular use of either electronic data storage or the Internet. Beginning in the late 1960s, such orders issued by US courts in civil litigation matters involving transnational corporations were viewed as intrusive upon domestic sovereignty by the jurisdictions

[81] Though recent governance rules approved by the European Parliament will allow some limited amount of contact between EUROPOL and data providers, subject to stringent privacy protections. European Parliament press release (5 November 2016), online: <http://www.europarl.europa.eu/news/en/news-room/20160504IPR25747/police-cooperation-meps-approve-new-powers-for-europol-to-fight-terrorism>.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

targeted, including Canada, the United Kingdom, France, and Australia — each of which enacted blocking statutes to prevent the companies from complying with the foreign orders.[82] Moreover, even today, the issue persists outside the cybercrime setting, as the advent of cloud storage has made it more difficult for companies involved in litigation to comply with court orders to disclose the contents of their cloud storage (or easier to refuse to comply, depending upon one's perspective), due to concerns about infringing the laws or sovereignty of the state in which the cloud storage facility resides.[83]

It is of interest that this issue has arisen once again in the US context, for as Google was at pains to point out in a recent filing in its own case on the issue,[84] the American government is well aware of the sovereignty issues at play, indications of which appear in sources such as the *United States Attorneys' Manual* and a Department of Justice manual on obtaining electronic evidence.[85] An interesting recent (if implicit) recognition of the issue is a new practice used by US authorities in corporate criminal prosecutions: to offer cooperative credit to companies being prosecuted so that they will "voluntarily" produce documents that are in another jurisdiction.[86]

This is not to say, however, that parties, courts, or governments who encounter the issue always recognize it. In the Canadian context, the most prominent case to have dealt with the kind of facts that might give rise to the *Microsoft Ireland* issue is *eBay Canada Ltd v Canada (National Revenue)*, where revenue authorities invoked a section of the tax statute that provided for the compulsion of documents relevant to a tax assessment, even if they were located in another state.[87] The information sought existed in electronic form on eBay's central servers in California and was easily electronically accessible to eBay Canada's personnel. The Canadian office's effort to resist the disclosure order was rebuffed by two levels of court, essentially on the basis that, since the data was so easily accessible, it was

[82] For a summary, see Kindred et al, *supra* note 23 at 277–82. Regarding Canada, see Stephen GA Pitel & Nicholas Rafferty, *Conflict of Laws*, 2d ed (Toronto: Irwin, 2016) at 41–42. And see *Restatement (Third) of Foreign Relations Law*, s 442, reporters' note 1.

[83] Yamri Taddese, "Focus: Cloud Services Create Challenges for e-discovery," *Law Times* (7 December 2015).

[84] *Google Warrant*, *supra* note 7.

[85] *Google Inc.'s Amended Objections to Magistrate's Orders Granting Government's Motions to Compel and Overruling Google's Overbreadth Objection & Request for Stipulated Briefing Schedule* (17 February 2017), filed as part of the *Google Warrant* case, *supra* note 7.

[86] Thomas P O'Brien et al, "US Department of Justice May Leverage 'Cooperation Credit' to Obtain Foreign-Based Evidence," *Paul Hastings* (23 November 2015), online: <http://www.paulhastings.com/publications-items/details/?id=boade769-2334-6428-811c-ff00004cbded>.

[87] *eBay* case, *supra* note 6.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

"formalistic in the extreme[88] to say that it was not actually in the possession of the Canadian company. The extraterritorial jurisdiction aspects of the disclosure order were avoided by this construction of the facts, though no true consideration was given to the international law issues or to the relevant state practice, perhaps because it was not raised by the parties.

As for Parliament, the Supreme Court of Canada noted in *Tele-Mobile Co. v Ontario* that the federal government had stated that it enacted production orders in the *Criminal Code* as a means of compelling individuals with possession or control over data located outside Canada to surrender it, so as to solve "the problem that has in part been created by inexpensive overseas data warehousing."[89] The implicit position is clearly that jurisdiction over the individuals who possessed or controlled the data is sufficient jurisdiction to order its production. This measure was taken seemingly without much[90] consideration of whether it was consistent with international law or, indeed, without recognition that Canada itself had opposed such measures before US courts.[91]

Also worth mentioning is the long-running struggle between the criminal authorities of Belgium and Yahoo, which began with a run-of-the-mill fraud investigation launched in 2007. Belgian authorities demanded that Yahoo produce Internet protocol addresses associated with email accounts that were implicated in the investigation, but Yahoo refused on the basis that it was not present in Belgium as it had no business infrastructure there and, thus, did not fall under Belgium's territorial jurisdiction. At every stage of the proceedings, it argued that the appropriate manner for Belgium to gather the data was by way of a MLAT request.[92] In December 2015, the Cour de Cassation upheld lower court rulings against Yahoo,[93] on the basis that the broadcast of Yahoo's services into Belgium gave it sufficient presence to base jurisdiction on the extended territoriality principle.

[88] *Ibid*, para 48 (Federal Court motion judgment).

[89] *Tele-Mobile Co v Ontario*, 2008 SCC 12, [2008] 1 SCR 305, para 40, quoting the statement of the parliamentary secretary to the minister of justice after second reading of the bill that created production orders. *Criminal Code*, *supra* note 4.

[90] The parliamentary secretary's statement did acknowledge the "nagging issue" of "extraterritorial searches," but simply presented the production order as a means of resolving the issue (*ibid*).

[91] *United States v Bank of Nova Scotia*, 740 F2d 817 (11th Cir 1984), in which the government of Canada was granted *amicus curiae* standing on the issue, though its argument was unsuccessful.

[92] See Steven de Schrijver & Thomas Daenens, "The Yahoo! Case: The End of International Legal Assistance in Criminal Matters" (September 2013), online: <http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1>.

[93] The court's ruling is available online (in Flemish): <http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1>.

Accordingly, Yahoo was required to respond to the request. The case appears to have proceeded on the assumption (similar to the Canadian position) that if Yahoo was within Belgium's jurisdiction, the latter could lawfully demand production of the data, without any explicit consideration of the *Microsoft Ireland* issue.[94]

To say that something is controversial or opposed in some examples of state practice is not, however, to say that the issue is settled. The Court of Appeals factums of the various parties and interveners in the *Microsoft Ireland* case display an interesting array of arguments that sketch out some of the major legal and policy angles. It is worth briefly reviewing some of these arguments for that reason, although the focus here will be on the international law issues rather than on the local legal peculiarities. Microsoft itself rested its argument essentially on traditional notions of extraterritorial enforcement jurisdiction: while the assertion of personal jurisdiction over the company and the actual act of disclosing the data to the government might occur on American soil, the execution of the warrant to retrieve the data happens in Ireland, where the data is stored, which amounts to extraterritorial enforcement. Even a proper interpretation of the relevant US statutes produces the conclusion that the MLAT procedure is the lawful route — not least because "in 2006, the US and EU negotiated … a self-executing treaty that expressly favours bilateral cooperation for data seizures, not unilateral intrusions into each other's territory."[95]

Microsoft also pleaded that the case had already caused international discord, a proposition confirmed by both the record of the case and the public dialogue among the state players. Ireland filed an *amici* brief in the case clearly stating its view that its territorial sovereignty was implicated and that the case represented a potential infringement thereof. It also asserted that the matter was covered by the MLAT between the states and indicated its willingness to execute the MLAT process "as expeditiously as possible."[96] Finally, it pointedly mentioned its own law to the effect that Irish courts might be empowered to "order the production of records from an Irish entity on foreign soil," but would give great weight to whether the order would violate the law of the foreign state.[97]

The European Union (EU) and the Council of Europe have taken even stronger postures. A brief was filed by Jan Philipp Albrecht, German member of the European Parliament and vice-chair of its Committee on Civil

[94] Though I make this comment guardedly, as I have only been able to consult English language summaries of the Belgian decisions in question.

[95] *Microsoft Ireland*, *supra* note 2 at 21 (Microsoft brief).

[96] *Ibid* at 7 (Ireland *amici* brief).

[97] *Ibid* at 9.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

Liberties, Justice and Home Affairs. He criticized the lower court decision as having "endorsed the by-passing of the EU MLAT and the respect for foreign jurisdiction inherent therein," his main pitch being that EU privacy protection standards are significantly higher than those of the United States, and, thus, avoiding the MLAT regime prevents the oversight required by European authorities in sharing data.[98] Moreover (and redolent of the earlier manifestations of this problem discussed earlier in this section), if the US court held that Microsoft must comply with the warrant, this would cause a conflict since EU laws would prohibit the transfer of data to the United States. Albrecht also noted that he was the European Parliament's rapporteur for the current negotiations between the EU and the United States for a treaty on the protection of personal data in cooperative criminal investigations.[99] Upholding the warrant, he said, "would forestall this future agreement and disturb these negotiations."[100] This view was supported by a letter from Vivane Reding, vice-president of the European Commission, in which she expressed the view that the magistrate's decision in *Microsoft Ireland* "bypasses existing procedures," is an exertion of extraterritorial jurisdiction that may breach international law, and causes companies to be caught in an untenable conflict of laws.[101] A similar stance was taken by the Council of Europe's commissioner on human rights.[102]

The best international law analysis was presented in the *amici* brief by Anthony Colangelo of Southern Methodist University's Dedman School of Law, who supported Microsoft's overall position but made a number of finer methodological points. He located the central problem as a matter of determining whether the warrant actually amounts to an extraterritorial action by the United States, a question he answered in the affirmative. He emphasized the principle of non-intervention, arguing that the warrant in question is an extraterritorial extension of enforcement jurisdiction into what is clearly a sovereign territorial interest of Ireland's, despite the fact that the intrusion is electronic rather than kinetic.[103] Importantly, the question of extraterritoriality is not appropriately answered unilaterally, as the lower court did, but, rather, with due consideration of the interests and positions of the relevant states, and he submitted that great weight

[98] *Ibid* at 6 (Albrecht brief).

[99] The treaty that resulted is discussed below. See European Commission, *Fact Sheet: Questions and Answers on the EU-US Data Protection "Umbrella Agreement,"* Press Release (8 September 2015), online: <http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>.

[100] *Microsoft Ireland*, *supra* note 2 at 12 (Albrecht brief).

[101] Letter available online: <http://www.nu.nl/files/nutech/Scan-Ares-MEP-in't-Veld-.pdf>.

[102] Council of Europe's Commission for Human Rights, *supra* note 78 at 77.

[103] *Microsoft Ireland*, *supra* note 2 at 10–11, 20–23 (Colangelo brief).

should be given to the views of both Ireland and the EU on this question. Finally, by circumventing the United States–Ireland MLAT, the procedure amounts to a breach of the treaty, specifically the "obligation to implement these agreements in good faith" under the *Vienna Convention on the Law of Treaties*.[104]

The briefs of other interveners and *amici* made a number of a similar points as well as a host of arguments regarding the interaction of US law and international law that are not strictly relevant here. An important point made by a group led by the Electronic Frontier Foundation was that establishing this kind of warrant procedure as permissible could very well lead to foreign regimes with weaker data protection laws feeling emboldened to compel businesses with presences on their territories to surrender the personal data of American citizens[105] — a strong example of the kind of "tit for tat" response that generally makes states conservative about the manner in which they exercise extraterritorial jurisdiction.[106] A coalition of data firms made a similar point, giving the example of personal data of American human rights activists stored on American computers being turned over to the Russian government, a situation that illustrated the kind of "international free-for-all" that could result.[107]

And the decision of the Court of Appeals? Given the amount of international law that was argued, the court's reasons are quite anaemic, turning essentially on the difference between a warrant and a subpoena under the domestic legislation involved (the *Stored Communications Act*).[108] Having decided that the instrument in question was actually a warrant, the court construed the warrant as a very territorially limited species of state action to which the usual statutory interpretation presumption against extraterritorial application applied. This was particularly the case here, given that the *Stored Communications Act* contained no language indicating any congressional intent towards extraterritorial application. The court rejected the government's argument that the order was in fact a kind of subpoena, although it cited its own and

[104] *Ibid* at 34. *Vienna Convention on the Law of Treaties*, 1969, 1155 UNTS 331.

[105] *Microsoft Ireland*, *supra* note 2 (*amici* brief of Brennan Centre for Justice at NYU School of Law, the American Civil Liberties Union, the Constitution Project and the Electronic Frontier Foundation).

[106] See Coughlan et al, *supra* note 17 at 68–71.

[107] *Microsoft Ireland*, *supra* note 2 at 25–26 (*amici* brief of Verizon, Cisco, Hewlett-Packard, eBay, Salesforce.com and Infor).

[108] *Stored Communications Act*, 18 USC § 2701 (1986).

other US case law to the effect that a subpoena requiring an individual in the United States to produce documents held abroad was lawful, without any consideration of the lawfulness of that point under international law.[109]

There was little international law analysis to speak of, other than the acknowledgement that the presumption against extraterritoriality was applied in order not to interfere with international relations. The factual apogee was the court's recognition of two points: (1) that Irish territory was implicated and (2) that Microsoft gathering the data simply amounted to the government acting indirectly rather than directly:

> [I]t is our view that the invasion of the customer's privacy takes place under the SCA [*Stored Communications Act*] where the customer's protected content is accessed — here, where it is seized by Microsoft, acting as an agent of the government. Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States.[110]

The high water mark of international legal analysis arrived in the tail end of the majority's decision, in which the court brushed up against the possibility that international law norms might be breached, though under the scope of "comity" rather than law:

> Our conclusion today also serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of cross-boundary investigations. … [W]e find it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to "collect" from servers located overseas and "import" into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States.[111]

Despite the fact that, as indicated above, the question of whether the warrant amounted to a breach of foreign sovereignty had been argued by the parties, the Court did not really entertain the question of whether there was a prospect of unlawful extraterritorial enforcement jurisdiction. Indeed, at several points in the judgment, there are indications that the

[109] *Microsoft Ireland*, *supra* note 2 at 32.

[110] *Ibid* at 39.

[111] *Ibid* at 42.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

distinction between prescriptive and enforcement jurisdiction was confused by both the government[112] and the court.[113]

Accordingly, for all of the heated discussion around the case, it has thus far resolved very little from an international law point of view; a Supreme Court appeal might change that, but at the time of writing, none had been announced. At most, it is an example of state practice (by way of a court decision) from which it can be indirectly inferred that the state in question feels that the act might be unlawful. Much turned on the fact that warrants are treated more restrictively than subpoenas under US law, which in both practical and international law terms is a distinction without a difference — in each case, the government is compelling a party to surrender data located in the territory of another state. The issue remains the one being explored in this section: is this lawful under international law? Most important, then, is the court's recognition that the execution of the warrant would take place in Ireland, despite being electronically initiated in the United States by a US company. As explored in detail above, this tends to be the position taken by states, and while the court did not refer to it, this view was reflected in the record. This point becomes more important in the actual international law analysis of the question, taken up the following section.

STATE PRACTICE

To the extent that the Irish and European positions expressed in the *Microsoft Ireland* case might be taken as expressions of *opinio juris* on the *Microsoft Ireland* issue, an examination of state practice reflects an even greater level of dissonance between *opinio juris* and state practice

[112] *Ibid.* At note 20, the court rejects a government argument that the presumption against extraterritoriality does not apply to the warrant provisions because they are procedural rather than substantive. The government seems to be missing the point that enforcement jurisdiction is quintessentially procedural since procedure amounts to actual actions by the state (as opposed to simply passing legislation that contemplates extraterritorial application), and that any presumption against extraterritoriality should apply with even more force to "procedure."

[113] For example, the amount of energy expended on the presumption against extraterritorial application obscures the fact that what is usually being discussed is whether the legislature (in this case, Congress) intended the legislation to apply to something outside the state's territory (prescriptive jurisdiction). There was no separation of the actual issue of whether the statute purported to empower the government to act outside its territory (enforcement jurisdiction), though this is where the court's decision ultimately rested. Also, at page 30, there is a discussion regarding the subpoena power, in which the Court appears to accept the conclusion from the earlier case law that an enforcement power (the subpoena) can be based on the fact that the state has prescriptive jurisdiction — though in fairness the court was simply summarizing the effect of that case law and not analyzing it.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

than is the case with the more general cross-border data seizure issue. In some cases, the dissonance is quite striking. For example, as mentioned above, while the United States and the United Kingdom are negotiating a treaty that will allow warrants for foreign-stored data to be executed, each has in place laws allowing the state to compel individuals within their territories to surrender data stored abroad;[114] and as also noted above, despite Ireland's sovereignty-oriented posture in the *Microsoft* case, it admits it has the same kinds of mechanisms available.[115] While one might suspect that France would be amenable to the position expressed by the EU and European Commission officials, French courts recently asserted jurisdiction to order Twitter to produce data relating to anti-Semitic hashtags that violated French laws,[116] dismissing Twitter's protestations that the data were stored in the United States.[117]

Beyond these well-publicized incidents, actual practice relating to the *Microsoft Ireland* issue can be difficult to track, as it tends to be rolled into the overall cross-border data question in the literature. However, a useful paper produced by international law firm Hogan Lovells in 2012 surveyed the issue quite directly with regard to ten different states,[118] and some indications of other state practice can be found in the doctrinal literature.[119] A chart that provided a rough illustration of this available data on state practice, then, would look like this:

[114] The United Kingdom's law is the *Investigatory Powers Act*, *supra* note 67; the US position is itself illustrated by the *Microsoft Ireland* case and see also Winston Maxwell & Christopher Wolf, "A Global Reality: Governmental Access to Data in the Cloud: A Comparative Analysis of Ten International Jurisdictions," Hogan Lovells White Paper (18 July 2012).

[115] *Microsoft Ireland*, *supra* note 2 (Irish *amicus* brief); see also Maxwell & Wolf, *supra* note 114 at 10.

[116] Angelique Chrisafis, "Twitter Gives Data to French Authorities after Spate of Anti-Semitic Tweets," *The Guardian* (12 July 2013), online: <http://www.theguardian.com/technology/2013/jul/12/twitter-data-french-antisemitic-tweets>.

[117] Angelique Chrisafis, "Twitter under Fire in France over Offensive Hashtags," *The Guardian* (9 January 2013), online: <http://www.theguardian.com/technology/2013/jan/09/twitter-france-offensive-hashtags>.

[118] Maxwell & Wolf, *supra* note 114. It is worth noting that some of the conclusions in the article were argued to have been overstated by European law enforcement officials, though apparently only to the extent that states permitting a *Microsoft*-style compulsion of data do so within limitations that involve the assessment of the state's territorial connection to the matter, individual, or data in question (T-CY, *Transborder Access and Jurisdiction*, *supra* note 48 at 48). The fact remains, however, that a number of states permit the technique to operate.

[119] Particularly Koops & Brenner, *supra* note 36.

Compel without MLAT	**Compel only where MLAT/cooperation**
Australia	Germany
United Kingdom	Japan
France	Brazil
Canada (though laws untested)	Netherlands
Denmark	South Korea
Ireland (though not clear)	New Zealand
Italy	EU
Spain	
Portugal	
Romania	
Malaysia	

There is certainly a bipolar quality to this situation. As one commentator remarked on the similar topic of surveillance, "[i]n this environment, the same action in response to a surveillance directive may be at once both legally required by one government's laws and legally forbidden by another's."[120]

ANALYZING THE PROBLEM

In light of the foregoing, the most that can be said about the issue from a customary international law point of view is that the current landscape reflects the overall state of play on cross-border electronic evidence gathering more generally. While states generally take a territorial sovereignty point of view, there is a dissonance between what states say (*opinio juris*) and what they do (state practice). In order to properly analyze the problem, then, we must resort to first principles. In my view, there is a compelling argument that a state engaging in behaviour similar to that of the US government in the *Microsoft Ireland* case is in breach of international law, specifically the prohibition on extraterritorial enforcement jurisdiction.

This point of view can emerge from both factual and legal analysis. Factually, a private individual is being compelled by the state to obtain data that it owns, possesses, or controls, which is stored on the territory of another state. It is important not to fall into the "computers are different" fallacy and remember that, despite its seemingly ephemeral quality, stored data like the kind at play in *Microsoft Ireland* is a physical thing that is quantitatively present in the foreign state. It is not truly any different than if the individual were being asked to obtain paper documents, or even tractors, from the foreign state.

Legally, the state's power to compel the surrender of things — enforcement jurisdiction — is being extended into the territory of the foreign state,

[120] Kris, *supra* note 12.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

absent the latter's permission and, in some circumstances, violating its laws. From a state responsibility point of view, it matters not that the courts or state entities issuing the compulsory orders are acting within their domestic jurisdiction and compelling entities that are within the issuing state's territory, because the ultimate effect is extraterritorial; that is to say, the breach of the customary prohibition on extraterritorial enforcement occurs at the moment the data is gathered by the compelled entity on the foreign state's territory and the compulsory order is consummated. The conduct is certainly attributable to the issuing state, since on any reasonable construction of the concept of agency the compelled individual is acting as the agent or proxy of the issuing state. This seems true whether the actors are properly considered to be the courts or the government and thus caught under Article 4 of the *Draft Articles on State Responsibility* or the compelled private individual itself, since it is under the direct control of the state and thus caught under Article 8.[121]

As outlined in the first section of this article, this kind of behaviour has been considered objectionable by states since the pre-digital era. Notably, this is a kind of conduct that is not just viewed by states as being unfriendly but also as directly engaging their territorial sovereign interests, as can be seen by the various European reactions to the original *Microsoft Ireland* decision. As explained in the previous subsection, laws and practice at the state level can certainly be viewed as fractured, but given that international law is consent based, the most methodologically sound reaction to this situation is to revert to the more conservative, positivist position. The balance of the evidence points to the conclusion that states view this kind of compulsion as unlawful when it is directed at their territories. Accordingly, until a clearer or more nuanced picture emerges, in my view it is safe to conclude that a *Microsoft Ireland*-style warrant, if executed, breaches the rule against the exercise of extraterritorial enforcement jurisdiction.

Conclusions

As noted at the outset of this article, the goal here has been relatively modest. It has been to demonstrate that the issue raised in the *Microsoft Ireland* case has generated further controversy in an already fractured discussion about how transnational electronic evidence gathering can, does, and should proceed. It has also sought to demonstrate that while the dialogue on the issue has framed this as a law enforcement issue with international aspects, it is best understood as an international law problem that pertains to law enforcement. And it will be concluded here that the latter point is more than a semantic one, in that international law problems require

[121] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, UN Doc A/56/10 (2001), arts 4, 8.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press

international law solutions — solutions that, to be sure, can be aided by the adoption of technological solutions and by inter-law enforcement dialogue at every level, but because of the sovereignty concerns involved, must ultimately take the form of old-fashioned inter-state cooperation.

Much heat is being generated on this issue, particularly as both the *Microsoft Ireland* and *Google Warrants* cases wend their way through the American court system, but thus far there is little light, at least in terms of solutions gaining traction.[122] Clearly this is a problem that is in need of a solution. On the law enforcement side, there is clear indication that the MLAT system as it currently exists is simply inadequate for the task, and this inadequacy may be leading to more informal, even unlawful, actions by the police. From the point of view of individuals and civil society, without distinct rules around cross-border evidence gathering, procedural protections do not necessarily follow the investigative actions. People are more likely to be subject to prosecution as a result of these activities, but potentially less protected by human rights regimes,[123] not to mention the principle of legality. And the problem is as pressing as it is intractable. As the Council of Europe's Cybercrime Convention Committee framed it in a 2014 report:

> in the absence of an agreed upon international framework with safeguards, more and more countries will take unilateral action and extend law enforcement powers to remote transborder searches either formally or informally with unclear safeguards. Such unilateral or rogue assertions of jurisdiction will not be a satisfactory solution.
>
> Furthermore, as victimisation grows, the public will ask why governments are not able to obtain data in a reasonable and legitimate way when lives are in danger and why justice frequently cannot be done.[124]

In terms of what solutions might be generated, that is far beyond the scope of this article. However, to return to the jurisdictionalist paradigm invoked at the outset, I would venture that in international law terms this is a jurisdictional problem that is in need of a jurisdictional solution. As old-fashioned as it might seem, some form of treaty arrangement, probably at both the bilateral and multilateral levels, offers the most practical solutions. As noted above, there is activity on this front, and there will undoubtedly be more to come.[125] What is vital, perhaps, is the manner in

[122] *Google Warrants*, *supra* note 7.

[123] Paul de Hert, "Cybercrime and Jurisdiction in Belgium and the Netherlands: *Lotus* in Cyberspace — Whose Sovereignty Is at Stake?" in Koops & Brenner, *supra* note 36, 71 at 110.

[124] T-CY, *Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY*, Doc T-CY (2014) 16 (3 December 2014) at 13–14 [T-CY, *Transborder Access to Data and Jurisdiction*].

[125] See note 60 above.

which this international law problem is solved and, in particular, that it not be solved simply to smooth the way for law enforcement but, rather, in a way that is mindful of the various concerns at play. In a recent piece, Jennifer Daskal and Andrew Woods proposed a simple, but effective, set of principles that might guide these efforts, arguing that such cooperation should be undertaken in a way that accomplishes: (1) expedited and reciprocal access to data; (2) significant attention to human rights requirements; and (3) the embedding of transparency and accountability.[126] In terms of human rights protections, the Internet and Jurisdiction Project has proposed six "building blocks for fair process": authentication, transmission, traceability, determination, safeguards, and execution.[127] Gail Kent has made quite detailed proposals for medium- to long-term solutions involving the creation of international agreements around data transmission regimes that harness technological tools and industry know-how.[128]

Most recently, some of these proposals have seen active implementation in the form of the newly in force *Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences*, which seeks to provide a governing framework for cooperation between EU states and the United States on information transfers in the criminal context.[129] However, this is clearly not an easy effort, as even in the EU space the only consensus that has thus far been built is around a "Guidance Note" on transborder access to data under Article 32 of the *Convention on Cybercrime*.[130]

There is no doubt that the nature of both electronic data and the Internet's infrastructure present challenges to the operation and application of

[126] Jennifer Daskal & Andrew K Woods, "Cross-Border Data Requests: A Proposed Framework," *Just Security* (24 November 2015), online: <https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/>.

[127] Internet and Jurisdiction Project, online: <http://www.internetjurisdiction.net/uploads/pdfs/Papers/Internet-Jurisdiction-SYNTHESIS-3-July-2013.pdf>.

[128] Kent, *supra* note 37 at 10–25.

[129] *Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences*, [2017] OJ L336/3, online: <http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=10861>. The Electronic Privacy Information Centre is following this development closely and has significant resources posted at <https://epic.org/privacy/intl/data-agreement/>.

[130] T-CY, *Guidance Note no 3*, *supra* note 54. After studying the issue and surveying state opinion, the T-CY had earlier concluded that a proposed protocol to the Convention addressing transborder access to data "would not be feasible." T-CY, *Transborder Access to Data and Jurisdiction*, *supra* note 124 at 13.

jurisdictional principles, particularly in the realm of enforcement, and this has put stress on that body of norms. Most of the literature in this area is geared towards figuring out essentially whether there is a "better way to do it," and it may be that such a better way can evolve and perhaps is evolving. However, I would suggest that, while the landscape is rapidly changing, we are by no means in the middle of a Grotian moment in international law in regard to jurisdiction. Notwithstanding these challenges, states still do adhere to a Westphalian-bound model, where things are either here or there, inside or outside their territories. Those most pungent markers of state sovereignty — borders — are as they ever were. Despite the restless advancement of technology, when it comes to the exercise of enforcement jurisdiction, no new frontiers are yet emerging.

https://doi.org/10.1017/cyl.2017.7 Published online by Cambridge University Press