Kennedy, Sally; Warren, Ian

Article

The legal geographies of extradition and sovereign power

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Kennedy, Sally; Warren, Ian (2020) : The legal geographies of extradition and sovereign power, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 3, pp. 1-18, https://doi.org/10.14763/2020.3.1496

This Version is available at:
https://hdl.handle.net/10419/224942

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

The legal geographies of extradition and sovereign power

Sally Kennedy
Deakin University, Geelong, Australia, s.kennedy@deakin.edu.au

Ian Warren
Deakin University, Geelong, Australia, ian.warren@deakin.edu.au

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1496

Abstract: This paper demonstrates how a request for the extradition of a Canadian citizen accused of online child luring by United States authorities opens up a complex series of domestic legal issues regarding access to, use and exchange of evidence under mutual legal assistance requirements. While these arrangements aim to protect vulnerable child victims from predatory online behaviour, they also skew established notions of due process and the rule of law to favour US sovereignty and criminal enforcement power. We conclude by explaining the impact of these issues on the dynamics of global online criminal investigations.

Keywords: Extradition, Mutual legal assistance, Online child sex offences, Sovereignty, Extraterritoriality

Article information

Received: 16 Sep 2019 **Reviewed:** 21 Dec 2019 **Published:** 16 Sep 2020

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/legal-geographies-extradition-and-sovereign-power

Citation: Kennedy, S. (2020). The legal geographies of extradition and sovereign power. *Internet Policy Review*, *9*(3). DOI: 10.14763/2020.3.1496

This paper is part of Geopolitics, jurisdiction and surveillance, a special issue of Internet Policy Review *guest-edited by Monique Mann and Angela Daly.*

INTRODUCTION

Article 24 of the Budapest Convention on Cybercrime (2001) (the 'Budapest Convention') contains specific provisions on extradition for various online offences, including crimes related to child pornography, computer-related fraud, and infringements of copyright (Clough, 2014; Council of Europe, 2001). It introduces jurisdictional requirements that supplement, and in some cases replace, those forged through pre-existing bilateral and

multilateral extradition arrangements that are incorporated into national laws. A key objective for the 47 member nations of the Council of Europe - and 28 other nations that have signed and ratified the Budapest Convention (Council of Europe, 2020), which include the United States (US), Canada and Australia - is to enhance cooperation in the investigation and prosecution of transnational online offending. This includes fast-tracking the extradition process for specified online offences involving terms of imprisonment of 12 months or more (Clough, 2014). These processes work in much the same way as the European Arrest Warrant (EAW) (Warren & Palmer, 2015, pp. 324-338).

While the trans-geographic nuances of online activity generate new forms of digital and data sovereignty where the ownership and control of information moves beyond any single nation state (see Couture & Toupin, 2019), extradition remains wedded to legal principles based on physical territory and national sovereignty. The voluntary nature of ratification also has the potential to limit the reach and enforceability of cooperative transnational treaties. In light of these issues, we argue that the fast-tracking mechanisms of the Budapest Convention do not address the inherent legal and geographic conflicts associated with established extradition procedures that tend to be slow, cumbersome, politically sensitive, and doctrinally technical.

Our central focus in this paper is to demonstrate how complex due process issues are embedded within the process of extradition. These fundamental issues are characterised by conflicting legal geographies that pre-date, and are not reconciled by, the Budapest Convention or other bilateral and multilateral arrangements seeking to fast-track the extradition process, irrespective of the nations involved. We demonstrate that, even with enhanced transnational online surveillance capabilities, investigators and prosecutors must be sensitive to the geographic impacts of due process that pre-date the digital age and have been forged through the historical development of extradition law. This convergence of law and geography has significant ramifications in light of the unknown international scale of global online surveillance by any nation (see Geist, 2015), the impact of this issue on the world's national legal systems (Svantesson, 2017), and the evolving role of extradition in reflecting the apparent willingness of certain nations, such as the US, to commence criminal proceedings for a wide range of offences to protect narrow commercial, moral or law enforcement interests (Bauman et al., 2014). These objectives, we argue, serve to undermine the very types of transnational justice cooperation envisaged by the Budapest Convention.

Extradition must be viewed in light of its ongoing political and legal ramifications that reflect, and contribute to, the degree of international comity between nations. For example, the US and Canada have a long history of contentious bilateral extradition arrangements pre-dating the digital age (Miller, 2016), which inform contemporary approaches to extradition for online and many other forms of offending. The US ratified the Budapest Convention in 2006, while Canada did so in 2015. This temporal split delays the coordination of the Budapest Convention requirements between these two nations, which also have to negotiate distinct approaches to due process that affect domestic criminal procedures for evidence collection, the apprehension and questioning of suspects, as well as the exchange of evidence and fugitives. Each of these factors can potentially undermine transnational justice cooperation and magnify the difficulties of determining an extradition request.

In addition, Article 24(6) of the Budapest Convention incorporates the principle of *aut dedere aut judicare*, alternately known as "extradite or prosecute". This is a central aspect of continental European extradition law that can offset prejudicial disparities "in domestic legal systems with respect to both substantive law and procedure", and the "potential for bias and

prejudice against the surrendered person, based solely on his [sic] foreign origin and nationality" (Plachta, 1999, p. 88). However, this principle is based on nationality, rather than a key aspect of the legal geography that characterises many forms of contemporary cyber offending, where the suspected offender can commit all or most of the wrongful activity outside of the affected jurisdiction (Mann, Warren, & Kennedy, 2018). Significantly, extradition laws and procedures historically developed in line with the presumption that an extraditee had fled the jurisdiction where the harmful act occurred.

As we explain, the contemporary legal geography of extraterritorial crimes involves a direct tension between theories of subjective and objective territoriality. These are central yet highly problematic rationales for asserting jurisdictional power beyond recognised national geographic boundaries. Our argument is framed in light of a leading Canadian case involving a request for extradition issued by the US in 2012 regarding the offence of child luring via the internet. The suspect was physically located in Canada at all times during the incident, but it became clear during approximately seven and a half years of legal proceedings in Canada that US enforcement surveillance had identified several child victims who were not mentioned in the initial extradition request. While this case pre-dates Canada's ratification of the Budapest Convention, we believe it aptly demonstrates the hazards of fostering transnational justice cooperation through distinct national systems, which encompasses both extradition and the transfer of criminal evidence through mutual legal assistance processes. We argue the separation of these issues reflects a different form of due process, or "rule-with-law" (Bowling & Sheptycki, 2015), that ultimately favours granting an extradition request, even if there are discernible due process and human rights concerns linked to the surrender of crime suspects to jurisdictions where their prior connection is limited (Mann et al., 2018).

Our argument proceeds in four parts. First, we outline how subjective and objective territoriality are embedded and highly problematic geographic aspects of extradition, and discuss their relationship to mutual legal assistance processes. Second, we provide a detailed description of the Canadian cases scrutinising the US request for the extradition of Marco Viscomi for alleged child luring. Of particular importance is the range of legal and factual issues considered by Canadian courts, and arguments questioning whether Viscomi could be sufficiently identified as the correct suspect via his subscription to the internet service provider (ISP) address identified by US authorities, an issue that has received limited scholarly attention to date. Third, we discuss the importance of focusing on due process of law in transnational cyber investigations, while at the same time suggesting that prevailing views of the mobility of data must be divorced from the idea that individuals facing extraterritorial criminal charges should be considered equally mobile. We consider this fosters a form of "rule-with-law" (Bowling & Sheptycki, 2015) that prioritises bilateral and multilateral interests in crime control over the protection of individuals who are sought for extradition. We conclude by suggesting the power of any nation to assert extraterritorial criminal jurisdiction is preserved through extradition processes (Svantesson, 2017), while greater credence should be given to holding transnational trials in the geographic location where the harm emanated (Dugard & Van den Wyngaert, 1998; Mann et al., 2018).

TRANSNATIONAL DATA, EXTRADITION AND MUTUAL LEGAL ASSISTANCE

Many authors claim that questions of internet jurisdiction require reformulating due to the

inherently un-territorial nature of global online data flows (Daskal, 2015; Svantesson, 2017). We disagree. This is because due process of law was built into many established stages of the criminal process, including domestic extradition laws and procedures, that sought to deal with transnational offending *before* the advent of the global world wide web. The significant question is whether and how these laws are upheld or subverted in any individual case. For example, the famed Kim Dotcom case, which remains unresolved at the time of writing despite eight years of hearings in the New Zealand (NZ) court system, involved significant questions about the legality of the search of Dotcom's residence by NZ police acting on a request by US authorities. While the parameters of a lawful search were clear under NZ law (Boister, 2017a; Palmer & Warren, 2013), the transnational nature of the offence added increased pressure on NZ investigators, resulting in the selective use of existing laws, or slippages in conventional notions of due process that became a form of "rule-with-law" (Bowling & Sheptycki, 2015). This can also extend to the tactical use of extradition in cases with or without online components, or where a suspect is wanted by one jurisdiction, yet transiting through another to a third destination (*United States of America v. Meng*, 2019). We suggest that rather than introducing new legal requirements to deal with the intricacies of cyber activity, existing extradition laws and due process requirements can appropriately balance the interests of the requesting nation in obtaining justice for transnational cybercrime suspects who might never have entered the jurisdiction where the effects of the wrongful act have occurred (Mann et al., 2018).

Despite these arguments, judicial practice in most Western nations remains tethered to the prevailing view that those suspected of online criminal activity should be considered as geographically mobile as the digital harms and evidence associated with their behaviour. We suggest the fast-track extradition measures in Article 24 of the Budapest Convention reflect this view. This logic can produce a complex set of legal geographies associated with sovereign power, particularly during extradition processes involving online child sex offences, where questions of bilateral and multilateral political comity risk undermining individual due process and human rights protections under the laws of extradition (Arnell, 2013; Arnell, 2018; Blakesley, 2008; Dugard & Van den Wyngaert, 1998; Murchison, 2007). We suggest that a renewed emphasis on established geographies of extradition is required to fully appreciate the limits of altering these processes for online offences. This requires understanding the distinction between subjective and objective territoriality, which was consolidated by the Harvard Draft Extradition Convention (see Burdick, 1935) and is regularly cited by leading scholars as a central geographic aspect of extradition law (Blakesley, 1984).

Subjective territoriality can serve as a bar to extradition by locating the trial where any key element of the crime has emanated, regardless of whether the effect is felt elsewhere. The forum bar test in English extradition law reflects this principle (Mann et al., 2018). By contrast, objective territoriality, or the "effects test", allows a nation to assert jurisdiction extraterritorially by commencing prosecution where the harm was experienced (Raustiala, 2009). Objective and subjective territoriality apply to various forms of criminal conduct, and have been asserted inconsistently by some jurisdictions, such as the US, to assert jurisdiction over offences with limited territorial impact (Blakesley, 2008, p. 137). However, most extradition requests are predicated on subjective territoriality, under the assumption that the offender is a fugitive from the location where the harm was committed (Abelson, 2009). Where the offence has occurred remotely, objective territoriality might make logical sense in terms of the nature of victimisation (Svantesson, 2017). However, this principle also raises many concerns about potential bias, because objective territoriality emphasises conceptions of harm, justice and penalty that are forged solely from the perspective of where the effects are experienced. This emphasis can serve to undermine due process for suspects located offshore at

the time of the offence (Mann et al., 2018).

We contend objective territoriality is less tenable in a digital age, where different nations are likely to share concurrent jurisdiction for the same conduct (Burdick, 1935, p. 93; Mann et al., 2018), and online crime suspects could be particularly disadvantaged by being extradited to a nation simply because it has chosen to exercise jurisdiction over their allegedly criminal offshore conduct. This logic becomes especially problematic as the impacts of most forms of transnational cyber offending are experienced in multiple locations, or in a single jurisdiction outside an alleged offender's immediate geographic setting. This enables the domestic surveillance, investigative processes and criminal laws of the requesting nation to be enforced transnationally, which can have problematic due process implications for the legality of cross-border operations involving multiple police agencies with different domestic investigative and surveillance powers (Bowling & Sheptycki, 2015), as demonstrated by the Kim Dotcom case (Boister, 2017a; Palmer & Warren, 2013). Moreover, shifting the trial forum, rather than extraditing an alleged offshore suspect, is less problematic in light of the global convergence of domestic cybercrime laws under instruments such as the Budapest Convention.

The inherent complexity of extradition and mutual legal assistance offsets the idea that both processes can simply be fast-tracked for certain types of crime. Each is activated by a series of formal requests between nations that are mediated by the judicial and executive arms of government. This creates a relatively complicated structure of judicial review in a receiving state if an extradition or mutual legal assistance request is challenged by a suspect. Whilst politicisation can create uneven or hierarchical relationships between nations, in some cases, such as the Gary McKinnon case in the UK, political oversight can offer an important accountability measure to foster bilateral legal cooperation, or potentially block the surrender of individuals or evidence for important humanitarian reasons (Mann et al., 2018). However, the primary responsibility for determining the legality and enforceability of an extradition request lies with the courts of the nation that receives the request, while model rules for mutual legal assistance offer considerable latitude for the "expedited preservation and disclosure of stored computer data, production of stored computer data and search and seizure of computer data" at the transnational level (Clough, 2014, p. 731). The admissibility of such evidence will ultimately be scrutinised at the trial location.

In supranational jurisdictions, such as the EU, streamlined procedures can simplify and fast-track the exchange of fugitives or evidence, including electronic evidence. For example, the EAW and European Evidence Warrant (EEW) operate in conjunction with the European Investigation Order (EIO). This structure aims to provide more direct transnational justice cooperation by attempting "to remove geographic boundaries through a form of centralisation" based on mutual trust in the operation of the established justice institutions of nations that are part of the EU (Warren & Palmer, 2015, p. 341). However, this regime is also criticised for prioritising the interests of the EU and national justice agencies at the expense of preserving the due process rights of individuals subjected to these streamlined procedures (Gless, 2015). It also raises significant questions about whether trust in transnational legal relations and international comity can extend beyond the EU, while retaining some degree of protection for individuals suspected of engaging in transnational crimes.

Although these cooperative transnational processes are forged through bilateral or multilateral agreements, including the Budapest Convention, that are subsequently incorporated into the domestic laws of Anglo-Western jurisdictions, there are growing concerns that many jurisdictions are too willing to accede to the enforcement interests of powerful nations, such as

the US. This is particularly evident in cases where an alleged online offender might never have physically entered the country (Mann et al., 2018; Palmer & Warren, 2013) or where digital platforms associated with the offence are owned, operated or governed by US laws and surveillance protocols (Geist, 2015; Goldsmith & Wu, 2006; Warren, 2015). Thus, rather than being un- or trans-territorial (Daskal, 2015), much online data in the English-speaking world is subject to the superior surveillance, enforcement and regulatory power of US corporate and law enforcement interests (Mann & Warren, 2018; Warren, 2015; Zuboff, 2019). This does not mean the US is the only jurisdiction exercising extraterritorial criminal enforcement and surveillance powers in similar ways. However, extradition and mutual legal assistance become benchmarks for determining where a criminal trial should proceed in light of various forms of extraterritorial online surveillance. This increasingly occurs in circumstances where justice officials of the receiving state might have been totally unaware of the alleged online misconduct, or where domestic laws in the jurisdiction issuing the extradition request establish different due process and human rights protections for citizens compared with non-citizens (US Department of Justice, 2019).

Case studies documenting extradition and mutual legal assistance indicate it can be viable to shift the location of a criminal trial to the source of the harm to facilitate prosecution whilst simultaneously protecting individual rights (Mann et al., 2018). This can prevent undue hardship when surrendering a suspect who has never entered the requesting country to face a potentially lengthy criminal trial or sentence if they are ultimately convicted. The idea of a "forum bar", which blocks extradition if a substantial proportion of the offence occurred in the jurisdiction where the extraditee is located, alters the jurisdictional geography of the incident by recognising the offence can be prosecuted at the source of harm (Mann et al., 2018). This relies on evidence obtained at the source of the crime, as well as evidence shared by foreign enforcement agents being shifted to accommodate the location of the suspect, rather than moving the individual to accommodate the interests of justice. This emphasis can streamline the otherwise lengthy series of appeals on technical aspects of extradition and mutual legal assistance, even if it remains outside the accepted contemporary norms of transnational justice cooperation.

Our examination of these issues involves the case of Canadian citizen Marco Viscomi. His challenges to extradition reinforce the complexity and time-consuming nature of these processes that must also consider the requirements of the Canadian *Mutual Legal Assistance in Criminal Matters Act* (1985) (*MLACMA*) and *Charter of Rights and Freedoms* (1982) (the *Charter*). These laws predate the Budapest Convention, which did not apply to Viscomi pending Canada's formal ratification in 2015. However, the decisions affecting Viscomi are important for highlighting the legal, surveillance and jurisdictional geographies that support US criminal law enforcement interests, while revealing equivalent problems with the inherent structure of extradition that can occur beyond these two nations.

THE COMPLEX CASE OF MARCO VISCOMI

Between May 2013 and November 2019, Marco Viscomi appeared before the Canadian judicial system on 13 reported occasions to challenge the US request for his extradition to face a charge of child luring. Child luring is the Canadian equivalent of US charges of sexual coercion of a minor and transporting visual depictions of sexually explicit conduct involving a minor through a computer. However, it is unclear whether either of these offences amount to child grooming, which is a notable omission from the Budapest Convention (Clough, 2014, p. 702). If convicted

under US law, Viscomi would be subject to a mandatory term of up to 30 years imprisonment. The appendix to this paper highlights the grounds for each decision, and demonstrates how Canadian courts have classified the evidentiary and procedural elements of the extradition request. Our emphasis in this section documents the legal and factual issues considered by the Canadian courts based on the allegations contained in the US extradition request.

US authorities claimed Viscomi communicated with a 17-year-old female located in Virginia Beach on 5 and 6 January 2012 via the internet chat room Tiny Chat. This communication progressed to a Skype video call, where Viscomi could see the young woman, but she could not see him. During the course of the online conversation, it is alleged Viscomi "coerced, threatened, extorted and otherwise manipulated this naïve young woman" into exposing her breasts and engaging in explicitly sexual and violent activities with her 13-year-old sister for his own "voyeuristic pleasure" (*United States of America v. Viscomi*, 2013, para. 2). The Skype session lasted approximately one hour and ten minutes, and Canadian authorities later discovered Viscomi had captured sexually explicit images of the two US victims on his computer.

A two-month investigation commenced after the girls' father reported the incident to US police, who conducted a forensic examination of the victim's computer. This led to an administrative subpoena being issued to Skype that revealed the screen and account names of the suspect, which were then linked by US authorities to an Internet Protocol (IP) address connected to Zing Networks, an ISP operating in Ontario. US police then made a request under the Canadian *Personal Information Protection and Electronic Documents Act* (2000) (*PIPEDA*) for Zing Networks to "voluntarily disclose any information needed to satisfy [the] government request" (*United States of America v. Viscomi*, 2014, para. 21). Common law at the time determined that an equivalent request by Canadian authorities did not require a search warrant (*R v. Ward*, 2012).

On 7 March 2012, US authorities shared details of the investigation with police in Ontario, who commenced their own inquiries. At the same time, US authorities were investigating another cross-border child exploitation case in Wisconsin linked to the same IP address, which involved "virtually identical predatory methods" (*R v. Viscomi*, 2016b, para. 61). This investigation was disclosed to authorities in Ontario, but the major focus of Viscomi's extradition and mutual legal assistance claims involved the evidentiary and legal issues associated with the Virginia Beach communications only.

The information provided to Ontario police by US authorities before the formal extradition request led to search warrants being issued at Viscomi's family home and student residence. After seizing three laptops and external hard drives, which were forensically examined in Canada, Viscomi was charged with two counts of child luring, extortion and uttering threats, which proceeded through the Canadian judicial system for approximately four and a half months. These charges were withdrawn on 10 August 2012 when the US issued its extradition request. On 16 August 2012, Viscomi was apprehended under an extradition arrest warrant based on the Record of the Case. This is the requesting state's summary of the evidence that supports the allegations, which at this stage in Viscomi's case only contained evidence obtained by the US authorities. He was also denied bail "for the protection of the public" due to the "horrific" facts of the case, including the "systemic psychological and physical abuse of children … [and] sadistic, sexualised conduct … which verges on torture" (*Viscomi v. Ontario (Attorney General)*, 2014, para. 6).

Our discussion of the progression of cases focuses on three key legal issues raised by Viscomi that questioned his eligibility for extradition, and the legality of the evidence obtained from both

US and Canadian searches. These issues raise doubts about the connection between the ISP account and Viscomi's identity as the person who unlawfully communicated with the US victims, the process of evidentiary exchange between US and Canadian authorities, and the human rights implications of Viscomi's surrender.

I. ISP AND IDENTITY

A key element of any extradition request is the ability to identify the suspect. Viscomi's identification was determined via his ownership of the Canadian ISP account. US authorities verified this through the chat log obtained from the victim's computer in Virginia Beach, which recorded screen and account names that were traced back to Viscomi's IP and residential addresses. Canadian authorities later determined this evidence matched Viscomi's Ontario driver's licence. Viscomi claimed this evidence did not sufficiently prove he was using the Canadian ISP account at the time of the incident. This contradiction between competing interpretations of the ownership and use of the Ontario ISP demonstrates several intersecting aspects of legal geography that were examined by Canadian courts. For example, the decision that Viscomi was the user of the account impacted the decision to deny bail, which can be granted in Canadian extradition proceedings unless detention is considered necessary to ensure attendance in court, for public safety or to maintain confidence in the administration of justice (see *United States of America v. Meng*, 2019, para. 22). These questions also inform rulings about the legality of evidence collected and exchanged through formal and informal trans-jurisdictional communications between the Canadian and US authorities (Bowling & Sheptycki, 2015; Palmer & Warren, 2013).

Viscomi claimed the US ISP evidence did "not logically connect him to the offence [and] amounts to no more than speculation that he may have been the perpetrator" (*United States of America v. Viscomi*, 2013, para. 8). However, the first Magistrate's ruling in 2013 supported a "reasonable inference" that Viscomi was the offender, which would justify proceeding to trial under Canadian law, even though it could not be conclusively proved he was the Skype user at the time of the US offences (*United States of America v. Viscomi*, 2013, para. 17). Notably, this allegation did not rest on any evidence collected from two Ontario search warrants that was later conveyed to US authorities under the mutual legal assistance sending procedure.

However, during the course of these proceedings, Canadian common law governing ISP evidence changed. The 2013 ruling in Viscomi was governed by the precedent established in the Ontario case *R v. Ward* (2012). This case ruled that Ontario police did not require a warrant to obtain ISP information. This ruling was subsequently overturned by the Canadian Supreme Court in *R v. Spencer* (2014), which determined that any information obtained from an ISP amounts to a search under section 8 of the *Charter*. If an ISP search is conducted without a warrant, any evidence can be excluded from trial in a Canadian court. Viscomi sought the "benefit of this change in the law, in order to argue retrospectively" that the warrantless search, and "all the subsequent warranted seizures that relied on it", violated his section 8 *Charter* rights (*Viscomi v. Ontario (Attorney General)*, 2014, para. 46).

This argument raises a temporal dimension to Viscomi's claims, as *Spencer* was handed down *after* Canadian evidence had been transferred to US authorities under the *MLACMA* proceedings. The key ruling on this issue was handed down in June 2015. It supported Viscomi's claim that ownership and use of the ISP account were separate and insufficient to infer he had committed the alleged US offences.

> The evidence could reasonably lead to a finding that Marco Viscomi … was the *subscriber* to the IP address at the time the crime was committed utilizing that IP address. However, on that evidence alone, it was simply too great a leap to draw the inference that he was the *user* of the IP address at the relevant time. (*United States of America v. Viscomi*, 2015, para. 18, emphasis in original)

Thus, Canadian law favoured the view that "information regarding the subscriber and the IP address cannot, without more, provide the necessary link to draw an inference about who used that IP address at a particular time" (*United States of America v. Viscomi*, 2015, para. 29). This meant US authorities required a stronger factual connection between the identity of the person involved in the Skype conversation and the holder of the Canadian ISP account. Presumably, this could only be possible by transferring the evidence obtained by Canadian authorities from the searches of Viscomi's computers. However, rather than specifying this requirement, the 2015 ruling indicated the initial decision regarding the connection between a subscriber and user of an ISP involved "a misapprehension of the evidence". In other words, there was:

> nothing … to establish that the *subscriber's residential address* and the *address associated with the IP address* are one and the same. Indeed, there is no evidence to explain what an IP address is, in the context of this case, or how it worked. We do not know on this record whether an IP address identifies a particular subscriber only, or a particular device only, or whether it identifies a particular residential address at which the IP address is located, or even whether the IP address is limited to one particular residential location or could have been used at different locations. (*United States of America v. Viscomi*, 2015, para. 25, emphasis in original)

This case also examined Viscomi's claim that a retroactive application of the 2014 *Spencer* ruling mandated the exclusion of evidence from a warrantless ISP search under section 24(2) of the *Charter*. However, this argument was rejected because the Canadian police in *Spencer* believed a warrant was not required, and the *Charter* breach was not considered sufficiently serious in light of the alleged offending to deem the evidence from the ISP inadmissible. This may mean that ISP evidence could still sustain prosecution under Canadian law, or support a police investigation into Viscomi's activities by US authorities, as the protection of the *Charter* does not apply outside the physical territory of Canada. The only way Canadian courts would accept an extraterritorial extension of the *Charter* would be for US police to commence "a lawful procedure in making contact with a Canadian entity" that could legally convert them "into Canadian actors" (*United States of America v. Viscomi*, 2015, para. 49). However, this result is questionable, as it would create "no basis for distinguishing between the conduct of Canadian and foreign officials in cases involving international police cooperation" (*United States of America v. Viscomi*, 2015, para. 49). This would ultimately render any legal and procedural distinctions between US and Canadian police search, seizure and evidentiary requirements irrelevant when dealing with transnational cyber-investigations.

II. MUTUAL LEGAL ASSISTANCE AND THE EXCHANGE OF EVIDENCE

The Canadian *MLACMA* is a key aspect of cooperative "investigative" procedure that gives life to the bilateral mutual legal assistance treaty (MLAT) between the US and Canada. The *MLACMA* procedure entitles US police "to obtain information about a US crime from a witness located in Canada who is willing to voluntarily assist" (*Viscomi v. Ontario (Attorney General)*, 2014, para. 43), and supplements the *PIPEDA* request that led to Zing Networks disclosing Viscomi's ISP details. However, evidence from the Canadian police searches must comply with the *MLACMA* "investigative" procedures, which aims to ensure the transnational exchange of evidence remains "expeditious" and "confidential" (*R v. Viscomi*, 2015, para. 30).

Canadian courts identify a "duty by treaty … to maintain the confidentiality of the MLAT application" and offer the "widest measure of mutual legal assistance" to limit the potential for a suspect to "meddle" in a transnational investigation (*Viscomi v. Ontario (Attorney General)*, 2014, para. 26). This aims to prevent the "loss of any evidence that has not yet been seized, [by] tipping off suspects, associates or accomplices in Canada or abroad" to ensure "the successful expeditious completion of the investigation" (*R v. Viscomi,* 2015, para. 52). As a key component of transnational investigative procedure, *MLACMA* processes must remain confidential, which enables law enforcement agencies "to quickly complete an investigation before the suspects become aware", while fostering a "legitimate interest in protecting the secrecy" of collaborative police processes (*R v. Viscomi*, 2015, para. 36).

Viscomi claimed he had a right to know about and legally challenge the sending procedure that enabled US police to issue the second extradition request. This was accompanied by a second Record of the Case containing evidence originally collected during the search of Viscomi's computer by police in Ontario that was sent to US authorities under the Canadian *MLACMA*. Viscomi claimed the confidential nature of the gathering and sending procedures under the Canadian *MLACMA* was unlawful, because he had no opportunity to scrutinise or contest the procedure in open court.

The second Record of the Case contained an expansive list of evidence, including images of and chat logs with the Virginia Beach victims involving the Skype screen name "Jamie Paisley" that corresponded with the January 2012 incident, images of and chat records with other young women, and links to IP addresses connected to Viscomi. This evidence also disclosed a common methodology, involving threats to install a remotely activated Trojan virus onto the victims' computers if they did not follow the Skype user's instructions (see *R v. Viscomi*, 2016a, paras. 40-42; *R v. Viscomi*, 2016c, para. 14). The obvious need to intercept and prosecute such transnational conduct highlights why both mutual legal assistance and extradition procedures must be conducted as expeditiously as possible (*R v. Viscomi*, 2015, paras. 25-30; *R v. Viscomi*, 2016a, para. 57).

However, MLAT procedures can also promote undue secrecy, as transnational criminal investigations are not grounded in a clear body of neutral laws that enshrine due process (Boister, 2017a; Bowling & Sheptycki, 2015; Palmer & Warren, 2013). While a right to know about and legally challenge a sending order under the *MLACMA* could compromise a complex cyber-investigation, the timing of this form of evidence disclosure also had direct bearing on Viscomi's ability to contest extradition. Canadian courts have found no "air of reality" to

Viscomi's claim that the original Canadian search warrants were invalid (*R v. Viscomi*, 2016a, para. 73), which could have resulted in the transfer of unlawfully obtained evidence to US authorities to support their investigation. This is a problem revealed in other transnational cyber-investigations instigated by the US, yet conducted according to the policing laws of other nations, such as the Kim Dotcom case (see Palmer & Warren, 2013). Moreover, as the second US Record of the Case openly disclosed the evidence transferred from Canada, the legality of the confidential exchange of evidence under the *MLACMA* has been consistently upheld. This did not prevent Viscomi from raising concerns about the ability of transnational evidence exchange to violate his fundamental rights under the Canadian *Charter*.

III. HUMAN RIGHTS ARGUMENTS

The relationship between extradition and human rights law is predicated on mutual trust that the justice systems in each participating jurisdiction operate according to common agreed standards (Marin, 2011). Thus, specific human rights protections within extradition treaties are generally limited (Boister, 2003). The application of international human rights safeguards can also be difficult to achieve in domestic courts (Murchison, 2007), even though they often play a crucial role in protecting individuals (Rose, 2002). Therefore, domestic rights protections such as the *Charter*, US Constitution and other national due process mechanisms play an important role in protecting individual rights during extradition. However, human rights protections become more difficult to balance alongside legal discussions of standard extradition principles, such as the rule of specialty, which confines surrender to only those charges listed in the Record of the Case. In the Viscomi case, this generated a delicate responsibility for Canadian extradition courts in balancing:

> the rights of Mr. Viscomi, … with the court's gatekeeper responsibility to ensure that the extradition process does not cripple the operation of the extradition proceedings. This careful balancing must respect the rights of the individual without losing sight of the importance of honouring Canada's international treaty obligations. (*R v. Viscomi*, 2016a, para. 62)

Viscomi unsuccessfully raised concerns about *Charter* violations stemming from the Ontario police searches, the subsequent disclosure of this evidence to US authorities, and its use in the second Record of the Case as admissible evidence supporting his extradition. For example, the court hearing this issue in March 2016 stated it was not "directly concerned" with any allegations of a *Charter* breach, but instead examined standard domestic *MLACMA* requirements concerning the disclosure of evidence (*R v. Viscomi*, 2016a, para. 68). These complexities are magnified in cases involving online criminal investigations, as both domestic and internationally recognised human rights protections can be viewed by law enforcement agencies as unduly restricting their capacity to suppress serious crime (Arnell, 2018; Bowling & Sheptycki, 2015). In Canada, extraditees ultimately bear the "onus of establishing a *Charter* breach" (*R v. Viscomi*, 2016a, para. 63), although the standard for meeting recognised international human rights requirements, including those that are incorporated into the domestic laws of most nations and throughout the EU, is extremely high (Mann et al., 2018).

Any potential *Charter* breaches resulting from the Canadian police investigation into Viscomi were considered by the courts to lie "at the lower end of the spectrum of misconduct … and had

no impact on the lawfulness of the search and seizure of the computer equipment" (*R v. Viscomi*, 2016b, para. 157). This means there was no *Charter* violation associated with the legitimacy of confidentially sending this evidence to US authorities, or its later use in the second Record of the Case.

A further series of human rights issues are tied to the pre-trial, trial and post-conviction processes in the requesting jurisdiction. Viscomi did not raise any specific human rights concerns, including possible physical or mental conditions that may be exacerbated by his surrender to the US. However, such issues have provided human rights protection against extradition for prosecutions commenced against individuals located in other jurisdictions at the time online incidents were detected by US authorities (see Mann et al., 2018). The Canadian courts also appear unconcerned about the potential violation of the specialty principle, with Viscomi's "uncharged conduct" considered as a possible "aggravating factor in sentencing on a conviction for the crimes for which [he] is committed for extradition" (*United States of America v. Viscomi*, 2019, para. 49). Further, there appears to be no issue with the US relying "on evidence about other victims on sentencing … [as] Canadian courts are similarly entitled in sentencing to take into account surrounding circumstances that could support a separate charge" (*United States of America v. Viscomi*, 2019, para. 50).

Such technicalities associated with reviewing the merits of the US prosecution case in a Canadian extradition forum are magnified by the rule of non-inquiry (Bassiouni, 2014; King, 2015; Pyle, 2001). Ordinarily, overseas courts examining extradition requests are unlikely to undertake a detailed examination of the operation of justice in a requesting state, because:

> it is not the responsibility of an extradition judge to cull out cases that may be viewed, on all of the evidence, as weak or unlikely to result in the conviction of the person sought … all of those issues are for the trier of fact in the foreign jurisdiction. (*United States of America v. Viscomi*, 2013, para. 13)

In other words, the reluctance of foreign extradition courts to inquire into US evidence collection or imprisonment practices renders many potentially valid human rights claims subject only to vague notions of political trust and comity. These political concepts underpin various forms of mutual cooperation that potentially undermine the notion of due process associated with many contemporary forms of transnational criminal law enforcement (Mann, et al., 2018; Warren, 2015).

CONCLUSION

In June 2019, Viscomi's arguments concerning the search warrants, evidence disclosure, the infringement of sections 6(1) and 7 of the *Charter*, the violation of the specialty principle, the use of extrinsic evidence from the second Record of the Case for future prosecutions and sentences, and the potential for civil commitment were again rejected by a Canadian court. It was decided there was "no unfairness" associated with any previous court decisions and the Minister's order favouring extradition "is entitled to a high level of deference on judicial review and should only be interfered with in the clearest of cases" (*United States of America v. Viscomi*, 2019, paras. 37, 59). This highlights that extradition is more an expression of the political content of transnational law than a question of due process. Such reasoning is also a

symptom of the highly technical nature of both extradition and MLAT procedures, which potentially undermine the very forms of transnational enforcement cooperation they are designed to foster. The Supreme Court of Canada declined to intervene in Viscomi's case in November 2019 and he was extradited to Virginia to stand trial in April 2020 (Daugherty, 2020). In August 2020 Viscomi pled guilty to two counts of producing child pornography. At a sentencing hearing set for January 2021 he faces a minimum of 15 years imprisonment and a maximum of 60 years, to be served in the US (Harper, 2020).

Viscomi's extradition proceedings took approximately seven and a half years to resolve in the Canadian courts before the US extradition request was ultimately granted. This time frame counters the rhetoric for expeditious procedures to deal with transnational cyber-investigations and its obvious benefits for victims, offenders and justice agencies in multiple jurisdictions. However, calls for the development of new modes for dealing with transnational cybercrime and related jurisdictional issues require caution. EU experience suggests there is considerable disquiet over the ready transfer of crime suspects across national jurisdictional borders to face trial in potentially unfamiliar geographic locations or legal cultures (see Gless, 2015).

Transnational cybercrime is possible through the mobility of digital computing technologies and data flows (Daskal, 2015). This creates an illusion that cybercrime suspects are geographically located where the effects of their activities are felt. When viewed in this way, it would make sense to place more emphasis on clearer MLAT procedures governing the collection and transfer of digital evidence, rather than simplifying extradition procedures through the removal of due process protections (Boister, 2017b). Our analysis also suggests due process remains important in all cases, whether this is promoted through clearer transnational data exchange protocols or shifting the prosecution forum to the source of online harm. While international comity dictates that the US had a viable claim for prosecution in this case, it is also perfectly feasible to hold the trial at the source of the harm given Canada had instigated criminal charges against Viscomi that were ultimately abandoned after the US extradition request. We suggest this contradiction can only be reconciled with greater attention to the types of extraterritorial harms that justify extradition, and consideration of when a forum bar can help promote both international comity and fairness for those accused of offshore crimes.

REFERENCES

Abelson, A. (2009). The prosecute/extradite dilemma: Concurrent criminal jurisdiction and global governance. *UC Davis Journal of International Law & Policy*, *16*(1), 1–38. https://jilp.law.ucdavis.edu/issues/volume-16-1/Abelson.pdf

Arnell, P. (2013). The European human rights influence upon UK extradition—Myth debunked. *European Journal of Crime, Criminal Law and Criminal Justice*, *21*(3–4), 317–337. https://doi.org/10.1163/15718174-21042032

Arnell, P. (2018). The contrasting evolution of the right to a fair trial in UK extradition law. *International Journal of Human Rights*, *22*(7), 869–887. https://doi.org/10.1080/13642987.2018.1485655

Bassiouni, M. C. (2014). *International extradition: United States law and practice* (6th ed.). Oxford University Press. https://doi.org/10.1093/law/9780199917891.001.0001

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. https://doi.org/10.1111/ips.12048

Blakesley, C. L. (1984). A conceptual framework for extradition and jurisdiction over extraterritorial crimes. *Utah Law Review*, *1984*(4), 685–761. Blakesley, C. L. (1984). A conceptual framework for extradition and jurisdiction over extraterritorial crimes. Utah Law Review, 1984(4), 685–761.

Blakesley, C. L. (2008). Extraterritorial jurisdiction. In M. C. Bassiouni (Ed.), *International criminal law: Volume II: Multilateral and bilateral enforcement mechanisms* (3rd ed., pp. 85–152). Martinus Nijhoff Publishers.

Boister, N. (2003). Transnational criminal law? *European Journal of International Law*, *14*(5), 953–976. https://doi.org/10.1093/ejil/14.5.953

Boister, N. (2017a). Global simplification of extradition: Interviews with selected extradition experts in New Zealand, Canada, the US and EU. *Criminal Law Forum*, *29*(3), 327–375. https://doi.org/10.1007/s10609-017-9342-7

Boister, N. (2017b). Law enforcement cooperation between New Zealand and the United States: Serving the internet 'pirate' Kim Dotcom up on a silver platter? In S. Hufnagel & C. McCartney (Eds.), *Trust in international police and justice cooperation* (pp. 193–220). Hart Publishing.

Bowling, B., & Sheptycki, J. (2015). Global policing and transnational rule with law. *Transnational Legal Theory*, *6*(1), 141–173. https://doi.org/10.1080/20414005.2015.1042235

Burdick, C. K. (1935). Codification of international law: Part 1 – Extradition. *American Journal of International Law Supplement*, *29*, 15–434.

Clough, J. (2014). A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation. *Monash Law Review*, *40*(3), 698–736. https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf

Council of Europe. (2001). *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Council of Europe. (2020). *Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(2), 2305–2322. https://doi.org/10.1177/1461444819865984

Daskal, J. (2015). The un-territoriality of data. *Yale Law Journal*, *125*(2), 326–398.

Daugherty, S. (2020). After seven year extradition fight, Canadian man arrives in Norfolk for 'sextortion' trial. *Daily Press*. https://www.dailypress.com/news/crime/vp-nw-canadian-extradition-viscomi-20200106-azg6n2bgavce7b4uva74ffl37q-story.html

Dugard, J., & Wyngaert, C. (1998). Reconciling extradition with human rights. *American Journal of International Law*, *92*(2), 187–212. https://doi.org/10.2307/2998029

Geist, M. (Ed.). (2015). *Law, privacy and surveillance in Canada in the post-Snowden era*. University of Ottawa Press.

Gless, S. (2015). Bird's-eye view and worm's eye view: Towards a defendant-based approach in transnational criminal law. *Transnational Legal Theory*, *6*(1), 117–140. https://doi.org/10.1080/20414005.2015.1042233

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.

Harper, J. (2020, August 12). Canadian man pleads guilty in 'sextortion' case involving Virginia Beach sisters. *The Virginian Pilot*. https://www.pilotonline.com/news/crime/vp-nw-viscomi-plea-20200812-2fg4bngvnrhy3evomo3w52xgmq-story.html

Mann, M., & Warren, I. (2018). The digital and legal divide: Silk Road, transnational online policing and southern criminology. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave handbook of criminology and the global south* (pp. 245–260). Palgrave MacMillan. https://doi.org/10.1007/978-3-319-65021-0_13

Mann, M., Warren, I., & Kennedy, S. (2018). The legal geographies of transnational cyber-prosecutions: Extradition, human rights and forum shifting. *Global Crime*, *19*(2), 107–124. https://doi.org/10.1080/17440572.2018.1448272

Marin, L. (2011). "A spectre is haunting Europe": European citizenship in the area of freedom, security and justice. Some reflections in the principles of discrimination (on the basis of nationality), mutual recognition, and mutual trust originating from the European Arrest Warrant. *European Public Law*, *17*(4), 705–728.

Miller, B. W. (2016). *Borderline crime: Fugitive criminals and challenge of the border, 1819-1914*. University of Toronto Press.

Murchison, M. (2007). Extradition's paradox: Duty, discretion, and rights in the world of non-inquiry. *Stanford Journal of International Law*, *43*(2), 295–318.

Palmer, D., & Warren, I. (2013). Global policing and the case of Kim Dotcom. *International Journal of Crime, Justice and Social Democracy*, *2*(3), 105–119.

https://doi.org/10.5204/ijcjsd.v2i3.105

Plachta, M. (1999). (Non-)Extradition of nationals: A neverending story? *Emory International Law Review*, *13*(1), 77–160.

Pyle, C. H. (2001). *Extradition, politics, and human rights*. Temple University Press.

Raustiala, K. (2009). *Does the Constitution follow the flag?: The evolution of territoriality in American law*. Oxford University Press.

Rose, T. (2002). A delicate balance: Extradition, sovereignty, and individual rights in the United States and Canada. *Yale Journal of International Law*, *27*(1), 193–215. https://digitalcommons.law.yale.edu/yjil/vol27/iss1/7/

Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press. https://doi.org/10.1093/oso/9780198795674.001.0001

United States Department of Justice. (2019). *Promoting public safety, privacy, and the rule of law around the world: The purpose and impact of the CLOUD Act*. US Department of Justice.

Warren, I. (2015). Surveillance, criminal law and sovereignty. *Surveillance & Society*, *13*(2), 300–305. https://doi.org/10.24908/ss.v13i2.5679

Warren, I., & Palmer, D. (2015). *Global criminology*. Thomson Reuters.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

CASES

R. v. Spencer, 2014 SCC 43, [2014] S.C.R. 212, No. 34644 (Supreme Court of Canada 13 June 2014). http://canlii.ca/t/g7dzn

R v. Viscomi 2014 ONCA 765, No. M44253 (Court of Appeal for Ontario 2014). http://canlii.ca/t/gf4hc

R v. Viscomi 2015 ONSC 61, (Ontario Superior Court of Justice 9 January 2015). http://canlii.ca/t/gfws4

R. v Viscomi, 2016 ONSC 1830, (Ontario Superior Court of Justice 17 March 2016). http://canlii.ca/t/gnrp4

R v. Viscomi 2016 ONSC 5423, (Ontario Superior Court of Justice 1 September 2016). http://canlii.ca/t/gt778

R v. Viscomi 2016 ONSC 6658, (Ontario Superior Court of Justice 25 October 2016). http://canlii.ca/t/gvkfz

R v. Ward 2012 ONCA 660, 112 OR (3d) 321, (Court of Appeal for Ontario 2 October 2012). http://canlii.ca/t/ftoft

United States of America v. Meng 2018 BCSC 2255, No. 27761–1 (Supreme Court of British Columbia 11 December 2018). http://canlii.ca/t/hwmhm

United States of America v. Viscomi 2013 ONSC 2829, (Ontario Superior Court of Justice 24 May 2013). http://canlii.ca/t/fxnq8

United States of America v. Viscomi 2014 ONCA 879, M44414 (C57211) (Court of Appeal for Ontario 5 December 2014). http://canlii.ca/t/gfjwc

United States of America v. Viscomi 2015 ONCA 484, No. C57211, C57910, C59973, C59982 (Court of Appeal for Ontario 30 June 2015). http://canlii.ca/t/gjsrg

United States of America v. Viscomi 2016 ONCA 980, M47285 (C62967) (Court of Appeal for Ontario 23 December 2016). http://canlii.ca/t/gwljk

United States of America v. Viscomi 2019 ONCA 490, No. C62967, C64283 (Court of Appeal for Ontario 14 June 2019). http://canlii.ca/t/jozto

Viscomi v. Attorney General of Canada; Attorney General of Ontario 2015 SCC 397, (Supreme Court of Canada 17 December 2015). http://canlii.ca/t/gmmrw

Viscomi v. Attorney General of Canada (on behalf of the United States of America) 2019 SCC 38760., (Supreme Court of Canada 28 November 2019). http://canlii.ca/t/j3n64

Viscomi v. Ontario (Attorney General) 2014 ONSC 5262, (Ontario Superior Court of Justice 11 September 2014). http://canlii.ca/t/g8zzk

APPENDIX

Table 1:
Summary of the progression of the Viscomi case through the Canadian judicial system

Case citation	Legal & factual issue	Outcome
United States of America v. Viscomi 2013 ONSC 2829 [24 May]	Can ISP records identify Viscomi as the offender to justify extradition?	Extradition certified: ISP evidence is sufficient to establish identity.
Viscomi v. Ontario (Attorney General) 2014 ONSC 5262 [11 Sep]	Was Viscomi entitled to evidence presented during the *ex parte MLACMA* hearing?	Dismissed: No relevant non-disclosure.
R v. Viscomi 2014 ONCA 765 [31 Oct]	Was the previous decision concerning the *ex parte MLACMA* decision correct?	Dismissed: Court does not have jurisdiction due to procedural regulations.
United States of America v. Viscomi 2014 ONCA 879 [5 Dec]	Should Viscomi receive bail?	Bail denied: No arguable ground for appeal.
R v. Viscomi 2015 ONSC 61 [9 Jan]	Do ss. 18 & 20 of the *MLACMA* violate ss. 7 & 8 of the *Charter*?	Dismissed: *MLACMA* is not unconstitutional & contains protections that comply with ss. 7 & 8 of the *Charter*.
United States of America v. Viscomi 2015 ONCA 484 [30 Jun]	Was the evidence sufficient for the Magistrate to infer Viscomi was the user of the IP address?	Decision set aside: Magistrate misapprehended the evidence.
Viscomi v. Attorney General of Canada; Attorney General of Ontario 2015 SCC 397 [17 Dec]	Was the dismissal of the ruling upholding constitutional validity correct?	Dismissed: Previous ruling was correct.

Case citation	Legal & factual issue	Outcome
R v. Viscomi 2016a ONSC 1830 [17 Mar]	Does Viscomi have the right to further disclosure prior to the second extradition hearing?	Dismissed: Additional disclosure would not impact the extradition decision.
R v. Viscomi 2016b ONSC 5423 [1 Sep]	Is the Canadian gathered evidence inadmissible due to *Charter* breaches?	Dismissed: Searches were lawful & any *Charter* breaches were minimal.
R v. Viscomi 2016c ONSC 6658 [25 Oct]	Does the Canadian and US gathered evidence identify Viscomi as the offender to justify extradition?	Extradition certified: Sufficient evidence.
United States of America v. Viscomi 2016 ONCA 980 [23 Dec]	Should Viscomi receive bail?	Bail denied: Potential flight risk & Viscomi may access the internet to reoffend.
United States of America v. Viscomi 2019 ONCA 490 [14 Jun]	Did the Magistrate or Minister err in any way?	Dismissed: No errors were made in either stage of extradition.
Viscomi v. Attorney General of Canada (on behalf of the United States of America) 2019 SCC 38760 [28 Nov]	Was the previous dismissal correct?	Dismissed: Court declined to hear appeal.