German Law Journal (2023), **24**, pp. 537–550
doi:10.1017/glj.2023.24

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Special Issue: International Law and Digitalization

Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts

Cedric Ryngaert

Utrecht University School of Law, Utrecht, Netherlands
Email: c.m.j.ryngaert@uu.nl

(Received 05 April 2023; accepted 05 April 2023)

Abstract

The most eye-catching effect of digitalization on the law of enforcement jurisdiction is the fading into irrelevance of territoriality. Insofar as the "physical" location of digital data—on a server—may be entirely fortuitous and may in fact not be known by the territorial state, it appears unreasonable for that state to invoke its territorial sovereignty as a shield against another state's claims over such data. To prevent a jurisdictional free-for-all, however, it is key that the exercise of extraterritorial enforcement jurisdiction in cyberspace becomes subject to a stringent test weighting all relevant connections and interests in concrete cases. Introducing such a weighting test means that extraterritorial enforcement jurisdiction is no longer governed by binary rules (allowed and not allowed), but becomes a matter of degree, requiring a granular, contextual assessment. It remains the case that such a flexible attitude towards extraterritorial enforcement jurisdiction is not universally shared, and that relevant state practice and expert opinion in favor of the "un-territoriality of data" has a particular Western slant.

Keywords: Enforcement jurisdiction; ubiquity; prescriptive jurisdiction; territoriality

A. Introduction

Cyberspace may appear to be the epitome of deterritorialization at work, as digital data are transferred at lightning speed between users and devices across the globe with little concern for territorial boundaries. Such deterritorialization poses a formidable challenge to the international law of jurisdiction, which is ordered around territoriality. In its original Westphalian understanding, territoriality assumes that, in principle, activities can be tethered to one State's physical territory. When activities become untethered to territory or, given their worldwide effects—tethered to a multitude of territories at the same time—doubts may be cast over the viability of territorial jurisdiction. Indeed, some authors writing in the field of cyberspace have proposed to abandon territoriality as a relevant jurisdictional principle, and instead to use notions such as genuine connection and reasonableness to assess the legality of jurisdictional assertions in cyberspace.[1]

[1] *See generally* Symposium, *A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft*, 109 AJIL UNBOUND 69–74 (2015).

Abandoning territoriality is not self-evident, however, as States continue to rely on territoriality to justify their jurisdictional assertions in respect of cyberspace.[2] States may well be cognizant of the challenges which cyberspace poses to territoriality, but, by and large, they attempt to solve the jurisdictional conundrum by relying on broad interpretations of territoriality[3] or on principles of extraterritorial jurisdiction. In the field of prescriptive jurisdiction, such an approach is less controversial than in the field of enforcement jurisdiction. This is because the international law of prescriptive jurisdiction, which governs the geographical reach of a State's norms, has always given considerable leeway to States to legislate as they see fit, as a corollary of the sovereignty and independence of the State, restrictions upon which cannot be presumed.[4] Such leeway may be normatively justified to the extent that mere prescription of a norm is far less coercive than actual enforcement of that norm. Prescription does not lead the prescribing State to enter the territory of another State, whereas enforcement may well have this consequence. Indeed, a State does not enter the territory of another State in case it does no more than adopt legislation with an extraterritorial reach or put a person on trial for violation of this legislation.[5] In contrast, it does enter another State's territory in case it actually enforces its laws abroad, for example, when it compels compliance with them through coercive measures, such as through searches, arrests and seizures carried out another State's territory. As such enforcement measures intrude far more deeply into another State's sphere of territorially delimited sovereignty, a State's enforcement jurisdiction is considered as strictly limited to its territory.[6]

Thus, we see that in the more liberally regulated field of prescriptive jurisdiction, States, taking their cue from the 19th century distinction between objective and subjective territoriality, as well as the 20th century territorial effects doctrine, exercise territorial jurisdiction as soon as cyber activities originate in, are completed in their territory ("ubiquity"),[7] or have a substantial effect

[2]*See* Jan Kleijssen & Pierluigi Perri, *Cybercrime, Evidence and Territoriality: Issues and Options*, 47 NETH. Y.B. INT'L L. 147, 169–70 (2017) (footnote omitted) ("[T]he basic principles of territoriality established under international law do not provide for clear solutions. However, as States will not wish to move away from these principles, solutions are required which, if not found within these agreed principles, should at least be compatible with them.").

[3]*See also* Bertrand de La Chapelle & Paul Fehlinger, *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*, GLOB. COMM'N ON INTERNET GOVERNANCE PAPER SERIES: NO. 28 (Apr. 2016), at 3 (explaining how to use the term "hyper-territoriality" in this respect).

[4]Case of the SS Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18–19, https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf

> Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable.

[5]*See also* Stéphane Beaulac, *The Lotus Case in Context. Sovereignty, Westphalia, Vattel, and Positivism*, *in* THE OXFORD HANDBOOK OF JURISDICTION IN INTERNATIONAL LAW 51 (Edward Guntrip, M. Fitzmaurice, Daniel Costelloe, Paul Gragl & Stephen Allen, eds., 2019).

[6]*See* SS Lotus 1927 P.C.I.J. at 18.

> Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.

[7]Jean-Baptiste Maillart, *The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime*, 20 ERA FORUM 375, 375–78 (1st ed. 2019) (discussing the ubiquity principle or constituent elements approach). For an extensive overview of relevant German and English practice. see JULIA HÖRNLE, INTERNET JURISDICTION: LAW AND PRACTICE 115–45 (2021), (discussing publication cases, in which illegal content created abroad reaches a territorial audience. She finds that, in Germany, "if an internet publication is likely to disturb the public peace and stir up racial hatred within Germany, this may be sufficient for jurisdiction." She finds that, in England, "in some criminal cases the courts decided that access to illegal publications is sufficient, while in other cases the court have applied the substantial measure test to examine whether the gist of the crime has been connected to England.").

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

there.[8] Where territoriality falls short, for that matter, States can still rely on accepted permissive principles of extraterritorial prescriptive jurisdiction, such as nationality, security, and universality.[9] Cyberspace does not pose structural challenges to the law of prescriptive jurisdiction. The main challenge is rather forensic: given the complex technical nature of cyber systems, how can a genuine (territorial) connection with the regulating State precisely be established?[10]

Structural challenges do exist, however, in relation to the international law of enforcement jurisdiction—on which this Article accordingly focuses. While the ubiquity principle in the law of prescriptive jurisdiction gives States flexibility to territorialize the "un-territoriality" of the Internet,[11] or to rely on principles of extraterritorial jurisdiction, such flexibility is decidedly restricted under the international law of enforcement jurisdiction, at least as traditionally understood. States can only exercise such jurisdiction outside their territory where the territorial (target) State consents, or where customary or conventional international law confers specific authority for such action. There is no such thing as a ubiquity principle or effects doctrine in the law of enforcement jurisdiction that allows for a broad interpretation of territoriality.[12] This means that States are in principle not allowed to carry out law-enforcement operations, including criminal investigations, on foreign States' territory. States wishing to obtain custody over a fugitive located abroad need to rely on extradition treaties. States wishing to secure foreign-based evidence need to make use of mutual legal assistance treaties.

This strict approach to extraterritorial enforcement jurisdiction has come under sustained criticism from both experts and States, however.[13] Discourse and practice increasingly de-emphasize the territoriality of data—its actual location on a server or a device—as a relevant consideration for the valid exercise of enforcement jurisdiction. The Norwegian Supreme Court's decision in the *Tidal*[14] case is instructive in this regard. Tidal is a music streaming company which was accused by Norwegian law-enforcement authorities of artificially inflating listening numbers, thereby defrauding other music artists of their share of subscription revenues. At one point, the authorities searched the companies premises in Norway, downloaded "source codes" from a server in the US, and stored them on a USB stick.[15] They also aimed to extract emails from a Google account belonging to a director based in Norway, while the data were stored on servers in other European countries—the exact location of the data was unknown.[16] The Norwegian Supreme Court did not consider it relevant that the data were located outside Norway, instead basing lawfulness of the enforcement action on the consideration that "[t]he relevant search was carried out by using the access credentials the company had given to" Norwegian law-enforcement authorities, and the action was aimed at a "Norwegian company and its employees present in this

[8]*See* MICHAEL N. SCHMITT, TALLINN MANUAL 2.0: INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS R. 9 (Michael N. Schmitt ed., 2017).

[9]*Id.* at R. 10. *See also* Budapest Convention on Cybercrime art. 22(1), Nov. 11, 2001, ETS No. 185, Ex. Rept. 109–6, for relevant jurisdictional principles in cyberspace, which confers jurisdiction on the territorial State, the State of nationality, the flag State, and the State of registration. Article 22(3) of the Convention also provides for *aut dedere aut judicare* based jurisdiction, referring to the duty to exercise jurisdiction in case of non-extradition based on nationality.

[10]*See* SCHMITT, *supra* note 8, at 57, suggesting reliance on "any substantial connection between the offence and the territory of a State" as the basis for jurisdiction. The question remains, however, at what point a territorial connection is sufficiently substantial to ground territorial jurisdiction.

[11]*See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326, 326–98 (2015) (defining un-territoriality).

[12]Mark Zoetekouw, *Internationaalrechtelijke Aspecten van het Wetsvoorstel Computercriminaliteit III* [*International Law Aspects of the Computer Crime Bill III*], 1 TIJDSCHRIFT VOOR INTERNETRECHT [J. INTERNET L.] 30, 30–33 (2017) (Neth.).

[13]Dan Jerker B. Svantesson, *Internet and Jurisdiction Global Status Report 2019*, INTERNET AND JURISDICTION POLICY NETWORK 109 (Nov. 27, 2019), https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf.

[14]*Tidal Music AS v. The Public Prosecution Authority*, HR-2019-610-A, (case no. 19-010640STR-HRET) (Mar. 28, 2019) (Nor.), https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2019-610-a.pdf.

[15]*Id.* at ¶¶ 6–7.

[16]*Id.*

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

country."[17] According to the Court, "the search will [not] affect another state to an extent that it constitutes a violation of the principle of sovereignty."[18] Such dynamics may weaken the strict prohibition of extraterritorial enforcement jurisdiction in relation to access to evidence abroad, although practice is certainly not (yet) uniform.

The propounded regulatory shift is informed by the technological features of how and where digital data—which can serve as evidence in criminal proceedings—are stored. Digital evidence of crime, including purely domestic crime, may be scattered all over the globe, be stored, split, copied, mirrored, and distributed "in the cloud" on servers chosen algorithmically by Internet Service Providers, for reasons of ease of user access and cybersecurity. Relevant data may be moved from one jurisdiction to another with the click of a mouse ("data volatility") and may be stored in different jurisdictions at the same time. The technical features of cloud computing render territorial location a contingent phenomenon. Combined with the sheer mass of digital data in which criminal law-enforcement agencies are potentially interested,[19] they make mutual legal assistance mechanisms appear outdated and impracticable.[20] Such impracticability is compounded in case it is unclear where relevant data is exactly stored, denoted as loss of—knowledge—of location. The end-result may be that cybercrimes are not adequately prosecuted, leading to an undesirable impunity gap which may be exploited by cybercriminals.[21]

The problems besetting the processing of requests for mutual legal assistance, especially the delays suffered, have led some States to act unilaterally to secure (likely) foreign-based digital evidence. States tend to make use of essentially two methods: (1) directly accessing data using technological means (direct access via remote techniques, including State "hacking"), or (2) ordering Internet intermediaries, for example, private actors, to produce data under their control—indirect access via production orders. Both methods raise concerns under international law as traditionally conceived, as they bypass State consent and appear to amount to prohibited extraterritorial enforcement jurisdiction. As relevant practice is expanding, however, the prohibition may lose force. New norms of customary international law may possibly crystallize, specifically allocating authority to States to exercise forms of "investigative" jurisdiction[22] with an extraterritorial dimension.[23]

Analyzing the arguments currently advanced, it is striking that the legitimating and boundary conditions for such jurisdiction are partly derived from notions belonging to the law of prescriptive jurisdiction. Advocates justify extraterritorial enforcement jurisdiction in cyberspace by relying on permissive principles of prescriptive jurisdiction, such as territorial ubiquity and the

[17]*Id.* at ¶ 68. The latter consideration is also relied on to justify *indirect access*, as discussed below. *See also id.* at ¶ 70, the Supreme Court explained their reasoning as "[t]he data remains on the server abroad. Also, no changes are made to the stored information, for instance in the form of deletion of encryption. A possible seizure is carried out by copying the data onto storage media in Norway."

[18]*Id.* at ¶ 71.

[19]*See* Explanatory Memorandum Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, at 1, COM (2018) 225 final (Apr. 17, 2018) [hereinafter *E. Com. Explanatory Memorandum*] (emphasis added) (explaining that in our contemporary era, digital evidence may in fact be the *only* evidence available).

[20]But for an argument in favor of strengthening mutual legal assistance instead of relying on unilateralism, see Sergio Carrera, Marco Stefan & Vasilis Mitsilegas, *Cross-border Data Access in Criminal Proceedings and the Future of Digital Justice*, REP. OF CEPS & QMUL TASK FORCE (Oct. 14, 2020), at 76–77.

[21]Kleijssen & Perri, *supra* note 2, at 149 (pointing out that "cybercrimes are hardly ever prosecuted due to the difficulties connected with the very nature of the network and of the electronic evidence, which requires immediate access to the data as well as cooperation between the law enforcement agencies and the providers").

[22]*See* Dan Jerker B. Svantesson, *Extraterritoriality in the Context of Data Privacy Regulation*, 7 MASARYK UNIV. J. L. & TECH. 87, 92 (2013) (explaining the term "investigative jurisdiction," although this definition focuses on data privacy rather than criminal law-enforcement).

[23]*Cf.* SCHMITT, *supra* note 8, at R. 11 (emphasis added) ("A State may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects, and cyber activities on the basis of: *(a) a specific allocation of authority under international law; or* (b) valid consent by a foreign government to exercise jurisdiction on its territory.").

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

nationality principle. At the same time, they limit potential jurisdictional overreach by relying on principles of jurisdictional restraint equally borrowed from the law of prescriptive jurisdiction, in particular genuine connection and reasonableness. This double discursive move blurs the lines between the law of prescriptive and enforcement jurisdiction. This process is arguably digitalization's main transformative effect on the law of jurisdiction.

This article discusses how this transformation unfolds in the context of techniques of direct remote access[24] respectively indirect access via production orders.[25] The last part zooms out and examines what the on-going dynamics mean for the future trajectory of the customary international law of enforcement jurisdiction in cyberspace. The main normative argument made in this contribution is that, given the nature of cyberspace and the volatility of data, the strict prohibition of extraterritorial enforcement jurisdiction should give way to a rule that allows extraterritorial enforcement action for investigative purposes in principle, but subjects such action to a number of limiting conditions.

B. Direct Remote Access

Faced with the limitations of mutual legal assistance requests, some States are tempted to unilaterally carry out extraterritorial network searches on foreign computers or servers with a view to securing evidence for use in criminal proceedings. Various techniques can be used in this respect. One technique is for law-enforcement authorities to simply seize and search a device, for example a mobile phone, on their territory and remotely access foreign-stored data accessible from it.[26] This technique was at issue in the aforementioned *Tidal* case.[27] Another—more extreme—technique is "state hacking," for example, law-enforcement authorities breaking directly into computers and searching networks outside the State. There is anecdotal evidence that authorities use such techniques to remotely access and control the "dark web," where illegal activities and transactions take place, such as the exchange of child pornography and the sale of narcotics and weapons.[28]

Techniques of remote access may have a domestic legal basis,[29] although it is a public secret that in some States, law-enforcement agencies carry out remote searches without domestic authorization.[30] In any event, there is no clear authorization under international law for such searches. As they amount to investigative acts that are eventually performed on the territory of another State, they appear to fall foul of the prohibition of extraterritorial enforcement jurisdiction, in the absence of *ad hoc* State consent or treaty arrangements.[31] Multilateral treaty arrangements explicitly authorizing such acts do not currently exist. Article 19.1 of the Budapest Convention on Cybercrime—the leading multilateral convention on cybercrime, which counts 66 Contracting

[24] *See* discussions *infra* Part B.

[25] *See* discussions *infra* Part C.

[26] *See E. Com. Explanatory Memorandum*, *supra* note 19, at 11 (indicating that 20 Member States allow this).

[27] *Tidal, supra* note 14.

[28] *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1075 (2017) (discussing, from a US perspective, "techniques that deploy surveillance software over the Internet to directly access and control criminals' devices").

[29] *See generally* WETBOEK VAN STRAFVORDERING [SV] [CODE OF CRIMINAL PROCEDURE] art. 539(a) (Neth.).

[30] Memorie van Toelichting Wet Computercriminaliteit III [Explanatory Memorandum Computer Crime III Act] Dec. 28, 2015 (Neth.) 45 [hereinafter *Neth. Explanatory Memorandum*].

[31] *See also* Maillart, *supra* note 7, at 382; Maziar Jamnejad & Michael Wood, *The Principle of Non-intervention*, 22 LEIDEN J. INT'L L. 345, 372 (2009) (footnotes omitted)

> The exercise of enforcement jurisdiction in the territory of another state, without its consent, breaches the non-intervention principle . . . Examples of prohibited extraterritorial enforcement jurisdiction include the collecting of evidence and police and other investigations (even if not purporting to use powers of compulsion) conducted without the consent of the territorial state.

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

Parties—empowers States to search and seize stored computer data, but explicitly limits this power to States' territory.[32] Admittedly, Article 32(b) of the same Convention on Cybercrime allows States Parties to "access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."[33] However, it is not clear whose consent precisely has to be obtained under this article. It is unlikely to be the service provider, as the provider may not have the lawful authority to disclose the data. More likely, consent has to be obtained from the suspect himself—consent which, for obvious reasons, he is unlikely to give.[34] Accordingly, Article 32(b) of the Convention on Cybercrime does not provide a legal basis for extraterritorial network searches.[35] Moreover, the provision is only workable in case the location of the data is known; it does not provide a solution in case of loss of knowledge of location.

Multilateral arrangements governing direct remote access are not expected in the short term. While an additional Protocol to the Budapest Convention is currently under negotiation, its draft provisions only strengthen mutual legal assistance procedures, while making limited allowance for extraterritorial production orders.[36] The draft text remains silent on direct remote access.

Nevertheless, it has been argued that remote network searches are, or should be authorized under international law, at least under certain circumstances. Various arguments have been advanced in this respect. The most extreme argument is that such searches are not extraterritorial in the first place, because the law-enforcement agencies carrying out the search remain in their own territory.[37] This argument is not overly convincing, as the search itself clearly takes place abroad. An arguably more common trope acknowledges that remote searches have an extraterritorial dimension, but that they can be justified on the basis of principles and doctrines of prescriptive jurisdiction. Thus, the Dutch Government explicitly bases investigative enforcement jurisdiction in cyberspace on prescriptive jurisdiction, and relies on the territorial ubiquity principle to justify enforcement jurisdiction.[38] On this view, extraterritorial enforcement jurisdiction over data stored abroad is parasitic on the existence of lawful prescriptive jurisdiction. A variation is that extraterritorial enforcement is allowed insofar as the suspect resides on the territory of the enforcing State or holds its nationality.[39] Also such a view takes its cue from the law of prescriptive jurisdiction. Indeed, as Jan Spoenle points out, "[t]hese references to the traditional territorial and active personality principles of general criminal jurisdiction might prove useful in reaching a consensus on establishing such a measure."[40] A final view has it that enforcement is allowed if the search pertains to serious crime which has a major effect on the State carrying out the search,

[32]Budapest Convention on Cybercrime, *supra* note 10, at art. 19(1) (emphasis added)

> Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: (a) computer system or part of it and computer data stored therein; and (b) a computer-data storage medium in which computer data may be stored *in its territory*.

[33]*Id.* at art. 32(b).

[34]Hörnle, *supra* note 7, at 223 ("Article 32(b)'s remit is limited, it does not apply to coercive, non-voluntary measures and does not overcome the fact that in many situations it will be unlawful for service providers to disclose data to law enforcement.").

[35]Budapest Convention on Cybercrime, *supra* note 9, at art. 32(b).

[36]*See infra* Part C.

[37]Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 Stan. L. Rev. Online 58, 66 (2017).

[38]*Neth. Explanatory Memorandum*, *supra* note 30, at 43, 49.

[39]*E.g.*, Jan-Jaap Oerlemans, *Jurisdictie en Grensoverschrijdende Digitale Opsporing* [*Jurisdiction and Cross-Border Digital Investigation*], *in* Monografieën recht en informatietechnologie [Monographies and Information Technology] 224 (Bert-Jaap Koops & Jan-Jaap Oerlemans eds., 2019) (Neth.).

[40]Jan Spoenle, *Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?*, Council Eur. Project on Cybercrime 11, n. 26 (Aug. 31, 2010), https://rm.coe.int/16802fa3df.

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

or to offenses that are internationally considered as particularly grave.[41] Such a view appears to draw on the effects doctrine and the universality principle under the law of prescriptive jurisdiction.

Where advocates of extraterritorial enforcement jurisdiction do not directly rely on permissive principles of prescriptive jurisdiction, they may instead rely, albeit implicitly, on the concept of jurisdictional reasonableness, which was also developed in the law of prescriptive jurisdiction as a tool of restraint to manage overlapping claims of prescriptive jurisdiction.[42] Reasonableness operates on the basis of a weighting of connections and interests of the various States potentially involved in the matter. Under this rubric, we may find a variety of arguments. For one, it can be considered reasonable for States to carry out remote searches in case of loss of (knowledge of) location.[43] Indeed, when the foreign State is not even aware that the data is located on its territory, it cannot be said to have a strong interest in opposing such searches—although it may be a good practice to seek its consent once the location is identified.[44] For another, it may be reasonable for a State to exercise enforcement jurisdiction where the enforcing State has validly obtained a user's login credentials, for example through user consent, or via wiretapping,[45] and this user is based in the territory, such as in the abovementioned *Tidal* decisions of the Norwegian Supreme Court.

Most commonly, advocates formulate a number of factors that serve as elements of an overall reasonableness-based interest-balancing test that ultimately informs decisions on extraterritorial enforcement. For instance, the explanatory memorandum accompanying the Dutch Act authorizing extraterritorial network searches lists as criteria

> The effort which is required to ascertain the identity and location of an automated network, the gravity of the criminal act, the involvement of the Dutch legal order (involvement of Dutch victims or Dutch infrastructure), the nature of the investigative acts—whether data is only copied or also made inaccessible, and the risk for the automated network.[46]

The territorial location of data, devices or networks is only one element of this test, and not the decisive one. Accordingly, this shift to reasonableness, and more generally the importation of notions belonging to the law of prescriptive jurisdiction, has the effect of drastically reducing the importance of strict territoriality as the linchpin of the law of enforcement jurisdiction. Territory is replaced by such flexible notions as effects, connections, and interests.

Nevertheless, donning the lens of a positivist lawyer, one would be hard-pressed to conclude that customary international law already allows for extraterritorial network searches.[47] Actual State practice remains limited after all. Moreover, it is not always publicly admitted, which disqualifies it as relevant practice for the formation of customary international law. At the same

[41] *Neth. Explanatory Memorandum*, *supra* note 30, at 46.

[42] See Restatement (Third) of Foreign Rels. L. U.S. § 403 (Am. L. Inst. 2018); Restatement (Fourth) of Foreign Rels. L. U.S § 405 (Am. L. Inst. 2022), for an overview of why it is not entirely clear whether reasonableness rises to the level of a customary international law. As I have argued, elsewhere, however, it may be a general principle of international law, or at least derive from general principles, see Cedric Ryngaert, Jurisdiction in International Law 145–89 (Cedric Ryngaert ed., 2nd ed. 2015).

[43] Bert-Jaap Koops & Morag Goodwin, Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law 76 (2015).

[44] Oerlemans, *supra* note 39, at 225.

[45] *Id.* at 224. *See also* Spoenle, *supra* note 40, at 11 (allowing direct access provided that such "access can be established by the sole usage of proper authenticating credentials," "those very credentials have to belong to or be used by a suspect," and "the credentials have to be obtained in a lawful manner"). *See also* Schmitt, *supra* note 8, at 70, (emphasis added) (explaining that law-enforcement agency obtaining, "under false pretenses, the log-on credentials to a closed online forum hosted on servers located abroad, but meant to be accessible to one or more users from the State" exercises *territorial* enforcement jurisdiction).

[46] *Neth. Explanatory Memorandum*, *supra* note 30, at 48 (author's own translation). Also in *Tidal*, *supra* note 14, ¶¶ 65–71 (The Norwegian Supreme Court's conclusion that "the search will [not] affect another state to an extent that it constitutes a violation of the principle of sovereignty" was based on a multi-factor test).

[47] *Tidal*, *supra* note 14, at ¶ 58 (observing that "no custom under international law exists in this area").

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

time, (public) foreign protest against such searches is few and far between.[48] Quite possibly, States prefer not to have their hands tied: Today's gamekeepers may become tomorrow's poachers. Accordingly, the practice of extraterritorial network searches is likely to remain in international legal limbo for some time. Nonetheless, this absence of legal certainty is unlikely to deter proactive States from taking measures to prevent the Internet from becoming a safe haven for criminals.[49]

C. Indirect Access—Production Orders

Apart from using direct means to access data held abroad, States also use means of indirect access. States can acquire indirect access to data by ordering Internet intermediaries to produce user data located abroad, for example the subscriber, traffic or content data relating to an email account stored on a foreign server,[50] possibly backed up with subpoena threats.[51] These Internet intermediaries may be incorporated in the territory, may have a representative there, or simply offer services to users based there.

Also, such production orders appear to be in tension with the prohibition of extraterritorial enforcement jurisdiction, as they bypass the consent of the territorial State. From the perspective of the territorial State, it may not matter much whether the data is directly or indirectly accessed by a foreign State. In both instances, the foreign State appears to carry out investigative measures on another State's territory.

Still, as such production orders are perceived to not directly intrude on a server abroad, there appears to be substantial international willingness to legally support them, at least within certain bounds. Under the US CLOUD Act, US law-enforcement agencies can now order -US-based Internet intermediaries to disclose information within their possession or control, regardless of location.[52] Other States, notably Belgium, have gone even further, and have ordered foreign-based Internet intermediaries to produce data to be used as evidence in domestic criminal investigations.[53] The European Union is currently mulling its own version of the CLOUD Act, on the basis of a Commission proposal of 2018.[54] Under the Commission's proposal, judicial authorities in one

[48]*Id.* at ¶ 59 (observing that "there is no information on inter-state reactions to a country's authorities accessing data stored in another state through coercive measures against legal entities in its own territory").

[49]*See Neth. Explanatory Memorandum, supra* note 30, at 50 ("Awaiting the further development of the international legal framework for the exercise of jurisdiction in combating computer crime, one will have to operate independently, to prevent that the Internet because a safe haven for crime.").

[50]*See* Maillart, *supra* note 7, at 380, for a discussion of why law-enforcement agencies are mainly interested in metadata (subscriber and traffic data) held by Internet intermediaries. These data may enable the agencies to locate the criminals. Obtaining them may be key to the success of a criminal investigation and prosecution.

[51]Insofar as an Internet intermediary has no presence or assets in the relevant State, such threats may lack credibility. Only the nuclear option of "market destruction" remains, for example barring the intermediary from offering services to users in the territory. As this option denies services to innocent users, open societies are unlikely to use it. *But see* Reuters, *Russian MPs Backs Bills Enabling Moscow to Block US Social Media*, GUARDIAN (Dec. 23, 2020, 6:47 AM), https://www.theguardian.com/world/2020/dec/23/russian-parliament-backs-bills-enabling-moscow-to-block-us-social-media, for a recent market destruction bill.

[52]CLOUD Act, H.R. 4943, 115th Cong. § 103(a)(1) (2018); *see* 18 U.S.C. § 2713 (2018)

> A [provider] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

See also United States v. Microsoft Corp., 138 S.Ct. 1186, 1188 (2018) (per curiam), *vacated as moot*, per introduction of the CLOUD Act.

[53]*See* Paul de Hert, Cihan Parlar & Johannes Thumfart, *Legal Arguments Used in Courts Regarding Territoriality and Cross-border Production Orders: From Yahoo Belgium to Microsoft Ireland*, 9 NEW J. EUR. CRIM. L. 326, (2018), for a discussion of the Belgian cases.

[54]*E. Com. Explanatory Memorandum*, *supra* note 20. *See* Council Directive 2014/41/EU, 2014 O.J. (L 130) 1 (EU), regarding the European Investigation Order (EIO) in criminal matters, but this Directive does not specifically focus on digital evidence. Stanislaw Tosza, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the*

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

EU Member State would be allowed to request (meta-)data from Internet intermediaries, including non-EU-based intermediaries which offer services in the -EU-, regardless of data location.[55]

In the meantime, the Cybercrime Convention Committee has prepared a Second Additional Protocol to the Budapest Convention on Cybercrime, opened for signature in May 2022, which authorizes extraterritorial production orders pertaining to subscriber information.[56] This Additional Protocol could further clarify the scope of Article 18(1)(b) of the Budapest Convention, which provides that "[e]ach Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control."[57] The Cybercrime Convention Committee espoused a wide reading of this provision, and posited that it allowed extraterritorial production orders in relation to subscriber information stored abroad and controlled by foreign service providers, as far as those providers offer services in the territory.[58] However, as a Second Additional Protocol addressing—*inter alia*—extraterritorial production orders was considered necessary, it is more likely that for some Contracting Parties the liberal interpretation of Article 18(1)(b) of the Budapest Convention was a bridge too far, even in respect of providers offering services in the territory.[59] Julia Hörnle has observed in this respect that Article 18 only creates a power under the domestic criminal procedures of Contracting Parties to the Convention, and "does not force the receiving state to cede sovereignty to the investigating state," which is under "no obligation to recognize or enforce the request outside MLA."[60]

The arguments proffered in favor of the international lawfulness of extraterritorial production orders somewhat mirror the arguments in favor of direct access. In perhaps a slightly more convincing manner, it has been submitted that orders for the production of foreign data are not truly extraterritorial insofar as they are directed at providers over which States have territorial or personal jurisdiction anyway.[61] Such an argument is in fact a replay of an older US argument

European Investigation Order and the European Production Order, 11 NEW J. EUR. CRIM. L. 161 (2020) (discussing the relationship between the EIO and the envisaged European production order). See Carrera et al., *supra* note 20, at 67–68, for an argument in favor of using the EIO rather than the European production order in relation to digital evidence, on the grounds that the former provides better effective remedies.

[55]*See E. Com. Explanatory Memorandum*, *supra* note 19, at art. 1.1 ("This Regulation lays down the rules under which an authority of 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."). Little progress has recently been made on this proposal, however, raising concerns over whether an EU regulation on European production orders will ever be adopted. There are also issues with the interoperability of the European production order and the 2nd Additional Protocol to the Budapest Convention, discussed in the next paragraph above. *See also* Carrera et al., *supra* note 20, at 36–44.

[56]Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, COUNCIL EUR. TREATY SERIES art. 7.1, (May 12, 2022), https://rm.coe.int/1680a49dab,

> Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

[57]Budapest Convention on Cybercrime, *supra* note 9, at art. 18(1)(b).

[58]Cybercrime Convention Committee, *T-CY- Guidance Note #10: Production orders for subscriber information (Article 18 Budapest Convention)*, COUNCIL EUR. (2017), https://rm.coe.int/16806f943e.

[59]*See* Borka Jerman Blažič & Tomaž Klobučar, *Removing the Barriers in Cross-border Crime Investigation by Gathering E-evidence in an Interconnected Society*, 29 INFO. & COMMC'NS TECH. L. 66, 69–70 (2020) (critiquing the T-CY- in this respect). *See also Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, *supra* note 56, at art. 7.1; Budapest Convention on Cybercrime, *supra* note 9, at art. 18(1)(b).

[60]HÖRNLE, *supra* note 7, at 205 (explaining art. 18(1)(b) of the Budapest Convention on Cybercrime as "the important distinction to instruments such as the executive agreements envisaged in the US CLOUD Act or the European E-Evidence Proposal").

[61]In re Warrant to Search a Certain E-mail Acct. Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

that discovery orders compelling US-based persons to produce documents they held abroad do not amount to an exercise of extraterritorial enforcement jurisdiction, but are simply territorial in nature.[62] Somewhat similarly, the Belgian Court of Cassation ruled that ordering a provider (Skype) to produce data located abroad or to perform a wiretap does not amount to an intervention of Belgian law-enforcement authorities abroad, as this only implies a duty of cooperation on the part of the provider.[63] A related, but also different argument is that, while production orders may have an extraterritorial dimension, such orders may be justified insofar as their addressees offer services on the territory of the issuing State, and thus participate in economic activities there.[64] The logic at play here is that, where a State has prescriptive jurisdiction over the activities of Internet intermediaries offering services to users on its territory,[65] it has ancillary enforcement jurisdiction over data controlled by these intermediaries, regardless of location.[66] Such an argument again conceives of enforcement jurisdiction as following prescriptive jurisdiction, in particular the effects doctrine. This comes with a twist, however, as the enforcement action does not normally assist criminal proceedings brought against the intermediary itself, but rather against an individual user, or suspect.

Admittedly, advocates of collapsing the distinction between prescription and enforcement are cognizant of the danger of jurisdictional overreach resulting from the application of the effects doctrine to the law of enforcement jurisdiction. Acknowledgement of this danger does not lead them to abandon extraterritorial production orders altogether, but rather to favor the adoption of mitigating principles or safeguards.[67] Adoption of such principles serves the purpose of legitimating the extraterritorial claim. Strikingly, these principles also draw on the law of prescriptive jurisdiction, in particular the notions of genuine connection[68] and reasonableness.

[62]*See* In re Grand Jury Subpoena Directed to Marc Rich & Co., 707 F.2d 663, 668–69 (2d Cir. 1983). *See* Cedric Ryngaert, *Conflicts of Jurisdiction over Orders to Produce Documents Located Abroad: Reappraising "Conflict of International Jurisdiction: Ordering the Production of Documents in Violation of the Law of the Situs,"* 48 BELG. REV. INT'L L. 423 (2015), for a discussion of this argument notably.

[63]Cour de Cassation [Cass.] [Court of Cassation], Feb. 19, 2019, AR P.17.1229.N, ¶¶ 9–10 (Skype Communications) (Belg.), https://juportal.be/content/ECLI:BE:CASS:2019:CONC.20190219.1/NL. *See also* Hof Van beroep Antwerpen [HvB] [Court of Appeals], Nov. 15, 2017, AR 2016/CO/1006 (Belg.).

[64]*Id.* at ¶ 9.

[65]These days, this is rather non-controversial. *See generally* CJEU, C-131/12, *Google Spain v. Agencia Española de Protección de* Datos, EU:C:2014:317 (applying EU law to the services offered by Google in the EU), http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

[66]*Cf.* Paul Schiff Berman, *Legal Jurisdiction and the Deterritorialization of Data*, 71 VAND. L. REV. 11, 26 (2018) ("[T]hose companies are purposely affiliating themselves with the foreign markets, and regulation by those communities is potentially justifiable.").

[67]For a discussion on the need for limitations and safeguards, *see generally id.* at 27 (suggesting an number of factors to "temper the potential problems associated with jurisdiction based only on effects;" Jennifer Daskal & DeBrae Kennedy-Mayo, *Budapest Convention: What is it and How is it Being Updated?*, CROSS-BORDER DATA FORUM (July 2, 2020) (footnotes omitted), https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

> States and many outside observers are—rightly so—worried about a law enforcement free-for-all, pursuant to which any government actor anywhere can simply compel production of data anywhere under domestic authority alone. This raises a fear of governments seeking access to data in order to harass and abuse, rather than investigate legitimate and properly-predicated crime. These are critical considerations to take into account—although the risks can and should be mitigated by the application of and insistence on baseline procedural and substantive rules.

See also Cass., AR P.17.1229.N, ¶¶ 9–10 (Skype Communications) (illustrating an understanding the desire to address crime, but calling for the application of mitigation principles derived from international human rights law).

[68]Pursuant to the genuine connection requirement, States can only exercise jurisdiction if they have a sufficiently strong connection with the subject of regulation. The genuine connection requirement has recently gained more prominence, *see* RESTATEMENT (FOURTH) OF FOREIGN RELS. L. U.S. § 407 (AM. L. INST. 2022) (suggesting it as the overarching customary international law requirement for any exercise of prescriptive jurisdiction to be lawful).

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

Just like in the context of restraints on direct access, these notions may take different forms. Most obviously, States may require that the issuing State notify the State where the data sought is located, or where the intermediary is incorporated.[69] That said, more elaborate mitigation mechanisms can certainly be envisaged. The European Commission's proposal for the Regulation for a European Production Order (EPO) offers a good illustration.[70] First, the scope *ratione personae* of the proposal is explicitly limited to providers offering services in the EU which have "a substantial connection to the Member State(s)."[71] Second, under the proposal, EPOs for the production of transactional or content data can only be issued for more serious criminal offenses—whereas orders for the production of subscriber and access data can be issued for all offenses.[72] Third, the EPO proposal features detailed, comity-based provisions on a review procedure where "compliance with the -EPO- would conflict with applicable laws of a third country prohibiting disclosure of the data concerned."[73] Most striking is the multifactor weighting test which a competent EU-based court is required to apply in case of conflicting obligations based on considerations other than fundamental rights or fundamental interests of a third country.[74] When determining whether to uphold or withdraw the EPO, the court is called on to pay heed to such factors as the third country's interest, the degree of connection to the relevant States, and the seriousness of the offence.[75] Such a multi-factor test, weighting multiple interests and connections, is a classic reasonableness test aimed at managing overlapping prescriptive jurisdiction and conflicting legal requirements.[76] In the field of enforcement jurisdiction, such a test prevents that extraterritorial production orders unduly encroach on third States' sovereignty and catch providers between a rock and hard place. At the same time, and most importantly, this mechanism of restraint also serves to justify the extraterritoriality of specific production orders.

As demonstrated by recent evolutions in the US, the EU and in the context of the Budapest Convention, there is an international dynamic at play in favor of more liberal rules for extraterritorial production orders, even if hemmed in by a number of jurisdictional restraints. However, this dynamic is far from uncontested. For one thing, the EU Commission proposal has not yet been adopted. In fact, rather drastic amendments have recently been proposed by the European Parliament.[77] For another, the Second Additional Protocol to the Budapest Convention is unlikely to command the support of all States Parties to the Budapest Convention,[78] given the wide

[69]On a duty of notification notably, *see* Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Coperation and Disclosure of Electronic Evidence*, Council Eur. Treaty Series art. 4, (May 12, 2022), https://rm.coe.int/1680a49dab (providing for *optional* notification).

[70]*E. Com. Explanatory Memorandum*, *supra* note 19.

[71]*Id.* at art. 2.4 (emphasis added).

[72]*Id.* at art. 5.4 (limiting the issuance of European production orders to criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years, or for specific cyber-dependent, cyber-enabled or terrorism-related crimes). The successful execution of such orders in relation to providers based in third countries may moreover depend on the conclusion of a bilateral agreement with the provider's home country (the US in particular). In particular, CLOUD Act § 105 requires that foreign governments enter into an executive agreement with the US concerning access to (certain) data.

[73]*E. Com. Explanatory Memorandum*, *supra* note 19, at arts. 15–16.

[74]There is no weighting test in case of conflicting obligations based on fundamental rights or fundamental interests of a third country. *See id.* at art. 15.6 (explaining that the competent EU-based court simply lifts the order in case a third country objects to the execution of the EPO on the basis of these grounds).

[75]*Id.* at art. 16.5. For similar factors, see *Criminal Justice Access to Data in the Cloud: Challenges*, Cybercrime Convention Committee (T-CY-), (Council of Europe, Strasbourg, Fr.) May 26, 2015, at 15, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59.

[76]*Cf.* Restatement (Third) of Foreign Rels. L. U.S. § 403(2) (Am. L. Inst. 2018) (listing a number of factors guiding a reasonableness-based-interest-balancing test).

[77]*See* Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Parl. Eur. Doc. A9-0256 (2020).

[78]While the Convention is adopted under the auspices of the Council of Europe, it also counts non-Member States as Contracting Parties: Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, and the United States.

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

divergences between the Contracting Parties. Moreover, the Protocol allows for the imposition of additional conditions as well as the possibility to append a reservation, which may not just mitigate but altogether exclude the compulsory nature of extraterritorial production orders.[79] What is more, even without reservations of their home States, foreign-based addressees of production order have the right not to disclose the relevant data, in which case only mutual legal assistance can be pursued.[80] If voluntary compliance remains the norm internationally,[81] extraterritorial production orders amount to mere requests which can be disregarded without penalty. They hardly qualify as instances of genuine extraterritorial enforcement jurisdiction.

D. Assessing Current Evolutions

The most eye-catching effect of digitalization on the law of enforcement jurisdiction, as follows from the discussion in the previous sections, is the fading into irrelevance of territoriality. Territoriality has been the bedrock principle of the law of jurisdiction, at least since the Peace of Westphalia. In respect of digital data, however, enforcement jurisdiction no longer follows the geographic location of the evidence sought. The Proposal for a European Production Order cannot be more clear in this respect, where it states that "the data storage location by itself does not suffice in establishing a substantial degree of connection."[82] In cyberspace, the territorial location of data at a given time is simply a function of algorithmic decisions of Internet intermediaries offering global cloud computing services. In order to retain their relevance, jurisdictional rules may have to bend to technological realities.[83] From a criminal law perspective, maintaining strict territoriality would encourage providers to store data on servers in "safe havens," a clearly undesirable outcome.[84] In some circumstances, moreover, the exact location of data may even be unknown, which renders reliance on territoriality a non-starter to begin with.[85] Insofar as the "physical" location of digital data—on a server—may be entirely fortuitous, and may in fact not be known by the territorial State, that State cannot reasonably invoke its territorial sovereignty as a shield against another State's jurisdictional claims over such data.

Accordingly, normatively speaking, the better option may be to accept the principled international lawfulness of "extraterritorial" enforcement jurisdiction over digital data, possibly by redefining it as a form of extraterritorial "investigative" jurisdiction in cyberspace.[86] This would leave intact the traditional prohibition of extraterritorial enforcement jurisdiction in the non-cyber domain, where territorial boundaries are still very much in existence. In the physical realm, there is in any event no indication of State practice and *opinio juris* in favor of a relaxation of the prohibition. That said, there may be one exception: in the case of human and drugs trafficking on the high seas, we see that some states exercise enforcement jurisdiction over vessels in apparent excess of what is allowed under the UN Convention on the Law of the Sea, a practice which may in

[79]See *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, *supra* note 56, at arts. 7(5)–(6), on additional notifications, instructions and supplementary information to be provided. See *id.* at art 7(9) on full or partial reservations to Article 7.

[80]*Id.* at art. 7(7). While this is framed as an exception, it risks rendering compliance with production orders merely voluntary and thus suboptimal.

[81]*See also* SCHMITT, *supra* note 8, at 70 ("[T]he private entities involved have no legal obligation to comply with such requests.").

[82]*E. Com. Explanatory Memorandum*, *supra* note 19, at art. 16.5(c).

[83]*See also* Berman, *supra* note 66, at 23–24 (submitting that "if jurisdictional rules do not map well onto the reality of human activity, it's a sign that jurisdictional rules need to change, not that we need to squelch or limit that human activity").

[84]Kleijssen & Perri, *supra* note 2, at 158.

[85]Spoenle, *supra* note 40, at 5.

[86]DAN JERKER B. SVANTESSON, SOLVING THE INTERNET JURISDICTION PUZZLE 159–71 (1st ed., 2017).

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

due course lead to the crystallization of a new permissive customary norm.[87] However, given the physical characteristics of the oceans, enforcement jurisdiction at sea has always been subject to a regime different from the general regime governing enforcement jurisdiction on land.

In order to adequately tackle crime in the Internet era, States should be granted more leeway to exercise enforcement—or investigative—jurisdiction over data, regardless of data location. However, to prevent a jurisdictional free-for-all, it is key that that the exercise of extraterritorial enforcement jurisdiction in cyberspace becomes subject to a stringent test weighting all relevant connections and interests in concrete cases. Introducing such a weighting test means that extraterritorial enforcement jurisdiction is no longer governed by binary rules (allowed or not allowed), but becomes a matter of degree, requiring a granular, contextual assessment. What may be acceptable in some circumstances, may be unacceptable in other circumstances.

Such flexibility has long been a characteristic of the law of prescriptive jurisdiction, where lawfulness is assessed *in concreto* by making use of such malleable concepts as effects, ubiquity, genuine connection, and reasonableness. It appears that these notions are now migrating to the law of enforcement jurisdiction in cyberspace. Thus, digitization is blurring the lines between the rigid law of enforcement jurisdiction and the more flexible law of prescriptive jurisdiction. Critics may perhaps object that such a "post-modern," case-by-case approach may lack predictability and legal certainty. However, this approach is hardly novel. It has not only been applied for quite some time in the law of prescriptive jurisdiction, but has an even longer pedigree in the conflict of laws—private international law. Especially in the -US-, the flexible notion of comity has been instrumental in solving disputes with cross-border elements.[88]

Nevertheless, this flexible attitude towards extraterritorial enforcement jurisdiction is not universally shared. There is no denying that relevant State practice and expert opinion in favor of the "un-territoriality of data" has a particular Western slant. Moreover, even within the West, contestation continues, as testified by the very limited public State practice in support of direct access, as well as the vicissitudes of the -EPO- and the Second Additional Protocol to the Budapest Convention.[89] Such contestation may largely pertain to the boundary conditions for the valid exercise of extraterritorial enforcement jurisdiction, but given the close link of these conditions with the principled lawfulness of such jurisdiction, it can hardly be discounted.

States which jealously guard their sovereignty and see an open Internet as a threat rather than a blessing will probably continue to treat digital evidence as any other piece of evidence and subject it to territorial jurisdiction. Such States may require that Internet intermediaries store data within their territory ("data localization"), thereby obviating the need for extraterritorial access. These States are not standing idly by, for that matter. Russia has recently circulated a proposal for a Draft United Nations Convention on Cooperation in Combating Information Crimes, which conspicuously does not provide for extraterritorial production orders.[90] While this proposal has not yet gained a lot of traction within the UN, the challenge to the Western approach to

[87]Cedric Ryngaert, *Enforcement Jurisdiction in A-Territorial Spaces: Addressing Crime on the High Seas and in Cyberspace*, *in* Transformations in Criminal Jurisdiction: Extraterritoriality and Enforcement (Michéal Ó Floinn, Lindsay Farmer, Julia Hörnle, & David Ormerod KC eds., forthcoming Aug. 2023).

[88]Berman, *supra* note 66, at 23 (stating that "one of the important lessons of conflict of laws, it seems to me, is that there is no single unifying grand theory that can provide an authoritative answer to every possible dilemma or account for the infinite variety of human activity that may arise," and on that basis offering a number of provisional principles on extraterritorial enforcement regarding data, which echo the principles discussed earlier in this contribution). *See also* William S. Dodge, *International Comity in Comparative Perspective*, *in* The Oxford Handbook of Comparative Foreign Relations Law 701 (Curtis A. Bradley ed., 2018), for discussion on comity.

[89]*See E. Com. Explanatory Memorandum, supra* note 19; Second Protocol, *supra* note 56.

[90]See *Draft United Nations Convention on Cooperation in Combating Information Crimes*, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021._E.pdf.

https://doi.org/10.1017/glj.2023.24 Published online by Cambridge University Press

law-enforcement in cyberspace, and more generally the conceptualization of cyberspace as an open space, is unmistakable.[91]

In light of these diverging approaches, universal customary international law regarding such orders is unlikely to crystallize. More likely is the crystallization of customary norms of regional scope, comprising (Western-oriented) liberal democracies with an open Internet. In parallel, such States may mutually adopt bilateral treaties in which they reciprocally recognize the validity of extraterritorial production orders, subject to the necessary safeguards.[92]

Competing Interests. The author declares none.

Funding Statement. No specific funding has been declared in relation to this article.

[91]*See* Allison Peters, *Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime*, FOREIGN POL'Y, https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/ (Sept. 16, 2019, 4:29 PM).

[92]Marcin Rojszczak, *CLOUD Act Agreements From an EU Perspective*, 38 COMPUT. L. & SEC. REV. 1 (2020); *See* HÖRNLE, *supra* note 7, at 219, for a plea in favor of including fundamental rights-informed safeguards.

Cite this article: Ryngaert C (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal* **24**, 537–550. https://doi.org/10.1017/glj.2023.24