International and Comparative Law Quarterly (2025), 1–31
doi:10.1017/S0020589325100985

ARTICLE

Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations

Jessica Shurson

Assistant Professor, School of Law, University of Sussex, Brighton, UK
Email: j.shurson@sussex.ac.uk

Abstract

Law enforcement authorities (LEAs) increasingly need to obtain digital evidence that is stored or controlled across borders. As a result, States increasingly exercise enforcement jurisdiction extraterritorially by imposing investigative measures on service providers that possess or control data outside the territory, without the State's LEAs physically entering another State's territory. This exercise of 'investigative jurisdiction' seemingly conflicts with the longstanding prohibition of the exercise of extraterritorial enforcement jurisdiction in international law. This article argues that given the development of State practice, longstanding jurisdictional principles should adapt to global technologies. Consistent with the principle of comity, this article conceptualises a limited form of investigative jurisdiction that respects sovereignty and minimises conflicts of law.

Keywords: investigative jurisdiction; enforcement jurisdiction; extraterritoriality; sovereignty; non-intervention; non-interference; digital evidence; electronic evidence; criminal investigations; transnational digital investigations

1. Introduction

Due to the advancement of internet-facilitated communications and cloud computing technologies, law enforcement authorities increasingly need to obtain digital evidence that is stored or controlled across borders.[1] As a result, routine domestic investigations have transformed into transnational digital investigations,

[1] A 2018 European Commission study found that 85% of criminal investigations in Europe involved digital evidence and two-thirds of these investigations needed a cross-border request for data. See European Commission, 'Impact Assessment accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings' (Doc No SWD(2018) final, 17 April 2018) 118 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN>.

raising issues of the proper scope of extraterritoriality in the context of a State's enforcement jurisdiction.

Consider an example of a domestic murder investigation in Paris: the victim was a resident and citizen of France, as is the suspect. The crime took place in Paris. As the French police investigate, they determine that the suspect's emails may contain important evidence of the planning of the murder. If the suspect's emails were stored with a local service provider, the police would use ordinary investigatory measures to obtain the evidence relatively quickly. If, however, the suspect used an email service provided by a foreign service provider, such as a United States (US)-based service provider, the French police may have to use a different type of investigative measure. Generally, US law prevents US-based service providers from disclosing the contents of emails to third parties without a US court-issued order.[2] Even though the crime took place in France, which is also where the suspect is located, the French police would need to engage with US law for the somewhat arbitrary reason that the suspect used an email service that happens to be run by a US-based service provider. Thus, the French police will need to use the slow and cumbersome mutual legal assistance treaty (MLAT) process—which provides for cooperation between States Parties to obtain assistance in the investigation and/or prosecution of criminal offences—to obtain the US court order, which can result in significant delays to the investigation.[3]

Many States in the position of France have decided that, rather than engage with the MLAT process, they will compel service providers (who offer services to users in that State) to turn over data through domestic investigatory measures. For example, courts in Belgium have required a US-based service provider to turn over data or be subject to monetary penalties.[4] To justify the imposition of domestic investigative measures on a service provider or data located outside the territory, States will often rely on connections between their territory and the service provider, such as the service provider's offering of services to users in that State (a 'targeting test'). States have traditionally used these types of extended territoriality principles to justify exercises of prescriptive jurisdiction, but not enforcement jurisdiction, which is strictly limited to the territory of a State. This entanglement of prescriptive and enforcement jurisdiction principles has led some scholars to propose that a new category of jurisdiction is emerging in international law—'investigative jurisdiction'.[5] This article builds on this previous scholarship to introduce a clear conceptualisation of the bounds of investigative jurisdiction within the context of transnational digital investigations. Drawing on international law principles and State practice in the US and Europe, this article identifies the sovereignty-related issues that arise in the

[2] Electronic Communications Privacy Act, 18 USC (ECPA) section 2703(c) (US).

[3] See Section 3.2 for discussion of MLATs.

[4] See discussion of Belgian cases in Section 3.3.1.

[5] C Ryngaert, 'Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts' (2023) 24 GLJ 537, 540; D Svantesson, 'Extraterritoriality in the Context of Data Privacy Regulation' (2013) 7 Masaryk University Journal of Law and Technology 87. Svantesson maintains investigative jurisdiction as its own type of jurisdiction apart from the traditional categories, but this article follows the approach of Ryngaert that investigative jurisdiction is properly understood as a subset of enforcement jurisdiction. The reasons for this will be explained further in the text accompanying nn 10–14.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

extension of a State's extraterritorial jurisdiction and conceptualises a limited form of investigative jurisdiction consistent with international law.

The main argument of this article is that the extraterritorial extension of investigative jurisdiction can be consistent with international law, subject to certain limitations. This argument may be somewhat controversial as it proposes a step away from the orthodox approach to enforcement jurisdiction. However, the limitations proposed respect the purpose of the strict territorial limitation on enforcement jurisdiction—thereby maintaining respect for the principle of the sovereign equality of States.

The global nature of data and technology requires this evolution in jurisdictional principles. Service providers possess and control data in a manner that may be independent of the user's location. These service providers rely on networks and data centres around the world to move and efficiently store data. Further, global service providers who are based in one country supply services to users worldwide, many of whom have no connection to the State in which the service provider is based. Thus, using these technologies creates two types of extraterritoriality that must be considered.

The first type of extraterritoriality, which this article refers to as the 'minimal extraterritoriality model', does not necessarily implicate the sovereign interests of other States. As in the French murder investigation example above, the data is 'extraterritorial' in that it is controlled by a service provider based in the US and may be stored outside France in the service provider's network infrastructure. The technology gives rise to extraterritoriality by allowing a global service provider that is based in a foreign State to control or store data outside the territory of the investigating State. However, the foreign State(s) in question (the location of the service provider and/or the location of the data) have a minimal sovereignty interest in the data in question, which solely concerns communications made within France by a French person.

The global nature of service providers, empowered by borderless data technologies, can also exacerbate existing extraterritoriality concerns. Investigators may more easily obtain data about foreign data subjects or in cases where criminal activity crosses borders. In this second type of extraterritoriality—the 'significant extraterritoriality model'—the potential conflicts of laws and sovereignty interests must be balanced more carefully to avoid the impermissible exercise of extraterritoriality. Consider an example: Country A's law enforcement authority (LEA) is investigating a drug trafficking case involving foreign nationals smuggling illicit substances into the territory of the investigating State (Country A). Through the course of the investigation, the LEA determines that the smugglers are communicating via email. The LEA obtains the order to obtain the data through the legal process as required under the law of Country A and serves the order on the email service provider. The service provider responds that the data requested by the LEA pertains to a national of Country B, whose law blocks the service provider from disclosing the data to the investigating State. The service provider has offices and offers services in both States. Without much detailed analysis, it is already apparent that Country B may have a significant sovereignty interest in protecting the data in question as it pertains to a citizen of Country B.

This article argues that to respond to both types of extraterritoriality (and the spectrum of potential deviations between the two models), the conceptualisation of investigative jurisdiction requires four limitations. First, the investigating State must

have jurisdiction to prosecute the criminal activity. Second, the investigating State must have jurisdiction over the service provider from whom it seeks disclosure of the data. Third, the exercise of investigative jurisdiction must be limited to digital evidence rather than physical evidence. Finally, investigative jurisdiction must not violate another State's sovereignty or illegally interfere with the data subject's fundamental rights. This final limitation may require balancing sovereignty interests and fundamental rights based on the principle of comity, which recognises that sometimes States should moderate an otherwise lawful exercise of jurisdiction when another State has a stronger connection to the data to be regulated.

How LEAs obtain cross-border data in an increasingly digital and globalised world has, by this point, become a well told story.[6] But this article retells this story focusing on a different angle—pulling out the sovereignty connections between States and digital evidence within the current State practice to identify the proper limitations of a principled conceptualisation of investigative jurisdiction based on comity. To do so, the article proceeds as follows.

Section 2 begins with an overview of the principles of jurisdiction, especially extraterritorial jurisdiction, under international law, which guides the analysis of State practice throughout the article and underpins the conceptualisation of investigative jurisdiction. Section 3 sets out the challenges posed by digital evidence to traditional consent-based mechanisms for cross-border evidence gathering. In response, some States impose extraterritorial investigative measures unilaterally, often relying on extended territoriality principles such as the effects test, which emphasises a connection to territory but results in an extension of jurisdiction that is extraterritorial. It then details this State practice in light of international law principles of jurisdiction and considers whether these extraterritorial investigative measures implicate the duty of non-intervention in the sovereign affairs of other States. Section 4 considers the comity principle as a mechanism for minimising conflicts of sovereignty in this context. The US and the European Union (EU) have instrumentalised this principle of sovereign deference to develop multifactor analyses that weigh the strength of jurisdictional claims over digital evidence. Considering the sovereignty interests identified through these comity analyses and those identified throughout the article, Section 5 concludes with a conceptualisation of investigative

[6] A representative selection of some relevant works on this issue includes: T Cochrane, 'Digital Privacy Rights and CLOUD Act Agreements' (2022) 47 BrookJIL 1; I Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in C Millard (ed), *Cloud Computing Law* (2nd edn, OUP 2021) 441; H Abraha, 'Law Enforcement Access to Electronic Evidence across Borders: Mapping Policy Approaches and Emerging Reform Initiatives' (2021) 29 IJLIT 118; J Hörnle, *Internet Jurisdiction: Law and Practice* (OUP 2020) ch 6; S Carrera, M Stefan and V Mitsilegas, 'Cross-Border Data Access in Criminal Proceedings and the Future of Digital Justice Navigating the Current Legal Framework and Exploring Ways Forward within the EU and across the Atlantic' (Centre for European Policy Studies, 2020) <https://www.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf>; P de Hert and J Thumfart, 'The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma: Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies' (Brussels Privacy Hub, Working Paper No 11, 2018) <https://www.ssrn.com/abstract=3228388>; AK Woods, 'Litigating Data Sovereignty' (2018) 128 YaleLJ 328; RJ Currie, 'Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the Next Frontier?' (2016) 54 CanYBIL 63; J Daskal, 'The Un-Territoriality of Data' (2015) 125 YaleLJ 326.

jurisdiction consistent with international law. The article concludes that traditional jurisdictional principles should evolve to meet these new digital challenges but must do so in a manner that respects sovereignty and fundamental rights.

2. Extraterritorial jurisdiction in international law

In the modern international legal system, all States are sovereign equals.[7] 'Sovereignty' is used in this article to refer to the legal attributes of a State that constitute the general competence to regulate matters within its territory and about its people. This definition of sovereignty necessitates corollaries, including the rules on jurisdiction and the duty of non-intervention in the internal affairs of another State.[8] Jurisdiction is used to refer to the authority of States to make laws (prescriptive jurisdiction), adjudicate disputes under those laws (adjudicatory jurisdiction) and enforce laws (enforcement jurisdiction).[9]

Investigative measures, such as production orders, warrants and search and seizure orders have been viewed traditionally as exercises of enforcement jurisdiction. As Crawford states, 'a summons may not be served, police or tax investigations may not be mounted, orders for production of documents may not be executed, on the territory of another state, except under the terms of a treaty or other consent given'.[10] Some may argue that a production order is merely sent to a service provider with offices abroad and, therefore, is not 'executed' until the State seeks to enforce the order through sanctions. But a production order is a State's act of executive power, not a mere request.[11] The order compels the service provider to disclose the data with the threat of sanctions for non-compliance.[12] This article agrees with the dominant view[13] that a production order in the context of transnational digital investigations is an exercise of enforcement jurisdiction as 'an exercise of compulsory state power'.[14]

States may exercise prescriptive jurisdiction, that is, the jurisdiction to regulate, within their territory. The evaluation, however, of what is territorial or extraterritorial has become 'increasingly a matter of appreciation'.[15] Prescriptive jurisdiction can also be asserted over an activity that has effects within the territory of the State (the 'effects test') or under the targeting test, which requires an intentional connection between the activity and the effect in the territory. Scholarship has termed these types of tests within EU law as 'territorial extension', which reflects the continued application of the

[7] J Cohen, 'Whose Sovereignty? Empire versus International Law' (2004) 18 Ethics & International Affairs 1, 12.

[8] J Crawford, *Brownlie's Principles of Public International Law* (9th edn, OUP 2019) 431.

[9] Hörnle (n 6) 9.

[10] Crawford (n 8) 462.

[11] Enforcement jurisdiction is also referred to as executive jurisdiction: ibid 440.

[12] As Judge Posner said with respect to similar court-issued subpoenas, the order is 'enforcing something rather than begging': *Leibovitch v Islamic Republic of Iran* 852 F3d 687, 698 (7th Cir 2017) (US).

[13] Ryngaert (n 5); U Kohl, 'Jurisdiction in a Network Society' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021) 69, 73; Crawford (n 8) 479; Currie (n 6); S Coughlan et al, 'Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization' (2007) 6 Canadian Journal of Law and Technology 29.

[14] Currie (n 6) 65.

[15] Crawford (n 8) 440–41.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

territoriality principle but where extraterritorial effects are present.[16] Given the development of these territorial extension tests, a 'genuine connection' rule has emerged in international law, which allows States to exercise prescriptive jurisdiction extraterritorially where there is a 'genuine connection between the subject matter of jurisdiction and the territorial base or reasonable interests of the State in question'.[17]

Traditionally, however, a State's exercise of enforcement jurisdiction is strictly limited to matters or persons within its territory. The classic articulation of this rule is derived from the *SS Lotus* case: a State 'may not exercise its power in any form in the territory of another State'.[18] Criminal investigations are typically confined to the territory of the investigating LEA, and an LEA may require the cooperation of another State to access evidence located within that State's territory. If an LEA agent of State A were to physically travel to and seize evidence in State B without the consent of State B, then the actions of State A's agent would be an exercise of extraterritorial jurisdiction and in breach of international law.

It is more difficult to ascertain whether an LEA acts extraterritorially when seeking digital evidence remotely and virtually.[19] The nature of data and technology is such that an LEA agent in State A may obtain data in State B without ever leaving State A. Thus, the inquiry is somewhat turned on its head to consider when a territorial enforcement action by the State's agent has an extraterritorial effect.[20] While, traditionally, international law has defined extraterritorial jurisdiction as 'the exercise of a jurisdiction by a state over activities occurring outside its borders', it may also be said that extraterritorial jurisdiction should include 'whether the exercise of jurisdiction (that may well, but need not, be extraterritorial) has any extraterritorial effect or implications'.[21] It is this type of extraterritoriality that this article seeks to address.[22]

[16] Scott introduced the term 'territorial extension', which she distinguishes from extraterritoriality by defining extraterritorial to denote a measure that 'imposes obligations on persons who do not enjoy a relevant territorial connection with the regulating state': J Scott, 'Extraterritoriality and Territorial Extension in EU Law' (2014) 62 AJCL 87, 89–90. Ryngaert and Taylor have taken forward the concept of 'territorial extension' in the context of data protection and privacy law but use the terms synonymously with extraterritoriality: C Ryngaert and M Taylor, 'The GDPR as Global Data Protection Regulation?' (2020) 114 AJIL: Unbound 5; M Taylor, 'The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect' (2015) 5 IDPL 246. Scott herself notes (ibid 91) that her definitions are 'not uncontroversial'. This article prefers to follow the approach taken by Ryngaert and Taylor and define investigative measures that require extraterritorial conduct or effects as 'extraterritorial'. By engaging the more restrictive view of these measures under international law, the case for investigative jurisdiction should be more resilient to critique.

[17] Crawford (n 8) 441; see also C Ryngaert, *Jurisdiction in International Law* (2nd edn, OUP 2015); FA Mann, 'The Doctrine of International Jurisdiction Revisited after Twenty Years'; American Law Institute, *Restatement (Fourth) of United States Foreign Relations Law* (2018) section 407.

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

[19] Daskal (n 6) 379.

[20] Hörnle (n 6) 149.

[21] D Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on US Businesses' (2014) 50 SJIL 53, 60 (quoting D Senz and H Charlesworth, 'Building Blocks: Australia's Response to Foreign Extraterritorial Legislation' (2001) 2 MJIL 69, 72, in the first quote).

[22] See also n 16.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

In digital investigations, the extraterritorial application of investigative measures is often justified by States using prescriptive jurisdiction principles for extended territoriality, such as the effects test or the targeting test.[23] This adaptation of prescriptive jurisdiction principles to instances of enforcement jurisdiction has led to a new category of jurisdiction, which this article refers to as 'investigative jurisdiction'.[24] This article only contemplates investigative jurisdiction in the virtual sense, which refers to States imposing extraterritorial investigative measures that do not require the LEA agent to physically enter the territory of another State. This article will show how State practice in this context questions whether the long-standing, strict territorial limitation on enforcement jurisdiction still constitutes an observed and respected norm in international law.

In addition to the territoriality principle, international law allows for the exercise of jurisdiction based on the personality principle. States have jurisdiction over their nationals, even outside of their territory, for example, by regulating the conduct of their citizens when they are abroad (active personality principle) or conduct that may harm their citizens (passive personality principle).[25] As will be seen in this article, the active personality principle signifies an important sovereignty interest of States that may justify blocking an exercise of investigative jurisdiction by another State.

The other corollary to sovereignty is the principle of non-intervention, defined by the International Court of Justice (ICJ) in *Nicaragua* as 'the right of every sovereign State to conduct its affairs without outside interference'.[26] Interference becomes a prohibited intervention when, first, States intervene in the affairs of other States 'on matters in which each State is permitted, by the principle of State sovereignty, to decide freely'[27] and, second, when States use coercion to interfere with the internal affairs of other States.[28] The non-intervention principle usually arises in cases involving armed interventions,[29] and its relevance to virtual interventions in cyberspace is just beginning to be explored.[30] The application of the principle of non-intervention to the extraterritorial imposition of investigative measures by LEAs has yet to be considered in the literature. While States have claimed sovereignty interests in blocking the disclosure of data to LEAs in other States, the principle of non-intervention has not usually been asserted. This article will consider whether the unilateral exercise of investigative jurisdiction may implicate this

[23] See Section 3.3.1.

[24] Ryngaert (n 5). See also D Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017).

[25] Hörnle (n 6) 87.

[26] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, para 202.

[27] ibid para 205.

[28] ibid.

[29] *Corfu Channel (United Kingdom v Albania)* (Merits) [1949] ICJ Rep 4, 35; *Armed Activities on the Territory of the Congo (DRC v Uganda)* (Merits) [2005] ICJ Rep 168.

[30] See T Moulin, 'Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward' (2020) 25 JC&SL 423; N Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace' in D Broeders and B van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (Rowman & Littlefield International 2020) 45; K Bannelier and T Christakis, *Cyber-Attacks, Prevention-Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale 2017); R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 JC&SL 212.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

principle and whether it is possible for States to avoid unreasonable interference in the sovereign affairs of other States by adhering to the comity principle.

3. Digital challenges to traditional consent-based mechanisms for cross-border evidence gathering

3.1. Nature of digital evidence

Modern communications and computing technologies have changed criminal investigations. Processes for obtaining criminal evidence have traditionally focused on the location of evidence, but digital evidence may lack a fixed or identifiable location. The proliferation of cloud computing and internet-facilitated communication technologies means that nearly every criminal investigation is likely to require digital evidence, much of which is in the control of global service providers who possess or control data within global networks and infrastructure.[31]

Cloud computing and internet-facilitated communication technologies control and store data largely independent of a territorial location.[32] The network infrastructure that service providers use to move and store data is often outside the user's territory, and the service provider may also be located outside of the territory.[33] Data may be stored in multiple locations, in fragments and with multiple copies.[34] Further, to maximise efficiency, data may be constantly moving through these networks and between data centres.[35] Consider an example: in a criminal investigation in London, police determine that data belonging to the suspect's CloudMail account may contain evidence of a crime. CloudMail is an American company with an Irish subsidiary that controls and processes data pertaining to CloudMail's United Kingdom (UK) accounts. CloudMail stores the content of the emails (the substance of the communication including the text or images sent) on servers in Iceland but copies some of the data onto servers in the UK. Subscriber information (name, location and phone number of account holder) is stored in a data centre in Ireland. This paradigm could have four relevant locations of data—the UK, the US, Ireland or Iceland. Further, at the time when the UK production order for the suspect's data is served on CloudMail's London office, some email data sent and received in the CloudMail account could be making its way through CloudMail's networks in different data packets to speed up the efficiency of CloudMail's systems. Like documents sent in multiple envelopes, these packets are not all routed through the same network. This situation introduces multiple potential locations of evidence, both unfixed and unknown.

Given the novel challenges of data, some States are moving past the location of data as a necessary factor to found jurisdiction. Section 3.3 will show that, rather than the location of data, some States focus on the location of the service provider who holds or controls the data, the location of the services offered by these providers and the location

[31] See n 1.

[32] WK Hon and C Millard, 'Cloud Technologies and Services' in C Millard (ed), *Cloud Computing Law* (2nd edn, OUP 2021) 3.

[33] ibid.

[34] Daskal (n 6).

[35] ibid.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

of the criminal activity for which the data may contain evidence. Given the often-arbitrary storage or routing locations, these territorial links make more sense in grounding jurisdictional claims.

3.2. Mutual legal assistance

Traditionally, when a State needs to obtain access to evidence located outside its territory, it makes an application pursuant to an MLAT to the State where the evidence is located for assistance in obtaining the evidence.[36] There are usually two basic steps to an MLAT process. First, the requesting State sends the request for evidence to the central authority of the requested State, where it is reviewed to ensure it meets domestic legal standards. Second, an independent judicial authority in the requested State will examine the request and issue a binding court order to obtain the evidence.[37] In practice, these two steps may involve many smaller steps, making the MLAT process lengthy in terms of time and resources.[38]

Requests for digital evidence have exacerbated the lengthy and cumbersome nature of the MLAT process. Andrew Keane Woods has identified three trends that undermine the traditional MLAT system: first, the increasing amount of digital evidence; second, that digital evidence is disproportionately controlled by foreign service providers; and, third, that those service providers either cannot or will not respond to foreign LEA requests for data.[39] In addition, the MLAT process has been critiqued as outdated when the data needed for a domestic investigation (i.e. the minimal extraterritoriality model) may be arbitrarily located outside the jurisdiction because a user chose a foreign service provider who controls or stores the user's data in another State.[40] Thus, both normative and efficiency issues call into question whether the MLAT process should continue to be the primary mechanism to access digital evidence across borders. Indeed, States have acted accordingly, seeking new methods or justifications to obtain evidence extraterritorially that bypass the MLAT system.

These MLAT bypass mechanisms may be cooperative, as seen in new treaties and arrangements for direct access mechanisms. This article uses the term 'direct access' to mean that an LEA in one State can send a production order directly to a service provider for data that the provider either possesses or controls in a second State. Direct access mechanisms can sometimes bypass the service provider completely, such as when LEAs directly access data held in another State through a network connection (i.e. government hacking).[41] However, these new cooperative mutual legal assistance reforms are all

[36] S Carrera et al, 'Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights' (Centre for European Policy Studies, 2015) 2 <https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf>.

[37] ibid 2, 7.

[38] T Lin and M Fidler, 'Cross-Border Data Access Reform: A Primer on the Proposed US-UK Agreement' (Berkman Klein Center for Internet and Society, September 2017) 3.

[39] AK Woods, 'Mutual Legal Assistance in the Digital Age' in D Gray and S Henderson (eds), *The Cambridge Handbook of Surveillance Law* (1st edn, CUP 2017) 659, 660.

[40] G Kent, 'Sharing Investigation Specific Data with Law Enforcement: An International Approach' (Stanford Public Law Working Paper No 18, 2014) para 34 <http://www.ssrn.com/abstract=2472413>.

[41] J Mayer, 'Government Hacking' (2017) 127 YaleLJ 570.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

predicated on the existence of an intermediary service provider and, thus, State practice is coalescing around this situation rather than unmediated direct access.

These new cooperative mechanisms for direct access are primarily limited to small groups of States that are already close allies. The most prominent example is the US Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act), which creates a framework for bilateral agreements with 'qualified foreign governments' (QFGs). These agreements allow QFGs to send production orders for all types of data directly to US-based service providers.[42] Current QFGs are the UK and Australia.[43] Negotiations with Canada and the EU are ongoing at the time of writing.[44] Similarly, the new EU e-Evidence Regulation sets up a direct access scheme within the EU. Based on principles of mutual trust and mutual recognition in Article 82(1) of the Treaty on the Functioning of the European Union, the e-Evidence Regulation creates a preservation order and a production order that may be served directly by authorities in one Member State on a service provider located in another Member State.[45]

The most significant new cooperative mechanism for direct access to digital evidence is also limited in the types of data it covers. The Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence (Second Additional Protocol) introduces a direct access mechanism for the disclosure of subscriber information and domain name information.[46] Article 7 provides that States Parties may send a production order directly to a service provider located in the territory of another State Party for stored subscriber information within the provider's possession or control. States Parties that sign the Second Additional Protocol must remove any blocking provisions within domestic law that would prevent a service provider in their territory from disclosing subscriber information under the Second Additional Protocol.[47] Article 8 contains similar provisions for domain name information.

[42] ECPA (n 2) section 2523(b)(4)(D)(iii).

[43] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (adopted 2024) TS No 33/2024 <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-ts-no332024>; Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (adopted 15 December 2021) <https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-and-australia>.

[44] United States Department of Justice (DoJ), 'United States and Canada Welcome Negotiations of a CLOUD Act Agreement' (Press Release, 22 March 2022) <https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement>; DoJ, 'Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations' (Press Release, 2 March 2024) <https://www.justice.gov/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations>.

[45] Regulation (EU) No 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation) art 1, recital 11.

[46] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (adopted 21 May 2022, not yet in force) CETS No 224, arts 6–7. Subscriber information is the data relating to the subscription of the service, such as name, address and date of account creation. Domain name information is similar information about the registration of a particular web address.

[47] ibid art 7.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

MLAT bypass mechanisms may also be impliedly cooperative, such as the informal voluntary regime for subscriber information and traffic data that has developed amongst US-based service providers. In the US, the Electronic Communications Privacy Act 1986 (ECPA)[48] allows US-based service providers to provide subscriber information or transactional data 'to any person *other than a governmental entity*'.[49] 'Governmental entity' is defined as a department or agency of the US (or one of the 50 state governments within the US).[50] Thus, the ECPA allows US-based service providers to voluntarily comply with foreign government requests for subscriber information and transactional data. It may be an unintentional quirk of the ECPA that it is easier for non-US LEAs to obtain subscriber information and transactional data from US-based service providers than US-based LEAs.[51] Nonetheless, the US has seemingly acquiesced to this informal, voluntary cooperation regime between US service providers and non-US LEAs for subscriber and traffic data.[52] Further, the US was a proponent of setting up the Second Additional Protocol, which essentially formalises this arrangement.[53] Ryngaert suggests that voluntary compliance with orders makes the orders merely 'requests' and thus are not 'instances of genuine extraterritorial enforcement jurisdiction'.[54] But the acquiescence of the US to foreign LEAs sending orders for data directly to service providers within its territory is an important point of reference on the sovereignty concerns of States, especially given that the ECPA explicitly blocks foreign orders for content data.

Further workarounds to the MLAT system are often unilateral, such as the exercise of extraterritorial investigative jurisdiction that is seen in the laws of the EU, US, UK and Belgium and described in the next section of this article. In addition, some countries require data (or copies of data) of citizens or persons within the State to be stored on computers or servers within their territory.[55] These 'data localisation' requirements mean that LEAs in countries like Russia and China have easier access to data as it is stored territorially.[56] Service providers usually oppose data localisation as it requires

[48] ECPA (n 2) sections 2510–2523.

[49] ibid section 2702(c)(6) (emphasis added). Transactional data is non-content data relating to the provision of the service, such as the source and destination of a message, the email addresses of recipients, dates, times, duration and format of services used: ibid section 2702. Transactional data may also be called 'traffic data'. See Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185 (Cybercrime Convention) art 1(d).

[50] ECPA (n 2) section 2711(4).

[51] The ECPA requires US-based LEAs to obtain an administrative subpoena for subscriber information and a warrant or court order for traffic data: ibid section 2703(c).

[52] Cybercrime Convention Committee (T-CY) Cloud Evidence Group, 'Final Report: Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY' (Council of Europe (CoE), 2016) 26–29 (evaluates statistics showing extensive use of this voluntary regime).

[53] DoJ, 'United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime' (Press Release, 12 May 2022) <https://www.justice.gov/opa/pr/united-States-signs-protocol-strengthen-international-law-enforcement-cooperation-combat>.

[54] Ryngaert (n 5) 548.

[55] D Svantesson, 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines' (Organisation for Economic Co-operation and Development, Digital Economy Paper No 301, 2020) <https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges_7fbaed62-en>.

[56] A Wang, 'Cyber Sovereignty at Its Boldest: A Chinese Perspective' (2020) 16 OhioStTechLJ 395; A Savelyev, 'Russia's New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction?' (2016) 32 Computer Law and Security Review 1.

additional resources, negating the efficiency gains of the cloud computing system and countering the ideal of an open and free internet. The protectionist stance of some States, like those enacting data localisation policies, means that the acceptance of investigative jurisdiction may be limited to certain States. As acknowledged by Ryngaert, thus far these States have tended to be Western States[57] although, at the time of writing, 49 States have signed the Second Additional Protocol.[58]

3.3. Unilateral mechanisms for digital evidence gathering

3.3.1. State practice

Many States have laws that provide for production orders for data with some extraterritorial effect, usually when the data is located outside the jurisdiction or the service provider who controls the data is physically located outside the territory.[59] Because there is no cooperation with the State in which the data or service provider is located (such as through an MLAT), these laws constitute a unilateral exercise of jurisdiction with extraterritorial effect. In other words, these States are exercising extraterritorial investigative jurisdiction.

One of the dominant justifications for a State to exercise jurisdiction over a service provider located outside its territory is based on the State having jurisdiction over the service provider who targets the territory with its services. This is the approach taken in the EU e-Evidence Regulation, the UK Investigatory Powers Act 2016 (IPA) and by Belgian courts in two leading cases on the extraterritoriality of production orders for digital evidence.

Under the EU e-Evidence Regulation, a Member State may order 'a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data'.[60] It defines 'offering services in the Union' to mean that service providers enable a service to be used by data subjects in a Member State and that service providers have 'a substantial connection' to the EU through either an establishment in the EU, a significant user-base in the EU or the targeting of activities towards a Member State.[61] This Regulation extends the jurisdiction of every Member State over data held by service providers located anywhere in the world as long as that service provider offers services to persons in one Member State. Service providers principally based in the US, and therefore subject to the ECPA's blocking provisions, may also be physically present or offer services in the EU that may bring them under the purview of the e-Evidence

[57] Ryngaert (n 5).

[58] CoE Treaty Office, *Chart of Signatures and Ratifications of Treaty 224* <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224>.

[59] A 2012 comparative study found that Australia, Canada, Denmark, France, Ireland, Spain and the UK all have laws that authorise the State to compel a service provider to permit access to and disclose data on servers outside of the States' territories. W Maxwell and C Wolf, 'A Global Reality: Governmental Access to Data in the Cloud' (Hogan Lovells White Paper, 2012) 13. This article will also show that the laws of Belgium, the US and EU allow for similar extraterritorial reach.

[60] e-Evidence Regulation (n 45) art 1(1).

[61] ibid art 2(4). Targeting criteria include factors such as the use of language or currency of a Member State, the ability to order goods and services in the Member State, advertising in a Member State and the availability of an app in the relevant national store: ibid recital 28.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

Regulation. This will likely create an intractable conflict of laws without data localisation practices in Europe or a US-EU CLOUD Act Agreement.[62]

Before the introduction of the e-Evidence Regulation, Belgian courts found that production orders had a sufficiently strong territorial connection to Belgium if certain connecting factors were present between the measure and Belgian territory. In the *Belgium Yahoo!* case, the Belgian public prosecutor demanded data be produced by Yahoo! pursuant to the Belgian Code of Criminal Procedure. Yahoo! refused on the ground that it is a US-based company and therefore the Belgian production order was an impermissible extension of enforcement jurisdiction that violated the sovereign equality of States.[63] On appeal, the Court of Cassation acknowledged that enforcement jurisdiction is generally limited to the territory of the State but found that the coercive measures in this case should be considered as falling within Belgium's enforcement jurisdiction when there is a 'sufficient territorial connecting factor between that measure and that territory'.[64]

The Court found that several connecting factors between Belgium and the production order to Yahoo! met this requirement. First, the coercive measure did not require any Belgian officials to act physically outside of the jurisdiction.[65] Second, the Code of Criminal Procedure criminalised non-compliance with a production order 'at the place where the requested information must be received', which was Belgium rather than the US.[66] Third, Yahoo! was 'present on the Belgian territory and subjects itself voluntarily to the Belgian law because it actively participates in the economic activity in Belgium' by offering services to users on Belgian territory.[67] Lastly, the data requested concerned telecommunications that otherwise took place in Belgium and, therefore, the Belgian prosecutor and court had jurisdiction to demand disclosure of the data.[68] A Belgian appeals court reached a similar conclusion in a comparable case against Skype —based in Luxembourg—because Skype offered services to users in Belgium, even though Luxembourg law prohibited the disclosure of data to foreign States.[69]

In the UK, the IPA provides for the issuing of interception warrants for data that constitutes the content of communications (in transit or stored within a telecommunications system)[70] that may be served on a 'telecommunications operator', broadly defined as operators who offer telecommunications services to persons in the UK.[71] This definition seems to leave service providers uncovered only if they do not

[62] J Shurson, 'Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts between EU and US Law' (2020) 28 IJLIT 167.

[63] Court of Cassation of Belgium, Case No P.13.2082.N, 1 December 2015.

[64] ibid paras 4–5. Quote is from the English translation: 'Nr. P.13.2082.N, Hof van Cassatie van België (Court of Cassation of Belgium), Translated by Johan Vandendriessche' (2016) 13 DE&ESLR 1.

[65] ibid para 6.

[66] ibid para 7.

[67] ibid para 9.

[68] ibid.

[69] Court of Appeal, Antwerp, Case No 2016/CO/1006, 15 November 2017. The Court of Cassation rejected the appeal: Court of Cassation, Case No P.17.1229.N, 19 February 2019.

[70] Investigatory Powers Act 2016 (UK) section 15 (IPA). The authorisation for obtaining communications data (non-content data such as traffic data and internet connection records) is explicitly extraterritorial in scope: ibid section 85.

[71] ibid section 261.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

provide or offer services to persons in the UK.[72] The IPA expressly provides that the relevant authority may serve the warrant 'on a person outside the United Kingdom for the purpose of requiring the person to provide assistance in the form of conduct outside the United Kingdom', which includes disclosure of the relevant data.[73] The IPA does allow providers to refuse to fulfil the warrant if it is 'not reasonably practicable', which may include a situation where the provider is barred from disclosing the data by the law of another country.[74] Thus, similar to Belgium and the EU, the UK extends its enforcement jurisdiction based on the provision of services to users within its territory.

The US also exercises extraterritorial investigative jurisdiction when service providers are incorporated within US territory, but the data may be stored overseas. US courts are not shy about demanding data disclosures from domestic service providers (or other companies like banks) for data stored outside its territory. Since 1982, US courts have found that subpoenas to US companies extend to documents, no matter their location, as long as they are within the 'possession, custody, or control' of a company that is physically present within the territory of the US.[75] Subpoenas as administrative orders, however, are distinct from warrants in US law. While subpoenas are used to compel the production of information generally, warrants are required to obtain the content of communications.[76] Because US law considers the content of communications to be especially private, the law requires a warrant for the disclosure, which is a more legally onerous process than a subpoena. Subpoenas may be issued by court clerks or licensed attorneys, whereas warrants may only be issued by a judge upon a showing of probable cause.[77] Traditionally, warrants were limited to evidence held within US territory, because warrants usually involved LEAs physically seizing evidence. This territorial limit was challenged by the US Government in the *Microsoft Ireland* case, in which the Second Circuit Court of Appeals found that a US warrant for content data served on Microsoft could not reach data that the service provider stored in Ireland.[78] In response to this case, in 2018, Congress passed the CLOUD Act, which clarified that warrants extend to any data within a service provider's 'possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States'.[79]

The US approach is consistent with the approach in the EU, UK and Belgium in that the location of the data itself is irrelevant to the determination of jurisdiction. US law is concerned only with the location of the service provider. However, unlike the European approaches, US law is arguably more limited in scope to service providers that have a sufficiently strong presence on US territory to trigger personal jurisdiction.[80] This

[72] UK Home Office, 'Interception of Communications Code of Practice' (2022) paras 2.4–2.5.

[73] IPA (n 70) section 41.

[74] ibid section 43. This also applies to the acquisition of communications data: ibid section 85.

[75] *In Re Grand Jury Proceedings (US v Bank of Nova Scotia)* 691 F 2d 1384 (11th Cir 1982) (US).

[76] Stored Communications Act, 18 USC sections 2701–2712 (1986) (US).

[77] Federal Rules of Criminal Procedure, rules 17 & 41 (US).

[78] *Microsoft v United States* 829 F3d 197, 221 (2nd Cir 2016) (US) *(Microsoft Ireland)*.

[79] ECPA (n 2) section 2713 (2018) (amended by Pub L 115-141, div V, section 103(a)(1), 31 March 2018, 132 Stat 1214). The CLOUD Act amended the Stored Communications Act, which is part of the ECPA.

[80] *International Shoe Co v Washington*, 326 US 310, 318 (1945) (SCOTUS); *Daimler AG v Bauman*, 571 US 117, 138–39 (2014) (SCOTUS).

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

determination is based on 'sufficient contacts' with the territory, not the targeting of services (though sufficient contact may be established through 'directed conduct' that includes, among other factors, the targeting of services).[81]

The evolution of connecting factors to territory is based on the location and activities of service providers rather than the location of the data itself. This makes sense given the technical realities of data. These connecting factors, typically used to justify the exercise of extraterritorial prescriptive jurisdiction, have been used by these States to justify the exercise of extraterritorial enforcement jurisdiction. In other words, these are clear examples of the exercise of extraterritorial investigative jurisdiction.

The potential for a conflict of laws arises whenever States exercise extraterritorial investigative jurisdiction unilaterally. These conflicts are usually raised by service providers that are caught between conflicting liabilities. Service providers are placed in this position when a court order in one country mandates disclosure of the data while a 'blocking' law in a different country simultaneously prohibits disclosure, as seen in the example of a French murder investigation in Section 1 of this article. A blocking statute is any law that may restrict disclosure of data, which includes data protection laws most prominently, but also laws intended to protect economic concerns or fundamental rights.[82] Some States consider the potential for such conflicts to impact negatively on service providers and may moderate the exercise of investigative jurisdiction accordingly, such as the UK IPA does. US and EU law also provide conflict resolution mechanisms for this situation based on the principle of comity. Before considering the application of comity analyses in more detail, it is necessary first to consider whether these conflicts implicate the principle of non-intervention. The physical incursion of a State agent into the territory of another State to seize evidence may constitute an unlawful intervention. As a starting point, would the digital incursion of a State through the unilateral exercise of investigative jurisdiction also violate this fundamental principle of international law? The following section explains that, in most cases, it is unlikely that investigative jurisdiction rises to the level of a prohibited intervention, thus necessitating a closer look at the principle of comity to resolve conflicting sovereignty interests.

3.3.2. Implications of State practice: the duty of non-intervention

This section argues that the extraterritorial exercise of investigative jurisdiction can be consistent with the international law principle of non-intervention. As discussed in Section 1, the sovereignty principle in international law has two corollaries—jurisdiction and non-intervention. These principles are linked. Exercising enforcement jurisdiction on the territory of another State may contravene the duty of non-intervention. In the *Corfu Channel* case, the ICJ held that the British navy unlawfully intervened in the

[81] DoJ, 'Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act' (White Paper, April 2019); but see T Cochrane, 'Hiding in the Eye of the Storm Cloud: How Cloud Act Agreements Expand US Extraterritorial Investigatory Powers' (2021) 32 DukeJComp&IntlL 153 (arguing that the US Constitution would not prohibit US courts from exercising jurisdiction over a foreign entity or individual).

[82] Walden (n 6) 443–44. See also H Buxbaum, 'Assessing Sovereign Interests in Cross-Border Discovery Disputes: Lessons from Aerospatiale Symposium: International Litigation' (2003) 38 TexILJ 87.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

sovereign affairs of Albania when it attempted to gather evidence on Albanian territory through physical force.[83] Do the virtual extensions of evidence gathering powers reviewed in this article also violate the non-intervention principle? If so, then the exercise of investigative jurisdiction should be considered to violate international law. Further analysis is needed to answer this question.

The ICJ defined the duty of non-intervention in the *Nicaragua* case as 'the right of every sovereign State to conduct its affairs without outside interference'.[84] Interference becomes a prohibited intervention when two conditions are met. First, States cannot intervene in the affairs of other States 'on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of political, economic, social and cultural system, and the formulation of foreign policy.'[85] Second, this '[i]ntervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones'.[86] The ICJ went on to state that coercion was 'the very essence of prohibited interventions' and was 'particularly obvious' when force, either through military action or indirect armed activities (such as support for opposition fighters), was present.[87]

Most of the case law and scholarship on the non-intervention principle can be found within the context of use of force and military action. Outside of this context, some scholars are beginning to look at the principle in the context of cyberattacks and electoral interference through online disinformation campaigns.[88] However, this scholarship is speculative about how the principle may apply in new contexts. Nonetheless, applying the principle of non-intervention in the context of cyberattacks and electoral interference is more straightforward than in the context of investigative jurisdiction.

In cases of electoral interference, the intervention is clearly related to affairs of the State on which the State should decide freely (i.e. its political system), and the relevant question becomes whether the coercive element is sufficiently present.[89] Buchan suggests that coercion requires acts 'of a sufficient magnitude', which are likely to be 'acts intended to force a policy change in the target State'.[90] This definition does seem somewhat circular. An act is coercion if it is forceful enough to change a policy, which is the required intent for a prohibited intervention. However, the point stands that 'mere influence' should not be enough to amount to coercion.[91] Whether misinformation or disinformation campaigns aimed at elections move beyond 'mere influence' to coercion is an open question.[92]

[83] *Corfu Channel* (n 29) 35.
[84] *Nicaragua* (n 26) para 202.
[85] ibid para 205.
[86] ibid.
[87] ibid.
[88] See n 30.
[89] Tsagourias (n 30) 49–50.
[90] Buchan (n 30) 223–24 (citing and agreeing with M Jamnejad and M Wood, 'The Principle of Non-Intervention' (2009) 22 LJIL 345, 348).
[91] ibid 224–25.
[92] Tsagourias (n 30) 48.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

Both Tsagourias and Buchan assert that the cyberattacks on Estonia in 2007 amounted to a prohibited intervention.[93] The cyberattacks harmed vital government websites and internet infrastructure for three weeks, resulting in economic loss, data loss and the loss of functionality of government services. The cyberattacks were a response to the Estonian Government's decision to move the Bronze Soldier statue, a Soviet-era war memorial. The cyberattacks are widely viewed as a Russian attempt to coerce Estonia into changing its decision about the location of the memorial. Buchan argues that a State's decisions regarding war memorials should be a free choice for the government.[94] Given this motive and the deleterious effects of the attack, it would meet the standard required by *Nicaragua* and amount to a prohibited intervention.

While cyberattacks may be the closest analogous situation considered by current scholarship, they remain vastly more serious than a production order directing a private company to disclose a copy of data. A production order should not cause a deleterious effect in the foreign State to the same extent as a cyberattack. Production orders usually require a copy of data to be made, not the deletion of data. However, it should be considered whether a production order has any other coercive effect beyond merely accessing the data and systems.

In the minimal extraterritoriality model, there may be no effect at all in the foreign State besides a service provider's employee making a copy of data and sending it to the LEA in the investigating State. The foreign State would have no interest in the data subject or criminal case.

In the significant extraterritoriality model, could it be said that an order for data on a citizen or resident of the foreign State is an intervention attempting to force a policy change in that State? It is unlikely. As the model case makes clear, the investigating State's internal affairs are prompting it to act, rather than intending to meddle in the affairs of a foreign State. Even with the cross-border issues that arise due to the data subject's location, the investigating State is issuing a production order to investigate and prosecute a crime that has occurred in its territory. If coercion is 'the very essence of … prohibited intervention', then the act of sending a production order to a private company that is primarily headquartered in another State (yet offers services in the investigating State) for the purposes of a criminal investigation in the investigating State would not seem to be a prohibited intervention.[95]

Even if a coercive order to a private company amounts to coercion under the *Nicaragua* definition, the coercion must be for the purpose of influencing a policy change in the foreign State. For the sake of argument, could a production order influence or be seeking to influence a policy change in a foreign State?

One might argue that routine production orders to service providers based in another State implicitly attempt to coerce the other State not to enforce its blocking statute. However, the action that is coerced by the production order is an action taken by a private company, not the government of the State in which it is located. Notably, that

[93] Buchan (n 30) 225–26; Tsagourias (n 30) 48.

[94] Buchan (n 30) 226.

[95] One could see here how the analysis has the potential to change when considering unmediated direct access by a government to networks, servers or data within a third State, such as in a case of law enforcement hacking. But this activity is beyond the scope of this article.

State would still be free to enforce its blocking statute. In most investigations, the investigating State's intention in issuing a production order is to obtain data for a domestic criminal investigation. Given that we must examine the intention behind State action to determine whether it rises to the level of a prohibited intervention, a coercive production order for data from a foreign State is not an intervention in the affairs of the State where the service provider is incorporated so much as it is an intervention in the affairs of a private company.

This observation raises an important point often overlooked in the literature on LEA access to data across borders. To what extent should the onus be on service providers to structure their businesses in such a way as to comply with their concurrent legal obligations? These global companies offer services in many States, so they voluntarily subject themselves to concurrent legal obligations. Service providers can structure their data storage so that the 'possession and control' over relevant data takes place in a jurisdiction that allows the service provider to comply with production orders from the States in which they offer services. Of course, this business structure may be expensive—one of the disadvantages of data localisation laws mentioned above. Service providers should not be able to locate themselves in jurisdictions that block disclosure of all the data they possess or control to avoid compliance with legal obligations for the disclosure of data in countries in which they offer services. To avoid regulatory arbitrage and data havens (like tax havens), the extraterritorial exercise of investigative jurisdiction should be accommodated as long as it does not unreasonably interfere with the sovereignty of another State.

In exceptional circumstances, it might be argued that the significant extraterritoriality model could result in a prohibited intervention in two types of cases. First, there may be a prohibited intervention if the State sending the production order intends to use the data disclosed to intervene in the sovereign affairs of a foreign State. For example, a case could involve a State seeking data on a foreign leader to blackmail that person into action (or inaction). Or, less directly, an autocratic regime may obtain data on many persons abroad to intimidate and suppress dissent, creating a chilling effect on freedom of expression. In these types of cases, it is possible for States to weaponise production orders as tools to intervene in the sovereign affairs of foreign States. These orders would violate the principle of non-intervention and be prohibited by international law.

Second, it may be possible that a production order could coerce a private entity to disclose data in an attempt to preclude the foreign State from prosecuting a crime over which it also has jurisdiction. The effectiveness of such a strategy would be questionable, however, given that a copy of the digital evidence should still be available to the foreign State. Similarly, the foreign State may not be barred by the principle of *ne bis in idem* (double jeopardy) if it contests the legitimacy of a foreign prosecution. In this scenario, the exercise of investigative jurisdiction would still be unlikely to reach the magnitude of an effect needed to amount to coercion. However, even if falling short of a prohibited intervention, these actions may still constitute an unreasonable interference in the sovereign affairs of another State. Investigative jurisdiction should be limited in these cases, as will be discussed in more detail in Section 5.4 regarding the fourth limitation.

Most cases involving extraterritorial investigative jurisdiction are unlikely to violate the duty of non-intervention. Given the nature of technology and global service providers, concurrent legitimate jurisdictional claims over the same data are bound

to occur. While international law allows for concurrent claims to jurisdiction, it does not provide for a second-level inquiry that orders these claims or resolves jurisdictional conflicts. The US CLOUD Act and EU e-Evidence Regulation include comity analyses to fill this gap in the law of jurisdiction. The following section will argue that the principle of comity is well suited to underpin a second-level ordering mechanism to ensure respect for the sovereign equality of States.

The exercise of investigative jurisdiction may be consistent with international law principles as long as the investigating State ensures that the exercise of jurisdiction does not interfere unreasonably with another State's sovereignty. This limitation on investigative jurisdiction is based on the principle of comity. Comity, as a principle of sovereign deference, may guide both the exercise of investigative jurisdiction and the resolution of conflicts of jurisdiction.

4. Comity

4.1. Comity in international law

The principle of comity is not well defined in international law. Scholars have defined comity variously as: 'a principle' by which 'courts seek to promote international harmony by giving deference to the sovereign interests of the affected nations';[96] 'a traditional diplomatic and international law concept used by States in their dealings with each other';[97] 'deference to foreign government actors that is not required by international law but is incorporated in domestic [US] law';[98] 'a jurisprudential principle holding that courts should acknowledge and in some cases defer to the legitimate sovereignty interests of other states';[99] 'a species of accommodation: it involves neighbourliness, mutual respect, and the friendly waiver of technicalities';[100] and 'neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other'.[101] A brief outline of the history of comity will show that it is best viewed as a principle of sovereign deference which means that States should sometimes moderate the exercise of their jurisdiction in deference to another sovereign State, even if the exercise of jurisdiction would not constitute a prohibited intervention.

Comity began as a principle to avoid conflicts of laws when sovereignty was strictly territorially applied. Early international law scholars observed that courts should sometimes apply foreign law in deciding disputes in domestic courts to avoid conflicts of laws, usually to facilitate cross-border trade.[102] In this early sense, comity was a discretionary principle, recognising the application of foreign law unless contrary to public policy.[103] Comity promoted goodwill, courtesy and reciprocity and was

[96] D Zambrano, 'A Comity of Errors: The Rise, Fall, and Return of International Comity in Transnational Discovery' (2016) 34 BerkJIntlL 157, 160.

[97] Ryngaert (n 17) 147.

[98] W Dodge, 'International Comity in American Law' (2015) 115 ColumLRev 2071, 2078.

[99] See Woods (n 6) 40–41 (arguing that sovereign deference works in the internet governance context because it encourages reciprocity).

[100] Crawford (n 8) 21.

[101] *Hilton v Guyot* 159 US 113, 163–64 (1895) (SCOTUS).

[102] J Paul, 'Comity in International Law' (1991) 32 HarvIntlLJ 1, 15.

[103] H Yntema, 'The Comity Doctrine' (1966) 65 MichLRev 9, 26.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

accepted as a pragmatic solution to the problem of increasingly concurrent claims of jurisdiction due to globalisation.[104]

Over the next 100 years, comity developed further in private international law, especially in US foreign relations law. In the context of antitrust regulation, comity evolved from a doctrine of recognition of foreign law into a doctrine of restraint, used by US courts to determine when US antitrust law should (or should not) be applied to foreign conduct or actors.[105] This doctrine was necessary to counterbalance the expansiveness of the effects test, which US courts used to justify the extraterritorial application of antitrust regulation.[106] US courts instrumentalised comity, developing multifactor interest-balancing analyses, which resemble the multifactor analyses in the US CLOUD Act and EU e-Evidence Regulation.[107]

US courts also adopted comity within the context of transnational discovery. As mentioned in Section 3.3, US courts have wide discretion in ordering the production of documents through subpoenas, as long as the court has jurisdiction over the party in control of the documents.[108] To mitigate the sovereignty concerns of foreign States that may also have jurisdiction over the party or information in question, US courts adapted the comity process used in antitrust cases to transnational discovery.[109] When parties may be subject to inconsistent laws on the production of information, US courts consider several factors to determine which State's law should apply. These factors may include the importance of the information, the territorial origin of the information, other available sources of information, the 'important interests of the United States' or of 'the State where the information is located',[110] the potential hardship of the party facing conflicting legal obligations and whether the party acted in good faith to comply.[111]

US courts' application of the comity-based, interest-balancing process has been criticised, however, as biased in favour of domestic interests.[112] Perhaps unsurprisingly, domestic courts tend to favour their interests over those of a foreign State in determining whether to exercise jurisdiction. Nonetheless, interest balancing based on comity at least 'requires courts to explicitly consider both domestic and foreign State interests'.[113]

[104] J Paul, 'The Transformation of International Comity' (2008) 71 LCP 19.

[105] Ryngaert (n 17) 152.

[106] H Buxbaum, 'Territory, Territoriality, and the Resolution of Jurisdictional Conflict' (2009) 57 AJCL 631, 645.

[107] See *Hartford Fire Ins Co v California* 509 US 764 (1993) (SCOTUS); *Timberlane Lumber Co v Bank of America NT* 549 F2d 597 (9th Cir 1976) (US).

[108] G Sant, 'Court-Ordered Law Breaking: US Courts Increasingly Order the Violation of Foreign Law' (2015) 81 BrookLRev 181.

[109] Also referred to as a 'reasonableness' test by some scholars: Ryngaert (n 5) 547.

[110] *Société Nationale Industrielle Aérospatiale v US Dist Court for S Dist of Iowa* 482 US 522, 544 n 28 (1987) (quoting *Restatement of Foreign Relations Law* (Revised) section 437(1)(c) (Tent Draft No 7, 1986)) (SCOTUS).

[111] *Linde v Arab Bank PLC* 706 F3d 92, 110 (2nd Cir 2013) (US); *In re Sealed Case (Chinese Banks)* 932 F3d 915, 932 (DC Cir 2019) (US).

[112] Zambrano (n 96) 176.

[113] B Van Alsenoy and M Koekkoek, 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the "Right to Be Delisted"' (2015) 5 IDPL 105, 117.

In the EU, comity is not generally used in private international law but remains a public international law concept of courtesy and diplomacy.[114] Thus, the e-Evidence Regulation's inclusion of a comity process like those found in US law is a new development in European law, which has imported private international law comity processes (predominantly used in the US) into European public law.

While comity processes developed in the context of private international law, the foundation of these processes is still linked to public international law as a doctrine of sovereign deference. These comity processes may be well suited to fill the gap in the international law of jurisdiction, which lacks a mechanism for ordering concurrent jurisdictional claims. These comity processes can provide a framework to weigh the jurisdictional links with one State against those with another to determine whether the exercise of jurisdiction is justified.[115] Thus, the principle of comity 'bridges' the divide between traditional public international law—and its conceptions of sovereignty and jurisdiction—and the conflicts of laws that occur in private civil suits.[116]

Comity bridges the gap between private and public international law, but the perspective of the court that is applying comity principles tends to differ between the two contexts. In private international law, courts focus on domestic law in determining whether a foreign law should apply.[117] This contrasts with some courts that consider comity processes as a requirement of public international law. For example, in the UK, the principle is used as a synonym for public international law[118] or to mean deference to sovereignty, such as in cases involving diplomatic or sovereign immunity.[119] As a principle of sovereign deference, comity underpins several 'comity doctrines', such as the 'assumption against extraterritoriality',[120] *lis alibi pendens* (or rules on anti-suit injunctions)[121] and *forum non conveniens*.[122]

These courts focus on whether a foreign law should be applied given the domestic position of its 'regulatory authority vis-à-vis other sovereigns'.[123] Or, as Maier puts it, '[t]he issue is one of normative perspective and the choice is between the internal perspective of the particular norms of one state and the external perspective of some

[114] B Pearce, 'The Comity Doctrine as a Barrier to Judicial Jurisdiction: A US-EU Comparison Note' (1994) 30 StanJIntlL 525, 172–73; T Schultz and N Ridi, 'Comity and International Courts and Tribunals' (2017) 50 CornellInt'lLJ 577, 580–81.

[115] *Case Concerning the Barcelona Traction, Light and Power Company, Limited (Belgium v Spain) (New Application: 1962)* (Merits) [1970] ICJ Rep 42, para 70.

[116] A Mills, *The Confluence of Public and Private International Law: Justice, Pluralism and Subsidiarity in the International Constitutional Ordering of Private Law* (CUP 2009) 259–64; D Childress, 'Comity as Conflict: Resituating International Comity as Conflict of Laws' (2010) 44 UCDavisLRev 11, 14; Paul (n 102) 34.

[117] Buxbaum (n 106) 649; HG Maier, 'Jurisdictional Rules in Customary International Law' in KM Meessen (ed), *Extraterritorial Jurisdiction in Theory and Practice* (Kluwer Law International 1996) 64, 79.

[118] See *Dallal v Bank Mellat* [1986] QB 441 (UK); *Oppenheimer v Cattermole* [1976] AC 249 (UK); FA Mann, *Foreign Affairs in English Courts* (Clarendon Press 1986) 137–39.

[119] *Belhaj v Straw* [2017] AC 964 (UK); *Fayed v Al-Tajir* [1988] QB 712 (UK); *Buck v Attorney-General* [1965] Ch 745, 770 (UK); see generally T Schultz and J Mitchenson, 'Rediscovering the Principle of Comity in English Private International Law' (2018) 3 ERPL 311.

[120] *Lawson v Serco Ltd* [2006] UKHL 3, 6 (UK).

[121] *Bloom v Harms Offshore GmbH & Co* [2009] EWCA Civ 632 (UK).

[122] *The Abidin Daver* [1984] AC 398, 411 (UK).

[123] Buxbaum (n 106) 649.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

neutral or, at least, less subjective standpoint'.[124] Similarly, Mills reasons that the perspective of the State actor (whether it be a policymaker or court) in conducting interest-balancing analyses can affect the decision's consistency with public international law.[125] Mills uses a subjective/objective distinction to elaborate on this point, which is evaluated from an international law point of view, which this article adopts to show how bias may be reduced in comity analyses.

Comity's bias problem arises primarily in the subjective interest analysis used in private international law. An interest is subjective from an international law standpoint when a State claims or asserts such an interest by regulation.[126] Basically, the State actor asks, 'is there a domestic law that applies?', not 'should there be a domestic law that applies given international law principles of jurisdiction?'. By contrast, an objective interest analysis does not focus on whether the State has claimed an interest, but on whether that State's claim is objectively legitimate.[127] Thus, the analysis does not just focus on whether the State has a law that applies, but on whether that law is consistent with international law principles of jurisdiction. In other words, the decision-maker must determine that there is 'a sufficient nexus between the state and the relevant events' by reference to jurisdictional principles, such as territoriality and personality.[128] Focusing on objective interests can eliminate bias because an objective interest-balancing analysis requires the court to look beyond the existence of applicable domestic law to the quality of the connections between the State and the case. By reframing the comity processes used in private international law (and adopted in the US CLOUD Act and e-Evidence Regulation) as public international law processes focused on preserving the sovereign equality of States, States may use these frameworks to order concurrent jurisdictional claims over digital evidence in a manner that is consistent with international law.

4.2. Comity frameworks in the CLOUD Act and e-Evidence Regulation

The CLOUD Act contemplates two types of comity processes: a statutory process for conflicts of laws between a US production order and the law in the State of the QFG, and the retention of the common law comity analysis (the multifactor test identified in Section 4.1 with regards to transnational discovery) for other conflicts. This distinction is important. While CLOUD Act Agreements are intended to significantly reduce conflicts of laws caused by the exercise of investigative jurisdiction, there may still be conflicts in limited situations. For these conflicts, the US considers special (and specific) deference to QFGs. The CLOUD Act also retains the common law comity analysis for conflicts of laws with States without an agreement, but it is often more deferential to US interests.[129]

[124] Maier (n 117) 79.

[125] Mills (n 116) 259–64. Mills identifies three different types of interest analyses in private international law and shows that objective and systemic interests are consistent with public international law principles.

[126] ibid 260.

[127] ibid 261.

[128] ibid 261–62.

[129] Sant (n 108).

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

A service provider would raise the potential conflict of a US order with the law of a QFG only when the required disclosure concerns a data target that is not a US person and the disclosure would violate the laws of a QFG.[130] In that situation, the court considers several factors to determine if the order should be upheld. These factors include the interest of the US in seeking the data, the interest of the QFG in prohibiting disclosure, the potential penalties on the service provider, the location and nationality of the data subject including any connection to the US, the service provider's connection to the US, the importance of the data and the availability of other means of access.[131]

These factors are similar to the common law comity analysis developed in US transnational discovery case law. The interests of each country as they relate to the disclosure of the data are considered generally, seemingly allowing for a wide measure of discretion. The importance of the information to the investigation and the availability of alternative methods of obtaining the information are also practical factors for the court to consider in both analyses. These considerations may influence the weight given to the general sovereignty interest of the investigating State, as cases involving vital digital evidence that may only be obtained by the investigative measure would weigh heavily in favour of the investigating State due to its strong interest in avoiding criminal impunity.

As with the common law comity analysis, the court may also consider the potential for hardship on the provider. Practically speaking, minimising hardship on service providers can be beneficial to ensuring sovereignty because it encourages service providers to be transparent about conflicting liabilities and bring challenges that implicate the sovereign interests of another State, which may include the fundamental rights of the data subject. The European Court of Human Rights (ECtHR) has recognised the service provider's role as an 'important safeguard' against abusive State surveillance practices.[132]

The CLOUD Act's statutory comity mechanism manages the risk of conflict with a QFG when enhanced extraterritoriality concerns based on nationality and territory are present. The statutory comity analysis, in effect, recognises that while the location of the data itself is not intrinsically tied to the sovereignty of the State in which it is found, the location of the target and the target's nationality may raise legitimate claims that a QFG has a stronger sovereignty claim to that target's data than the US.[133]

The EU e-Evidence Regulation 'provides for a specific mechanism for judicial review where compliance with a European Production Order would prevent a service provider from complying with legal obligations deriving from the law of a third country'.[134] The Regulation does not call the mechanism a 'comity' analysis. However, recital 74 states that this mechanism is included to 'ensure comity'.[135] The e-Evidence Regulation is the first piece of EU legislation in the criminal justice context to reference comity. While the EU has coordination systems for resolving situations where multiple States have

[130] ECPA (n 2) section 2703(h)(2).
[131] ibid.
[132] *Roman Zakharov v Russia* (2016) 63 EHRR 17, para 269.
[133] J Daskal, 'Privacy and Security Across Borders' (2019) 128 YaleLJ: Forum 1029, 1036.
[134] e-Evidence Regulation (n 45) recital 74.
[135] ibid.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

the competence to prosecute a criminal case,[136] this is the first conflict resolution mechanism that references comity in EU criminal law.

Under the e-Evidence Regulation, when a service provider raises a challenge to an order based on a conflict of laws with a third country, a court considers several factors in assessing whether the order should be upheld.[137] The Regulation directs the court to put particular weight on the interests of the third country, including fundamental rights and national security interests, and the connection between the criminal case and the States in question.[138] This connection should be considered in reference to the location, nationality or residence of the data subject or the victim of the criminal offence and the location of the crime itself. The factors also include the connection between the service provider and the third country (with data location not being enough to establish a connection), the interests of the investigating State in obtaining the data, the seriousness of the criminal offence, the importance of obtaining the evidence quickly and the potential penalties for the service provider.[139]

These factors indicate similar sovereignty considerations as under the US comity analyses but with a few additions. The victim's location, nationality and residence are considered, which tie into the passive personality principle in international law, adding another dimension to the ties between personality and sovereignty. The location of the criminal offence is also a relevant interest of the States involved.

Special attention is drawn to the potential that the third State's interests are based on protecting fundamental rights or national security. It may signal that courts should consider fundamental rights and national security considerations to be sufficiently weighty to preclude the investigating State's exercise of extraterritorial investigative jurisdiction. Recital 74 details that one of the purposes behind the review mechanism is 'to protect the individual concerned'.

Another of the purposes behind this review mechanism is 'to ensure comity with respect to the sovereign interests of third countries'.[140] In particular, the European Commission was concerned that the e-Evidence Regulation may result in 'legitimisation of similar production orders by non-EU countries with respect to data held in the EU or providers headquartered in the EU', especially for non-EU countries that lacked similar fundamental rights safeguards.[141] It suggested that the conflicts-of-laws provision may mitigate those sovereignty concerns by showing deference to foreign law such that, in the reciprocal situation, Member States could request that third countries defer to EU data protection law under a similar comity analysis.[142] This reciprocity is foundational to the principle of comity in public international law.

[136] For example, EU Agency for Criminal Justice Cooperation, 'Guidelines for Deciding "Which Jurisdiction Should Prosecute?"' (2016) <https://www.eurojust.europa.eu/publication/guidelines-deciding-which-jurisdiction-should-prosecute>.

[137] e-Evidence Regulation (n 45) art 17.

[138] ibid.

[139] ibid.

[140] ibid recital 74.

[141] European Commission (n 1).

[142] ibid 58–59.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

5. The concept of investigative jurisdiction

Given this State practice and the principles of jurisdiction discussed throughout this article, this section sets out a conceptualisation of extraterritorial investigative jurisdiction that is consistent with international law principles. To this end, four limitations on investigative jurisdiction are required. The first three limitations indicate first-order considerations, that is, they are requirements that States have a suitable basis for exercising investigative jurisdiction. The final limitation is a second-order consideration concerning the reasonableness of the exercise of jurisdiction based on comity, which involves the strength and balancing of State sovereignty interests and fundamental rights.[143]

5.1. First limitation: jurisdiction over the criminal activity

First, the investigating State must have jurisdiction to prosecute the crime. Jurisdiction to prosecute is established by showing a connection between the State and an element of the crime based on one of several principles of jurisdiction—the personality principle (based on the nationality of the suspect or victim), the protective principle (based on a legitimate interest of the State to defend itself), the universality principle (for an offence so grave any State may prosecute it) or the territoriality principle (where an element of the crime occurred or had an effect on the territory of the State).[144] If the State does not have jurisdiction to prosecute a crime for which the data in question is expected to be evidence, then the State cannot exercise investigative jurisdiction.

Importantly, this cannot be the only limitation or condition on exercising jurisdiction. As Paul de Hert and Cedric Ryngaert have both identified, allowing any State with prescriptive jurisdiction over criminal activity to have jurisdiction over any digital evidence that may pertain to such criminal activity would dramatically expand the scope of production orders.[145] This expansive scope might implicate the sovereignty interests of other States. These interests are addressed in the other limitations.

5.2. Second limitation: jurisdiction over the service provider

The second limitation on investigative jurisdiction requires the investigating State to have jurisdiction over the service provider. Rather than the physical location of data, this article has shown that States focus on the service provider's location, or the location of the services offered to establish the connection to justify jurisdiction. Given the globalised nature of service providers, it does not make normative sense to require the consent of the State where the service provider is predominantly based for every

[143] Ryngaert (n 5) 187: 'the checks and balances offered by the law of prescriptive jurisdiction, which comprises of first-order (territoriality, nationality, universality) and second-order limitations (connection, reasonableness), may be well suited for a tailored delimitation of enforcement jurisdiction in cyberspace'.

[144] Hörnle (n 6) 83.

[145] C Ryngaert, 'Enforcement Jurisdiction in A-Territorial Spaces: Addressing Crime on the High Seas and in Cyberspace' in M Ó Floinn et al (eds), *Transformations in Criminal Jurisdiction: Extraterritoriality and Enforcement* (Hart Publishing 2023) 184, 185; P de Hert et al, 'Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From *Yahoo Belgium* to *Microsoft Ireland*' (2018) 9 NJECL 326, 352.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

production order from every country in which the services are offered. While the State of the service provider's primary location may have a greater sovereignty interest in some of the activities of service providers subject to their laws, it does not necessarily have a strong enough sovereignty interest to justify acting as the gatekeeper for all data held by that service provider.

Jurisdiction over the service provider may be established in several ways, as shown in the State practice reviewed in this article. States may establish jurisdiction over a service provider headquartered in (or with certain business contacts with) the territory, as the US has done. States may establish jurisdiction over service providers based on the provider offering services in the territory or targeting residents with services, as Belgium, the EU and the UK have done. States can permissibly apply extended territoriality principles, like the targeting and effects tests, to establish a genuine connection to the service provider, subject to the other relevant limitations. Finally, States may also establish jurisdiction over service providers through a relevant international agreement based on mutual trust, such as the UK-US CLOUD Act Agreement.

Whether investigative jurisdiction applies to LEAs' unmediated direct access to digital evidence is a separate and controversial question. This article has focused on the jurisdictional scope of production orders that demand data from service providers as intermediaries. However, LEAs may obtain data from various sources beyond service providers. These unmediated direct access mechanisms include publicly accessible data available via the internet,[146] data from the data subject(s) themselves either by consent or court order[147] and data obtained through network investigative techniques—that is, data remotely and directly accessed through a network without consent, often referred to as 'government hacking'.[148] These mechanisms deserve distinct treatment for several reasons. First, the laws authorising direct access may differ from those authorising production orders to service providers as data intermediaries. Second, State practice is more limited in direct access cases, especially for network investigative techniques. Third, unmediated direct access implicates a different analysis given that there may be no intermediary to act as a check on State power. As shown throughout this article, challenges to production orders based on conflicts of laws and sovereign interests are brought by service providers, making service providers an essential check on State power. For these reasons, a comprehensive analysis of the scope of investigative jurisdiction without the limitation of access through an intermediary should be the subject of future research.

5.3. Third limitation: digital evidence and the virtual/physical distinction

Third, investigative jurisdiction must be limited to the production of digital evidence through virtual investigative measures. This limitation respects the traditional territorial limitation on enforcement power for physical access by foreign State

[146] See Cybercrime Convention (n 49) art 32(a).

[147] T-CY, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)' (T-CY Doc No (2014)16, adopted 3 December 2014) 6 <https://rm.coe.int/16802e726e>.

[148] Mayer (n 41).

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

officials to evidence within another State and the non-intervention principle's focus on physical coercion.

By contrast, virtual access is defined here to refer to the investigative measures that LEAs use to obtain digital evidence without the LEA agent physically leaving the territory of the investigating State, as seen in the examples reviewed in this article. These virtual measures involve either the LEA agent or the service provider (acting on the orders of the State) obtaining data that is accessible through a computer network, as contrasted with a physical measure to obtain data by seizing a physical computer or server. Strictly speaking, this type of access can have physical consequences, such as data being moved from one server to another to produce a copy of the data. This type of action can be contrasted with measures taken to delete, remove or alter data, which may violate another State's territorial sovereignty and the non-intervention principle, as discussed in Section 3.3.2.[149] But, generally, measures to obtain copies of data to fulfil production orders should be primarily regarded as virtual or digital in nature.

Investigative jurisdiction for virtual access differs from physical access given the nature of digital evidence. As discussed, data is 'un-territorial'—it may be partitioned and stored in distributed infrastructure, with multiple copies and/or in locations chosen by the service provider's systems for functional purposes (where those locations may be unrelated to the user).[150] Thus, the historical reliance of the law on the physical location of evidence does not make sense when applied to digital evidence. For example, suppose that digital evidence is stored in a server in Iceland by an American service provider, where the data concerns a UK person. In that case, it makes no sense that UK authorities would need to seek permission from the Icelandic Government to obtain the data. If the sought-after data was split between servers in Iceland and Ireland, it would not make sense for UK authorities to seek the permission of both the Irish and Icelandic Governments to obtain the data. In a situation where the location of the data is unknown, location cannot be determinative of the jurisdictional basis for obtaining the evidence. Digital evidence is already different from physical evidence by its very nature, and it throws the traditional evidence gathering paradigms into disarray.

Thus, it makes normative sense for virtual investigative measures to obtain digital evidence to be treated differently from physical investigative measures to obtain physical evidence. The paradigm-shifting nature of digital evidence is the type of technological change that requires a shift in long-standing jurisdictional principles.[151] A virtual investigatory measure usually involves territorial enforcement action by a State's agent

[149] See *Tidal Music AS v Public Prosecution Authority*, HR-2019-610-A (Case No 19-010640STR-HERT, 28 March 2019) paras 70–71 (Supreme Court of Norway). For an English translation, see <https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2019-610-a.pdf>. The Norwegian Supreme Court held there was no sovereignty violation when a LEA remotely copied data from a server in another country because 'no changes were made to the stored information, for instance in the form of deletion or encryption'.

[150] Daskal (n 6).

[151] See Ryngaert (n 145): 'A realist should admit that, because of technological evolutions, the law of jurisdiction may and should evolve too'. See also PS Berman, 'Legal Challenges of Data Dominance: *Yahoo! v LICRA* and *Microsoft-Ireland* cases' in H Watt et al (eds), *Global Private International Law: Adjudication without Frontiers* (Edward Elgar 2019) 392, 403: 'new technologies that alter the culture are precisely the sorts of changes that tend to result in shifts to well-settled legal principles'.

with an extraterritorial effect. There are no boots on foreign ground, so to speak. Because the incursion into foreign territory is not physical, the exercise of virtual jurisdiction has the potential to be minimally invasive. Coupled with the volatile nature of digital evidence described in Section 3, other States should accommodate this type of minimally invasive measure. Of course, whether States should accommodate digital investigatory measures depends on the other limitations discussed in this article.

Not all virtual investigative measures will be permissible exercises of investigative jurisdiction. Rather, this third limitation continues to recognise the prohibition on physical incursions into the territory of another State, as discussed in Section 3.3.2 concerning the principle of non-intervention. Where a virtual investigative measure violates the sovereignty of another State, it is also prohibited. For example, as mentioned in Section 3.3.2, deleting or altering data on a foreign server may violate sovereignty and non-intervention principles. Whether other types of investigative measures unreasonably interfere with another State's sovereignty will require determinations of the strength of the connection between the interested States and the digital evidence sought. In this regard, a comity-based analysis of connecting factors may be used to ascertain whether a virtual investigative measure violates another State's sovereignty, which brings us to the fourth limitation.

5.4. Fourth limitation: sovereignty and non-intervention

The fourth limitation requires States to moderate an exercise of investigative jurisdiction when it would infringe on another State's sovereignty or violate the fundamental rights of the data subject. A comity analysis, like those in the CLOUD Act and e-Evidence Regulation, may guide the exercise of extraterritorial investigative jurisdiction in this regard. The most likely trigger for a comity analysis will be a conflict of laws with another State raised by the service provider. However, this limitation applies regardless. States should be aware of the types of cases and the types of digital evidence that may implicate the sovereignty interests of another State. This deference to another sovereign State is the very essence of comity.

An in-depth examination of the many different types of cases that may require a comity analysis is outside the scope of this article and will be the subject of future work. For now, it is worth noting that the factors within the US and European comity analyses highlight both the territorial and, perhaps most importantly for the blocking State, the personality principles on which these sovereign interests may rest. Returning briefly to the two models of extraterritoriality shows how these principles may be applied.

In the minimal extraterritoriality model, in which only the nature of the global service provider or its data storage practices gives rise to extraterritoriality, the exercise of investigative jurisdiction is unlikely to infringe on another State's sovereignty. The comity factors reviewed in this article show that considerations such as the location of the criminal activity and the citizenship, residency or location of the data subject are likely triggers for the sovereignty interests of another State. When all these factors are connected solely to the investigating State, it makes normative and principled sense to allow the investigating State to impose investigative measures on a global service provider whose services have been used in the territory of the investigating State. If some of these factors also relate to another State, then there is greater potential for the

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

sovereignty interests of another State to be triggered, as is contemplated by the significant extraterritoriality model. In these types of cases, States should not employ investigative measures that may infringe on another State's sovereignty without securing that State's consent to the measure.

A case that is elsewhere along the spectrum of extraterritoriality may then turn on a more detailed assessment of the importance of the evidence, its likelihood of being lost without efficient and expedited access, the type of data being sought[152] and the seriousness of the criminal offence under investigation. Consistent with comity's spirit of reciprocity, States should also want to encourage service providers to bring challenges based on conflicting sovereignty concerns for all States. If service providers are penalised severely for non-compliance, then they may choose to comply rather than raise potential conflicts of laws. Thus, States should consider whether the burden of sanctions might incentivise the future cooperation of service providers.

Finally, while jurisdictional and sovereignty analyses usually do not turn on the application of fundamental rights, such a consideration should be included given the risk of abuse of production orders that are often made without notice to the data subject[153] and the potential that the investigating State may not extraterritorially extend rights' protection to targets of orders outside its territory.[154] When the blocking State's sovereignty interest concerns the application of fundamental rights safeguards—such as those covered by data protection laws—then that interest should outweigh the application of the investigative measure. The e-Evidence Regulation's comity analysis pays special attention to fundamental rights' protection,[155] and States should similarly encourage consideration of this issue. If States wish to extend investigative jurisdiction extraterritorially, then those States must also extend their fundamental rights protections accordingly. Courts are beginning to recognise this obligation, with the ECtHR and the Bundesverfassungsgericht (German Federal Constitutional Court) finding that the obligation to respect rights follows the State action regardless of where the data subject is located.[156] Nonetheless, not all States require LEAs to observe fundamental rights' protections for foreign targets of production orders, including, most prominently, the US.[157]

[152] While not expressly a factor in the CLOUD Act or e-Evidence Regulation comity analyses, the State practice reviewed in this article has shown that the type of data being sought may be a relevant factor as States seem less concerned with blocking the disclosure of subscriber information and traffic/transactional data. See the discussion of voluntary cooperation and the Cybercrime Convention Second Additional Protocol in Section 3.2.

[153] Confidentiality orders usually either accompany a LEA demand for data from a service provider, such as in the US pursuant to ECPA (n 2) section 2705(b), or are the default position by law, such as under the IPA (n 70) section 57. See also e-Evidence Regulation (n 45) art 13.

[154] J Hörnle, 'What Triggers the Extraterritorial Application of Fundamental Rights?—From Effective Control over Territory to State Act Theory in Cross-Border Surveillance' in Ó Floinn et al (n 145).

[155] e-Evidence Regulation (n 45) art 17(6)(a).

[156] See *Wieder and Guarnieri v United Kingdom* (2024) 78 EHRR 8; Bundesverfassungsgericht, Judgment of the First Senate of 19 May 2020 – 1 BvR 2835/17, para 97. The author has relied on the English version: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html>.

[157] A Lubin, 'We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance' (2017) 18 ChiJIL502.

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

6. Conclusion

In the context of transnational digital investigations, some States are moving past the strict territorial limitations on enforcement jurisdiction in favour of extended territoriality principles like the effects doctrine and the targeting test, traditionally used by States to extend the exercise of prescriptive jurisdiction. States usually justify the exercise of jurisdiction over data in the possession or control of global service providers through some type of connection to the State's territory by focusing on the location of the service providers, services, criminal activity or data subjects. The evolution of territorial connecting factors away from the strict location of the digital evidence makes sense, given the 'un-territorial'[158] nature of data in modern communications technologies. In addition to the territoriality principle, States also assert their sovereignty in this context over the data of their own citizens and residents. This practice implicates the personality principle as a justification to block the jurisdiction of a third State that seeks disclosure of data through an extraterritorial exercise of investigative jurisdiction.

The exercise of extraterritorial investigative jurisdiction using extended territoriality principles may lead to conflicts of sovereignty interests, sometimes through an express conflict of laws and obligations on the service providers in possession or control of the sought-after digital evidence. States may minimise the risk of these conflicts occurring by entering into agreements that negotiate permissible extraterritoriality of investigative measures, such as a CLOUD Act Agreement. Nonetheless, States are likely to continue to unilaterally exercise investigative jurisdiction and even cooperative agreements do not eliminate the possibility of conflicts of laws.

State practice has shifted towards some degree of permissible extraterritoriality when exercising investigative jurisdiction, especially in cases involving the minimal extraterritoriality model. However, the nature of digital evidence may also exacerbate existing extraterritoriality concerns, such as those in the significant extraterritoriality model. States must be cautious in exercising investigative jurisdiction in those situations.

Comity is a principle of international law that States must sometimes moderate their exercise of jurisdiction in deference to another sovereign State. This principle can guide States in determining whether to exercise jurisdiction by allowing a weighing of jurisdictional connections to identify the State with the strongest connection to the digital evidence. New legal developments that provide for extraterritorial investigative jurisdiction in the US and EU are accompanied by comity-based judicial review mechanisms to defer to other sovereign States when necessary.

International law principles of jurisdiction must adapt to advances in technology and communications. But future questions remain about the proper role of intermediaries in digital investigations and whether investigative jurisdiction should be exercised in transnational digital investigations when there is no service provider to act as an intermediary between LEAs and data. Presently, these intermediaries are essential to ensuring investigative jurisdiction is exercised in a manner that is consistent with international law.

[158] Daskal (n 6).

https://doi.org/10.1017/S0020589325100985 Published online by Cambridge University Press

Finally, it is acknowledged that the State practice and literature reviewed in this article is primarily limited to Western liberal democracies and Western-oriented scholars. Data localisation laws and related digital sovereignty initiatives in non-Western States show that those States are unlikely to view extraterritorial investigative jurisdiction as compatible with the sovereign equality of States. Indications of the global view of investigative jurisdiction remain conservative—the newly adopted (but yet to be ratified) United Nations Convention on Cybercrime is limited to traditional forms of mutual legal assistance for production orders and other investigatory measures seeking data across borders.[159] For these reasons, it is unlikely that customary international law will ever recognise investigative jurisdiction in the manner conceptualised by this article. At most, investigative jurisdiction will likely be limited to a small group of States, such as those reviewed in this article, alongside bilateral treaties that formalise direct access mechanisms.[160]

Nonetheless, it must be acknowledged that strict views of territoriality and investigative measures are just as likely to negatively impact the sovereignty of States by not allowing LEAs to obtain necessary digital evidence in cases that are primarily domestic investigations. In these cases, represented by the minimal extraterritoriality model in this article, only the nature of technology and global communications service providers gives rise to a need to exercise enforcement jurisdiction extraterritoriality. Subject to the limitations outlined in this article, investigative jurisdiction in these cases should be accommodated in international law.

Acknowledgements. I am very grateful to Christian Henderson, Julia Hörnle, Katalin Ligeti, Dave Michels, Daragh Murray and Ian Walden, whose comments on this draft and earlier versions of the work made it significantly stronger. I am also thankful to both anonymous reviewers, along with the editors at the journal, for helpful feedback and edits. Any errors remain my own.

[159] UNGA 'Report of the Third Committee: Countering the Use of Information and Communications Technologies for Criminal Purposes' (27 November 2024) UN Doc A/79/460.

[160] Ryngaert (n 5) 550.

Cite this article: J Shurson, 'Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations' (2025) ICLQ 1–31. https://doi.org/10.1017/S0020589325100985