Chapter 16: Enforcing Criminal Jurisdiction in the Clouds and International Law's Enduring Commitment to Territoriality

Stephen Allen

Published in Stephen Allen, Daniel Costelloe, Malgosia Fitzmaurice, Paul Gragl, and Edward Guntrip (eds.) *The Oxford Handbook of Jurisdiction in International Law* (OUP, 15 Sept 2019)

Abstract

As a result of the phenomenon of Cloud computing data is now often stored in data-centres, which may be located in a different jurisdiction to the one in which the data owner/possessor (or service provider) is based. The issue of cross-border data storage has become a major problem for criminal justice authorities around the globe because, in general, the officials of one State cannot search, unilaterally, for data located within another State's territory, with a view to accessing and retrieving it. This prohibition constitutes a specific manifestation of international law's long-standing requirement that a State cannot enforce its jurisdiction in the territory of another State, in the absence of consent. Nevertheless, the dramatic growth in trans-border criminality has meant that this territorial limitation now risks undermining the extent to which individual States are able to satisfy their positive obligations to maintain the integrity of their criminal justice systems and to uphold the rule of law more generally. The Cybercrime Committee, which is responsible for monitoring the 2001 Cybercrime (Budapest) Convention, and individual States have tried to overcome the difficulties associated with unilateral trans-border activity in the criminal context. This chapter examines the Committee's key proposals in this area insofar as jurisdictional considerations are engaged. In addition, the chapter focuses on the Belgian Supreme Court's decision in the *Yahoo! Case*; and the *Microsoft Warrant Case*, which was being considered by the US Supreme Court before Congress enacted the CLOUD Act. These cases have prompted judges and lawyers to contemplate the jurisdictional implications of cross-border criminality for the investigation (and prosecution) of criminal offences and the way in which municipal legal systems and international law interact in concrete situations. Consequently, these sites of action have considerably explanatory resonance irrespective of the manner in which they were dealt with by the courts and legislatures involved.

1. Introduction

There has been a startling increase in the volume of electronic data, stored on connected computer networks in recent years. This data may constitute evidence in connection with the investigation, and prosecution of, criminal offences within national legal systems. Due to the phenomenon of Cloud Computing, data is now often stored in data-centres, which may be located in a different jurisdiction to the one in which the data owner (or possessor) is based. The issue of cross-border data storage has become a major problem for criminal justice authorities because, in general, the officials of one State cannot search, unilaterally, for data located within another State's territory, with a view to accessing and retrieving it. This prohibition constitutes a specific manifestation of international law's long-standing requirement that a State cannot enforce its jurisdiction in the territory of another State, in the absence of consent.[1] Nevertheless, the dramatic growth in trans-border criminality has meant that this territorial limitation now risks undermining the extent to which individual States are able to satisfy their positive obligations to maintain the integrity of their criminal justice systems and to uphold the rule of law more generally.

At this point, it may be useful to demonstrate the difficulties presented by the Cloud Computing model in the present context through a series of hypothetical examples. In the first scenario an individual, who resides in State A, has an email account which allows her to store data on a service provider's Cloud network. However, for operational reasons, her uploaded data is stored in a data-centre located in State B. If the data owner engages in activity in State A in violation of its criminal law – and the activity generates incriminating data which is retained in State B – can the officials of State A (acting unilaterally and from within that State's territory), access the data stored in State B and retrieve it for the purpose of their investigations? In a second scenario, would the position be any different if the data owner in question is based in State B instead (assuming the service provider is registered in State A in both scenarios)? And, in a final scenario, if State A's officials understand that the sought-after data is stored in a data-centre situated in an extra-territorial setting, but they do not know its exact whereabouts, can they undertake a unilateral remote search for the

[1] See the S.S. *Lotus Case* (1927), Judgment No 9, PCIJ, Series A, No 10, 18. The International Law Commission has specifically drawn attention to the unlawfulness of public officials conducting criminal investigations in another State's territory: the *Report of the International Law Commission* (2006), Annex V, para 22, 526.

data through the service provider's Cloud network (again assuming that it is registered in State A)?

The possible answers to each of these scenarios will depend on a range of factors which involve materially different conceptions of the exercise of enforcement jurisdiction and, in particular, how the notions of territoriality and extra-territoriality may be interpreted in specific situations. Will the investigating State be acting within its own jurisdiction if its officials compel an individual, present in its territory, to hand over data which is stored in a third State, or does this exercise of public authority amount to an instance of extra-territorial enforcement jurisdiction? Alternatively, if the officials of the investigating State demand that a service provider (established in its territory) turn over data belonging to an individual who lives in a third State – with the data in question being stored on a server in that State – does this amount to a lawful exercise of territorial enforcement jurisdiction or to an unlawful instance of extra-territorial jurisdiction by the investigating State? And, finally, if the geographical location of the sought-after data remains unknown, how can the orthodox approach to enforcement jurisdiction retain any value for regulatory purposes? This essay explores these issues.

The Cybercrime Committee, which is responsible for monitoring the Council of Europe's 2001 Cybercrime (Budapest) Convention,[2] and individual States have tried to overcome the difficulties associated with unilateral trans-border activity in the criminal context. Nevertheless, this essay argues that they have consistently under-estimated international law's enduring commitment to a territorial conception of enforcement jurisdiction. In particular, their reform proposals have not paid enough attention to jurisprudential developments in the fields of extra-territorial jurisdiction and State responsibility and their failure to appreciate the applicable international legal doctrine has, potentially, serious consequences for the international legal order in general. Against this background, the essay examines the key proposals which have been advanced by the Cybercrime Committee in order to illustrate the ways in which the Committee has sought to address the challenges of unilateral trans-border activity in connection with the conduct of criminal investigations and to consider their viability from an international legal perspective, insofar as jurisdictional considerations are

[2] The Council of Europe's Cybercrime (Budapest) Convention (2001) CETS 185, has been ratified by 55 States.

engaged. In taking such an approach, I am not trying to advocate in favour of the status quo. Clearly, international law needs to find ways of responding to the borderless character of criminal activity in the digital age, but such an ambitious objective is beyond the scope of this chapter. Instead, this essay seeks to draw attention to the consequences, for States and the inter-State system, of certain choices which are currently being mooted at the global level. To this end, in addition to considering the proposals developed by the Cybercrime Committee, this essay pays particular attention to two significant cases – the Belgian Supreme Court's 2015 decision in the *Yahoo! Case*;[3] and the *Microsoft Warrant Case*, which was being considered by the US Supreme Court when Congress intervened by enacting the 'CLOUD' Act 2018.[4] These cases have prompted judges and lawyers to contemplate the jurisdictional implications of cross-border criminality for the investigation, and prosecution, of criminal offences and the way in which municipal legal systems and international law interact in such situations. Consequently, it is clear that these sites of action have considerably explanatory resonance irrespective of the manner in which they were dealt with by the courts and legislatures involved. They will, therefore, by treated more in the way of 'thought experiments' than compelling precedents for the present purposes.

2. Cyberspace and Territorial Jurisdiction

As noted above, a State cannot enforce its jurisdiction within the territory of another State without its consent.[5] The traditional approach to enforcement jurisdiction is underpinned by the principles of territoriality, non-intervention, and State consent,[6] and it represents a clear manifestation of sovereign authority.[7] But despite the strength of the orthodox position, in recent times, institutional actors have made a concerted effort to overcome the practical difficulties that Cloud Computing, and the internet more

[3] The *Yahoo! Judgment*, Belgian Court of Cassation, 1 December 2015, Case No P13.2082.N/1.
[4] *United States v Microsoft Corp* (the *Microsoft Warrant Case*), Case No 17-2 (2018). The Clarifying Lawful Overseas Use of Data (CLOUD) Act was enacted on 23 March 2018. See the Supreme Court's judgment, 17 April 2018: <https://www.supremecourt.gov/docket/docketfiles/html/public/17-2.html> accessed 12 September 2018.
[5] This classical position was fully endorsed in the Lotus Judgment, n 1, 18 and 19.
[6] See *the Island of Palmas Case* (1928) 2 RIAA 829. Regarding the principle of non-intervention, see Article 2(7) of the UN Charter and the Declaration on the Principles of International Law concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, UN General Assembly Resolution 2625(XXV), 24 October 1970.
[7] See James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th edn, 2012), 456 and 479.

generally, present for the exercise of State jurisdiction in ways that are, seemingly, in conformity with international law. Many of these attempts at reform focus on the regulatory challenges which flow from the ubiquitous effects of online activity and the sheer scale of conduct which the technological gains of recent years have facilitated.[8] As a result, many of the leading scholars have been preoccupied with the prescriptive component of the extra-territorial claims made by States and the often dramatic occasions when their judicial authorities have followed through on them via the exercise of adjudicative jurisdiction. But while the challenges presented by the internet, and the phenomenon of Cloud Computing in particular, have created a novel problem, it is important to appreciate that international law has long maintained a flexible attitude to the exercise of prescriptive jurisdiction and that, by and large, its generous approach to the allocation of jurisdiction has been broadly successful.[9]

To be sure, there are considerable difficulties with the exercise of prescriptive jurisdiction in extra-territorial settings and it is not my intention to minimize them. But it is undeniable that scholars, practitioners and institutional actors have come up with plausible solutions to many of the challenges arising from conflicting and excessive jurisdictional claims. However, there is a stark difference in the way that international law has sought to govern the exercise of enforcement jurisdiction. Indeed, its historical approach has been characterised by a firm commitment to the territoriality principle. While the *Lotus* decision has been the subject of much criticism in recent years,[10] the PCIJ's ruling on the nature and scope of enforcement jurisdiction has been consistently followed down the years without serious debate.[11] When viewed against the backdrop of other core tenets of classical international law – territorial sovereignty, non-intervention and State consent – an inflexible territorial conception of enforcement

[8] See Michael A Geist, 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction' (2001) 16 Berkeley Technology Law Journal 1345; Uta Kohl, *Jurisdiction and the Internet* (Oxford University Press, 2007); Chris Reed, *Making Laws For Cyberspace* (Oxford University Press, 2012); Andrew Murray, 'The Uses and Abuses of Cyberspace: Coming to Grips with the Present Dangers, in Antonio Cassese (ed) *Realizing Utopia: The Future of International Law* (Oxford University Press, 2012), 496. Paul Schiff Berman, *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders* (Cambridge University Press, 2012).

[9] See Bruno Simma and Andreas Müller, 'The Exercise and Limits to Jurisdiction' in James Crawford and Marti Koskennemi (eds), *The Cambridge Companion to International Law* (Cambridge University Press, 2012), 134.

[10] Eg see Alex Mills, 'Rethinking Jurisdiction in International Law' (2014) British Yearbook of International Law 187, 192-194. In addition, the judgment produced a fair amount of controversy when it was delivered. See, eg Hersch Lauterpacht, *The Function of the Law in the International Community* (Cambridge University Press, 1933, 2011 reissue), 102-104.

[11] This has been noted by several scholars in recent years. See Kohl, n 8, at 200; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2015, 2nd edition), 9; and Mills, n 10, 195.

jurisdiction seems to be a good fit, from a systemic perspective. However, the problems associated with online activity and remote data storage, especially in the context of criminality, have prompted institutional actors to reconsider the viability of maintaining a territorial conception of enforcement jurisdiction in digital settings and, especially, in Cloud environments.

Mutual Legal Assistance Treaties (MLATs) represent the traditional way in which States have sought to regulate cases of cross-border criminality.[12] This approach has the distinct advantage of conforming to the consent-based requirements demanded by international law, when enforcement actions are carried out in the territory of another State. However, MLATs have been widely criticised for not being fit for purpose.[13] Specifically, they have been condemned for being un-wielding, slow and inefficient, in sharp contrast to data which can be moved, hidden, changed or deleted instantaneously. In addition, it is apparent that such arrangements are incapable of addressing the so called 'loss of location' problem as they presuppose the existence of established legal processes between identifiable States who have given their consent for this reason.[14] However, it has been widely acknowledged that the territorial model cannot respond to the challenges posed by the sheer volume of cross-border criminality which has been, inadvertently, unleashed by the internet, and by the Cloud Computing model becoming the preferred means of data storage in contemporary computing practice. Indeed, the inability of the orthodox approach to cope with the huge amount of remotely stored data which is relevant to the investigation of criminal offences calls into question the capacity of a State to satisfy its core positive obligation of maintaining the integrity of its criminal justice system, a charge that clearly justifies a thorough re-examination of the value of adhering to a territorial conception of enforcement jurisdiction. In the circumstances, the Cybercrime Committee and other institutional actors have advanced cogent proposals in an effort to find new and innovative ways of moving beyond the traditional approach to

[12] This approach constitutes the principal means of resolving the jurisdictional problems at the level of enforcement in the Budapest Convention. E.g. see Agreement on Mutual Legal Assistance, Between the USA and the European Union, (2003), OJ 34 (2006); and the Treaty Between the USA and Ireland on Mutual Legal Assistance in Criminal Matters, (2001), Treaty Doc No 107-9 (2002).

[13] See Bert-Japp Koops and Morag Goodwin, 'Cyberspace, the Cloud and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law', Tilburg, December 2014, 26-27.

[14] The loss of location problem refers to the great difficulty of establishing the whereabouts of data stored on remote computer networks in many cases for technological reasons. This challenge will be examined in detail in section 4 below. Establishing the location of data is significant because the regulatory system which allocates jurisdiction, and thus authority, is based on territorial determinants.

enforcement. Certain of these proposals will be examined in the following sections but first, it is worth explaining the phenomenon of Cloud Computing and saying something about the environment within which it operates.

3. The Phenomenon of Cloud Computing

3.1. The Notion of 'the Cloud'

In *Riley v. California*, the US Supreme Court described Cloud Computing as 'the capacity of internet-connected devices to display data stored on remote servers rather than on the device itself'.[15] As previously noted, recent technological developments have introduced profound changes to the manner in which computing services are organised, including the way that data is stored. Consequently, a considerable amount of personal data is now stored, remotely, in data-centres. Cloud Computing services may take a number of different forms, depending on the requirements of the user;[16] and they offer clear advantages to users and service providers alike. For users, Cloud Computing offers flexible, location-independent access to computing resources while enabling service providers to pool their computer resources and to allocate them swiftly in response to user demand.[17] But while Cloud Computing is often viewed as an activity which occurs in a virtual environment, in reality, such services depend on the workings of computer hardware and physical storage facilities which have 'real-world' locations.[18] Indeed, the Cloud Computing model is founded on the extensive use of corporeal data-centres which, inevitably, come within the territorial jurisdiction of one State or another. Another central feature of Cloud Computing is that a user's data will often be broken up, copied and distributed across a number of servers for the

[15] (2014) 134 S Ct 2473, 2491.

[16] The 'Software as a Service' model focuses on end-user application functionality. Such services extend to the uploading of data on to web-based email accounts (e.g. Microsoft's Outlook); the offering of document hosting facilities (eg Google-docs); and social networking sites (such as Facebook). See W Kuan Hon, Julia Hornle and Christopher Millard, 'Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3', (2012) Queen Mary University of London, School of Law Legal Studies Research Paper No 84/2011 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240> accessed 12 September 2018, 3.

[17] Ibid.

[18] ibid, 4.

purposes of efficiency and security.[19] As a result, fragmented and mirrored data may be kept in different legal jurisdictions.[20]

Against this background, Cloud Computing has generated two interrelated difficulties for Law Enforcement Agencies (LEAs). The first involves situations where the officials of an investigating State gain access, by unilateral means, to data which is located in the territory of another State; the second concerns the same kind of unilateral trans-border activity with the difference that the geographical location of the sought-after data is unknown to the searching officials. This phenomenon has been labelled the 'loss (of knowledge) of location': one of its consequences is that, because the investigating officials cannot establish the whereabouts of the data in question, they do not know which State's territorial jurisdiction is being violated as a result of their activities.[21]

3.2. The Blurring of Online and Offline Criminality

The trans-border jurisdictional challenge is not restricted to cases where criminal activity occurs exclusively online ('cybercrime'). 'Real-world' crimes increasingly generate electronic data.[22] Perhaps, therefore, it comes as no surprise that the Budapest Convention is not restricted to cybercrime per se; instead, it covers the investigation of all specific instances of criminality which generate electronic evidence, too.[23] The generating and storing of electronic data in Cloud facilities has led, invariably, to the creation of a number of legal rights and obligations for the users and providers of such services. Specifically, the data owner/possessor may have entitlements to privacy and data protection, regarding the remote storage of content

[19] Ian Walden, 'Law Enforcement Access to Data in Clouds' in Christopher Millard (ed), Cloud Computing Law (Oxford University Press, 2013) 285, 287-288.

[20] However, the way in which data is controlled and located, in Cloud environments, remains an operational decision for the service provider in question.

[21] And, therefore, which State to approach for the purposes of securing its consent in order to render their extra-territorial actions lawful.

[22] For example, incriminating photos can be taken and uploaded, emails can be drafted and/or sent and, of course, such activity creates traffic data showing the whereabouts of a smart-phone user, times/dates and Internet Protocol addresses used.

[23] Article 14 of the Budapest Convention provides:

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

(2) Except as specifically provided otherwise […] each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: […]

(c) the collection of evidence in electronic form of a criminal offence.

data.[24] Service providers will, inevitably, be engaged in the processing of such personal data and they may also be deemed to be data controllers as well.[25] Data owners/possessors and service providers will also have specific rights and obligations in respect of 'traffic data',[26] and 'subscriber information'.[27] The cogency of a data owner/possessor's rights are organised across a spectrum with content data attracting the greatest level of protection followed by traffic data with subscriber information being viewed as less significant, at least from a rights perspective.[28]

3.3. The Jurisdictional Impacts of Cloud Computing

The technological advances associated with Cloud Computing have had at least two major consequences for the present purposes. First, service providers may choose to store data on connected computer networks where its servers are situated not only in a different jurisdiction to the data owner/possessor in question, but also in a separate jurisdiction to the one where the service provider itself is established. The practice of exporting data does not necessarily stem from an attempt to avoid the jurisdictional reach of a given State nor should it be viewed as a response to concerns about regulatory over-reach, although, of course, these may be reasons for following such a practice. Instead, as was explained in the Court of Appeals proceedings in the *Microsoft Warrant Case*, it is an arrangement which is often adopted in order to promote network efficiency.[29] In that case, the US criminal justice authorities

[24] For example, see Articles 8 of the 2000 EU Charter on Fundamental Rights (2012/C 326/02). Content data is not defined in the Budapest Convention. However, para. 209 of the Convention's 2001 Explanatory Report states that it: 'refers to the communication content of the communication; i.e. the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)'.

[25] The concept of 'processing of personal data' what constitutes a controller are set out in Article 2 of the 1995 EU Data Protection Directive (95/46/EC).

[26] See Article 1(d), Budapest Convention.

[27] See Article 1(c), Budapest Convention.

[28] The Cybercrime Committee's Guidance Note No 10 (Article 18) states that: 'Obtaining subscriber information may represent a lesser interference with the rights of individuals than obtaining traffic data or content data', para 2.2. The extent to a data owner/possessor or service provider has privacy rights/duties in respect of traffic data remains contentious. In its 2015 *Yahoo!* decision, n 3, the Belgian Supreme Court acknowledged that it would not have been able to hold that the data in question (traffic data) had to be turned over to the Belgian authorities if it had qualified as content data. Further, these categories invariably determine the level of authorisation required for LEAs to obtain access and obtain for the purposes of criminal investigations under municipal law. Judgment, para 9. See Walden, n 19, 290, for the UK position (although this work was published before the 2016 Investigatory Powers Act was enacted). The US position is set out in see the Court of Appeals Decision in *Microsoft v United States*, No 14-1985 (2d Cir 2016) Judgment, 16-19. On the wider significance of 'big data' see B J Koops, 'Law, Technology, and Shifting Power Relations', (2010) 25 Berkeley Technology Law Journal, 973.

[29] See *Microsoft v United States*, ibid, 8.

demanded that Microsoft hand over emails (i.e. content data), which were the subject of a Stored Communications Act 1986 probable cause warrant issued in relation to the suspected commission of drugs trafficking offences in the US. It was not disputed that the data in question was stored in a data-centre, belonging to Microsoft, in Dublin, Ireland.[30] The central issue in the litigation was whether the US authorities may compel a service provider to deliver content data located in another State's territorial jurisdiction, without its consent. As a result, this case can be used to illustrate the problems associated with unilateral trans-border activity where the location of the data in issue is known to the officials of the investigating State.[31] Secondly, Cloud Computing arrangements may make it is very difficult to establish the national location of any specific data which is stored in a given service provider's Cloud (i.e. which of its data-centres houses the data in issue).[32] This phenomenon has been termed the 'loss of (knowledge of) location' but even if the data's actual location is unknown to the authorities of the searching State, the data must, in fact, exist somewhere even if the data is stored in the form of fragmentary and replicated pieces.

Both situations are deeply problematic for national LEAs, albeit in different ways, because their actions in Cloud and online settings must observe the territoriality principle for the purposes of enforcement jurisdiction. Specifically, if an LEA conducts criminal investigations in the jurisdiction of another State, they may be violating that State's territorial integrity, jurisdictional competence and sovereign authority as a matter of international law. The territorial whereabouts of a particular data set determines which State is entitled to exercise enforcement jurisdiction and, therefore, which criminal justice system has the authority to investigate, prosecute and adjudicate in relation to a given matter.

The extra-territorial data storage problem presents a clear obstacle to the authority of the investigating State. However, if the location of the data in issue is known, the investigating LEA may be able to approach the other State with a view to conducting a search within its territory, pursuant to pre-existing MLAT arrangements. For example, in the *Microsoft Warrant Case*, Microsoft had structured its operations in

[30] Via a wholly-owned subsidiary company registered in Ireland. Microsoft maintained that no copies of the emails which had been exported to Ireland, were retained in the US.
[31] The *Microsoft Warrant Case* will be examined in section 6 below.
[32] It might be argued that individual internet users can be easily identified by the IP addresses they use but this is to overestimate the accuracy of geolocation technologies and to overlook the way in which proxy servers can be used to avoid identification and detection. See Koops and Goodwin, n 13, 43.

such a way that the data in issue was stored at a particular location for reasons of network efficiency. It claimed that, in order to secure lawful access to that data, the US authorities should have used the MLAT arrangements the US government had had concluded with Ireland and/or the EU for this purpose instead of trying to obtain the data unilaterally, in contravention of international law.[33] In sharp contrast, the loss of location problem is more fundamental because it cannot be said with certainty where the sought-after data is situated. Consequently, it is very hard to establish which State has jurisdiction to enforce its criminal justice regime in a concrete case. In such circumstances, it may be virtually impossible for a given national LEA to secure access to the data in issue through the use of lawful means. As discussed below, certain Sates have sought to overcome the twin difficulties generated by Cloud Computing by using self-help methods. However, by engaging in unilateral trans-border practices for the purpose of accessing and retrieving data in such situations, investigating LEAs may be behaving in a manner which is contrary to established international law.

4. The Problem of Loss of (Knowledge of) Location

4.1. Jurisdiction and the Budapest Convention

A State's criminal justice authorities, invariably, possess the legal authority to access and seize data obtained through the search of a connected computer system situated within its *national territory*. This position was confirmed in the Budapest Convention. In particular, Article 19 requires State Parties to enable their respective LEAs to search, or access: a computer system, and any data stored within it (Article 19(1)(a)), or a computer-data storage facility located within their own national territory (Article 19(1)(b)). Further, Article 19(2) allows for an *extended* network search where the national authorities: 'have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system'. In such cases, the Convention provides that they, 'shall be able to expeditiously extend the search or similar accessing to the other system'. Finally, under Article 19(3), State Parties are required to empower their own LEAs to seize or secure computer data obtained pursuant to a search undertaken in accordance with the terms of Article 19(1) and (2) and to copy any data obtained; to render it inaccessible or to delete it. Nevertheless, these powers are subject to

[33] See the US/EU and the US/Ireland MLATs, n 12 and see section 6 below.

conditions and safeguards, set out in Article 15, which render certain international standards of human rights protection applicable in relation to their exercise.[34]

4.2. Article 32, Budapest Convention: The Narrow Territorial Exception

The Budapest Convention grounds itself in the ordinary principles of jurisdiction.[35] Notwithstanding this orthodox approach to jurisdiction at a general level, the Convention did come up with an original solution to the problem of unilateral trans-border access to stored computer data. In particular, Article 32 provides that:

> 'A Party may, without the authorisation of another Party:
> (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
> (b) 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.'

Article 32 allows LEAs to engage in unilateral trans-border access if the data owner/possessor has voluntarily consented to such access, or if the service provider has given lawful consent for this purpose. However, there are a number of obvious difficulties with this provision. First, it is unlikely that an individual, who may well be a suspect, will be prepared to consent to such access due to the risk of self-incrimination.[36] Secondly, as the Cybercrime Committee acknowledges, a service provider is unlikely to be able to give lawful consent because the material contractual terms and conditions of any service agreement will not be sufficient to show that the data owner/possessor has given his or her informed consent for this purpose.[37] Finally, it is highly doubtful that a service provider would be able to give valid consent in any

[34] Article 15(1) provides that: 'Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the [ECHR and ICCPR] and other applicable international human rights instruments, and which shall incorporate the principle of proportionality'.

[35] See Article 22, Budapest Convention.

[36] See Jan Spoenle, 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?' (2010) Council of Europe Project on Cybercrime Discussion Paper (Strasbourg, Council of Europe), 7.

[37] See Council of Europe Cybercrime Convention Committee, *Report of the Transborder Group for 2013* (2013) 30, 5 November 2013, 5; and the Council of Europe Cybercrime Convention Committee, *T-CY Guidance Note No 3 Transborder Access to Data (Article 32)*, 3 December 2014, para 3.6.

event as this may well violate the core principles of data protection law.[38] As a result, many service providers are unwilling to allow access to LEAs or to hand over data, in the absence of judicial order. Finally, as stated previously, if the national location of the data is unknown (or uncertain), then Article 32 will be inapplicable as the provision requires that the data be stored in the territory of another State Party. In sum, Article 32 does not really address the issue of trans-border access effectively. Notwithstanding this conclusion, at a conceptual level, the provision is significant because it displaces the territoriality principle in a narrow range of cases based on the consent of by private individuals (and other non-State actors) rather than the directly affected State.

It is notable that Article 15 was not drafted so as to be applicable in relation to the exercise of the *substantive* rights and obligations enumerated in the Budapest Convention. The text makes it clear that the human rights protections identified in this provision are only relevant to the exercise of the procedural powers set out 'in this Section'.[39] In any event, Article 15 was not meant to be engaged in extra-territorial situations. Accordingly, it is hard to see how these human rights protections can be read into situations involving the operation of Article 32 as a matter of course. It may be argued that recent jurisprudential advances, which has widened the scope of extra-territorial jurisdiction, could be harnessed in order to trigger such protections where it can be shown that the targeted individuals come within an investigating State's jurisdiction.[40] However, the prospect of these rights being afforded to individuals whose data is the subject of unilateral trans-border investigation by a foreign LEA was not envisaged, or endorsed, in the 2001 Convention.

One highly questionable way of addressing this difficulty is to adopt the mind-set that if it cannot be established which State's jurisdictional competence has been violated by the remote, unilateral investigative actions of another State, then it should be assumed that the data is located within the territorial jurisdiction of the searching State without further enquiry. Another approach would be to assume that, because it

[38] This point assumes that a data protection regime applies in relation to the activity in question.
[39] See the Council of Europe Commissioner for Human Rights, *The Rule of Law on the Internet and in the Wider Digital World* (2014), 94.
[40] See, eg *Al-Skeini and Others v UK* (2011) 53 EHRR 18; Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles and Policy* (Oxford University Press, 2011); Samantha Besson, 'The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to' (2012) 25 Leiden Journal of International Law 857.

is highly unlikely that the affected State will ever discover that the remotely accessed/obtained data was actually located within its territory, then in the absence of knowledge, only a nominal infringement of its sovereign authority has occurred. Both approaches are without foundation from the standpoint of international legality. But, as discussed below, they do seem to have influenced the responses and recommendations of institutional actors to the jurisdictional challenges engendered by unilateral trans-border access. Moreover, this point of view appears to be particularly attractive when unilateral trans-border activity can be justified on exceptional grounds.

In these circumstances, it is perhaps unsurprising that some States have chosen not to wait for international consensus to emerge on this issue. Specifically, certain LEAs have been accessing and retrieving data stored on connected computer systems in a manner that may, ostensibly, be consistent with the terms of Article 19(2) of the Budapest Convention while ignoring the provision's qualification, which restricts the exercise of such investigatory powers to the searching State's own territory.[41] Further, certain LEAs have also adopted the practice of conducting extra-territorial searches for data located in Cloud facilities that are not dependent on the existence of a connected computer network based in the investigating State's territory. In other words, in such cases, an LEA would be engaging in a free-standing remote search rather than an extended search of a computer system situated within its national territory. Both these practices encroach on the territorial jurisdiction of another State and, therefore, they amount to a patent violation of international law. As noted above, a State may consent to the exercise of enforcement jurisdiction, by another State, in its territory in specific situations, via established MLAT arrangements, the use of which prevents what would otherwise amount to a wrongful act as a matter of international law. Consequently, in the absence of consent, such conduct may lead to a finding of State responsibility, in appropriate cases.[42]

4.3. Extending Unilateral Trans-border Access

[41] In this context, it is worth noting that Article 88 of the Belgian Code of Criminal Procedure allows the Belgian criminal justice authorities to access data known to be abroad in exigent circumstances and subject to certain conditions. The Dutch practice is to permit an extra-territorial search for data, on an exceptional basis, if the data's location is unknown (or if a remote search was undertaken by mistake) subject to a good faith requirement. See Koops and Goodwin, n 13, 55 and 84-87.
[42] See section 6, below.

The Cybercrime Committee has been grappling with the jurisdictional challenges posed by unilateral trans-border access for a number of years now. In 2011, it set up a sub-group, the Trans-border Access Group (TAG), to examine the jurisdictional problems that such activity posed for international law with a view to drafting an additional protocol to the Budapest Convention.[43] The TAG identified several ways in which the jurisdictional challenges associated with unilateral trans-border activity could be addressed. They included, inter alia, unilateral trans-border investigative activity in the territory of another State *without its consent*, if the criminal justice authorities of the searching State: (a) gained access with the lawfully-obtained authentication credentials of the data owner/possessor in question; or (b) they were acting in good faith or if their actions were justified by exigent circumstances (e.g. in response to an imminent danger, to prevent physical harm or the destruction of evidence).[44] The TAG also considered excising the territorial restriction contained in Article 19(2) so that an LEA could search for data, via a connected computer network, *beyond* its national territory.[45] In this respect, it recommended that such an approach should only be applied if the data was known to be in the territory of another State Party, or *when its location was unknown*.[46] Moreover, in its 2013 Annual Report, the TAG stated its view of the consequences of the loss of location in the clearest possible terms when it concluded that: 'It is not possible to apply the principle of territoriality if the location of the data is uncertain'.[47] This observation is particularly troubling from the perspective of international law because it reveals an eagerness to cast aside the primary principle of enforcement jurisdiction – territoriality – in favour of untried and untested alternatives. The default position should be that where the sought-after data's location is uncertain, the searching State should not attempt to access, or retrieve, data located in an extra-territorial setting due to the constraints imposed by the territorial character of enforcement jurisdiction. Nonetheless, it should be acknowledged that such a straightforward response prioritizes the principle of territoriality over a State's duty to maintain the integrity of its criminal justice system.

[43] See the Council of Europe Cybercrime Convention Committee, *(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding Transborder Access to Data* T-CY (2013) 14, 9 April 2013.
[44] ibid, 2-6.
[45] Ibid, 5-6. Also see the Council of Europe Cybercrime Convention Committee, *Annual Report of the Transborder Group* (2013) 30, 5 November 2013, n 37, para 296.
[46] Draft Elements, ibid.
[47] See the *2013 Annual Report of the Transborder Group*, n 37, para 298.

Consequently, it is evident that alternative approaches need to be considered in order to find a way of achieving a better balance between these competing legal obligations.

One of the TAG's most interesting recommendations concerned the adoption of what has been termed 'the power of disposal', an approach which offers a way of establishing a connection between a searching State and a data owner/possessor, for the purpose of undertaking a remote search in accordance with the established principles of jurisdiction in international law.[48] This model does not focus on the location of the data for the purpose of determining enforcement jurisdiction. Instead, it concentrates on the whereabouts of the individual (or individuals) who have the right to alter, delete, supress or render unusable the sought-after data.[49] The proposal anticipates that the power would be subject to certain conditions and safeguards. For the present purpose, the most significant are: (i) that it would be only exercisable where the location of the data in question is unknown, or uncertain (i.e. it is meant to address the loss of location problem); (ii) that it could only be used where the LEA has secured the suspect's authentication credentials, thus, ensuring access is obtained in a lawful manner; (iii) that the individual data owner (or possessor) whose data is targeted is in the territory of the searching State;[50] and (iv) that additional safeguards are needed – including the observance of fundamental human rights protections – in certain situations, especially where content data is being sought. [51] It has also been suggested that the power could only be used in exigent circumstances and/or pursuant to a judicial order.

The power of disposal does not try to displace the requirement of a territorial connection. Instead, it offers a different understanding of the required territorial link. Specifically, by focusing on the location of the data owner/possessor rather than the whereabouts of the data in question, the exercise of enforcement jurisdiction is, supposedly, transposed from the extra-territorial realm into the domestic one by the act of establishing the presence of the suspect in the searching State's territory. Accordingly, this innovative approach is still based on the requirement of a territorial connection for the purpose of exercising enforcement jurisdiction. Nevertheless,

[48] See Spoenle, n 36.
[49] Spoenle suggests that such a legal power is recognised by the Budapest Convention. points to Article 2 (concerning illegal access) and Article 4 (data interference) in support, ibid, 10.
[50] The power could also be exercisable in respect of a national of the searching State, ibid, 11.
[51] Spoenle refers to Article 15 BC in this regard but he does not appear to have appreciated the limit placed on the application of this provision, ibid, 12.

according to this method, the presence of the data owner/possessor within the territory of the investigating State takes precedence over the location of the data in issue and it is this which provides the jurisdictional trigger, in such cases.[52]

However, the power of disposal model does not readily acknowledge the fact that, in cases where the data is situated outside the searching State's own territory, the investigating LEA will still need to conduct a remote search for the material data in the territory of another State. As a result, the officials of the searching State will, inevitably, be exercising coercive public power in another State's jurisdiction, in violation of its sovereign authority. The proposed approach, therefore, ignores the extraterritorial aspect of the investigating State's activities preferring instead to focus on the whereabouts of those individuals who own, possess or control the data in question. Such an approach does not solve the problems associated with enforcement jurisdiction and, therefore, it does not offer a principled alternative to the general prohibition which was famously articulated in the *Lotus* decision.

Further, the power of disposal would seem to necessitate the drawing of a distinction between the exercise of jurisdiction over things (i.e. data), on the one hand, and persons, on the other. It could be argued that this approach might be supported by the fact that the investigative actions carried out by the agents of the searching State would not necessarily involve them physically entering another State's territory, or require the exercise of coercive powers over *persons* located there.[53] The strong implication being that the exercise of jurisdiction over property is somehow less intrusive than its exercise over persons. International law has never sought to distinguish between persons, things and events for the purpose of exercising either prescriptive or enforcement jurisdiction. Further, the idea that an individual's rights can be clinically separated from his or her property rights is completely untenable.[54] Moreover, from another perspective, such an approach would appear to endorse an unparalleled form of universal jurisdiction in relation to data; consequently, this argument lacks a secure jurisprudential foundation. It has been suggested that the power of disposal amounts to a *procedural* measure which does not involve the

[52] For the purposes of the power of disposal, such a focus is logically necessary because the location of the data is considered to be unknown or uncertain.
[53] See the position adopted by the Belgian Supreme Court in the *Yahoo!* Case, n 3, as discussed in section 6 below.
[54] See the provisions of the International Covenant on Civil and Political Rights (1966) 999 UNTS 171 (ICCPR); and the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), ETS No. 5 and Article 1 of Protocol 1 to the ECHR.

exercise of coercive power by State officials,[55] but it remains unclear why this is supposedly the case. The proposal's originator, Jan Spoenle, may have reached this conclusion because the power would be exercisable in respect of property rather than a given individual, or individuals. However, as discussed above, any such a distinction belies a misunderstanding of the implications of the exercise of public power in the context of fundamental human rights. Spoenle, evidently, understands that safeguards are needed to protect such rights, particularly in relation to content data, but he does not seem to appreciate that its implementation would depend on the exercise of broad coercive powers, by the public officials of the investigating State, in any event. Finally, it is hard to see how the use of lawfully-obtained authentication credentials could satisfy the broad requirements of legality as their use would involve State officials impersonating the individual concerned rather than providing a degree of legitimacy for an LEA's actions, in exceptional circumstances.

The TAG's recommendations – including the proposed power of disposal – attracted strong criticism from key institutional actors – including the European Parliament – due to serious concerns about the consequences that wide-ranging forms of unilateral trans-border access would have for the fundamental rights of directly affected individuals (especially suspects); the legitimate interests of third parties, (e.g. service providers); for the integrity of data protection regimes; and for the sovereign authority and territorial jurisdiction of those States affected by such extra-territorial activities.[56] In 2014, in response to such pressures, the Cybercrime Committee decided to drop its plans for the reform of trans-border access to data along these lines.[57] But since this setback, the Committee has redoubled its efforts to find the means to address the rapidly growing trans-border aspects of everyday criminality, which now represents a serious threat to the effective functioning of national criminal justice systems. In particular, in 2016, the Cybercrime Committee set up the Cloud Evidence Group (CEG) which was tasked with exploring whether new ways of addressing the jurisdictional challenges posed by the Cloud Computing could be found.[58] The CEG's proposals will be explored in detail below but, rather than seeking

[55] Spoenle, n 36, 10.
[56] See the Council of Europe Cybercrime Convention Committee, *Transborder Access to data and Jurisdiction: Options for Further Action by the T-CY* (2014) 16, 10.
[57] ibid, 12.
[58] Council of Europe Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for consideration by the T-CY,* T-CY (2016) 5.

to tackle the loss of location problem, the Group chose to channel its efforts into situations where the data's location is known. Nonetheless, in its Final Report, the CEG made it clear that the loss of location problem still needs to be addressed. To this end, it urged the Cybercrime Committee to reconsider the TAG's proposals, in the context of the recently revived process of the drafting of an additional protocol to the Budapest Convention.[59] As a result, those proposals remain alive and so it is important that, when institutional actors are reconsidering them, they have a clear understanding of their implications for international law and that any proposed reforms in this area are either consistent with the existing fundamental principles of the international legal order or seek to bring about the progressive development from a position of knowledge and understanding.

5. Unilateral Trans-Border Activity where location of data is known

5.1. Using Production Orders in Extra-Territorial Settings

The prospective use of production orders as a means of compelling individual data owners/possessors and service providers to hand over data to national LEAs, quickly gained significance in the CEG's work and this way of addressing the jurisdictional challenges presented by cross-border criminal activity has subsequently been championed by the Cybercrime Committee. The Budapest Convention seems to lend its support to the possibility that production orders may provide the basis for a fresh approach to the problems associated with the exercise of unilateral trans-border jurisdiction. Specifically, Article 18(1) of the Convention provides that:

> 'Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
>
> (a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
>
> (b) 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.'

[59] ibid, 144. Also see the Council of Europe Cybercrime Convention Committee, *(Draft) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*, T-CY (2017) 3.

Thus, Article 18(1)(a) allows the LEA of a State Party to issue production orders to individuals within its national territory requiring them to submit specific computer data stored in a computer system which is in their possession or under their control. Alternatively, under Article 18(1)(b), a service provider may be ordered to submit 'subscriber information' in its possession or control where it offers services in the territory of a Party. It is notable that, under this provision, a service provider is liable to produce information of a much more limited nature than in cases where a production order is addressed to the data owner/possessor.[60]

In its Guidance Notes on Article 32 and Article 18, the Cybercrime Committee made it clear that these provisions were adopted without prejudice to any additional powers provided for by the municipal laws of Parties to the Convention.[61] In other words, it recognises that States retain a wide margin of discretion as far as jurisdictional claims are concerned, an approach which is consistent with international law's orthodox position regarding the exercise of prescriptive jurisdiction. In addition, the Guidance Notes do not directly seek to challenge the established territorial conception of enforcement jurisdiction.[62]

Nonetheless, the most significant observation as far as Article 18(1) is concerned is that, in relation to both Article 18(1)(a) and (b), the sought-after data need not be within the ordering State's territory for it to be subject to a production order.[63] The functional scope of Article 18(1) was elaborated upon by the Cybercrime Committee in its corresponding Guidance Note. Specifically, the Committee stated that while production orders have the capacity to manifest an extra-territorial dimension, because they facilitate the retrieval of data which may be located in the territory of another State, such orders were justifiable because the individual addressees of a production order are persons who *freely* exercise possession or control over the sought-after data.[64] The key requirement as far as the functioning of Article 18 is concerned is that the recipient of a production order is present in the territory of the ordering State at the material time. Like the contemplated extension to Article 32

[60] See Article 18(3); the Budapest Convention's Explanatory Report (2001) para 177; and Guidance Note No 10 (Article 18), n 28, para 2.2.
[61] Guidance Notes No 3 (Article 32), n 37, para 3.2; and No 10 (Article 18), ibid, para 3.3; and para 293 of the Explanatory Report, ibid, para 293.
[62] See Guidance Note No 10, ibid, para 1. Article 32 was developed as a narrow exception to the territorial conception of enforcement jurisdiction. H Kaspersen, 'Cybercrime and Internet jurisdiction. Discussion paper (draft)' (2009) (Strasbourg, Council of Europe Project on Cybercrime), 27, para 75.
[63] See Guidance Note No 10, ibid, paras 3.1. and 3.5; and the Explanatory Report, n 60, para 173.
[64] See Guidance Note No 10, ibid, and the Explanatory Report, ibid.

regarding unilateral trans-border access, considered in the previous section, it is apparent that the territoriality principle is being re-orientated from one focused on the location of the sought-after data for the purposes of determining the issue of enforcement jurisdiction to the whereabouts of the data owner/possessor instead.

It is clear that Article 18 was not designed to cover instances where LEAs are directly involved in the search for remotely stored data. Instead, it appears to be a relatively modest device, one intended to operate in situations where either the identity of the individual data owner/possessor, or the relevant service provider, is known.[65] In the Committee's view, production orders constitute a less intrusive measure when compared with the search and seizure powers set out in Article 19 of the Budapest Convention. In addition, production orders still require the identity of the suspect to be known, and therefore, they cannot address the loss of location problem. Further, Article 18 only requires service providers to supply subscriber information as opposed to traffic or content data. Accordingly, while such orders certainly have the capacity to make a meaningful contribution to resolving the jurisdictional challenges presented by trans-border criminality, at best, they could only ever amount to a partial solution to these enduring problems.

One significant difference between the approaches adopted in Articles 32 and 18 respectively *seems* to be that, in relation to the operation of production orders, the investigating State would not be exercising coercive enforcement powers directly within the jurisdiction of another State; rather it would be requiring the individual data owner/possessor – or the relevant service provider in relation to subscriber information – to take the necessary steps to access and retrieve data which is located in another State's jurisdiction. In other words, in such cases, it appears that the ordering State is allowed to use indirect means to acquire the sought-after data. Nonetheless, on this reading, the searching State is still exercising its coercive authority, but as this is being done within its own territory its actions would *seem* to be in conformity with the territorial conception of enforcement jurisdiction. Thus, at first glance, it appears as though Article 18 provides the legal foundations in support of a credible – if somewhat limited – solution to the challenge of securing access to data in trans-border situations.

[65] Of course, knowing the identity of individual concerned is essential to the process of serving a valid production order in the first place.

However, the basis for the Cybercrime Committee's assertion that production orders are less intrusive than the search and seizure powers contained in Article 19 is questionable.[66] Production orders may be a more limited measure in terms of their scope of application, and, of course, they rely on indirect means of enforcement in relation to data which is located in an extra-territorial location, but there can be no denying that they involve the use of coercive powers by State officials against a recipient. Further, it appears that the Cybercrime Committee's interpretation of a production order has been guided by private law examples. Specifically, the CEG viewed Article 18 production orders as being comparable to inspection orders, which may be issued by the national authorities for the purpose of gathering digital evidence stored, via Cloud facilities, on servers located abroad in anti-trust cases.[67] It would appear that, in relation to both the functioning of inspection orders and production orders, the recipient is required to turn over data despite its extra-territorial location. The vital common element being that the recipient is present on the territory of the ordering State and the measure was issued under its executive authority under the terms of its national law.

But, in drawing an analogy between Article 18 production orders and inspection orders issued pursuant to EU Competition Law, the Cybercrime Committee failed to appreciate the difference between a measure developed for use in the context of civil litigation and one devised for the purpose of exercising criminal jurisdiction.[68] The coercive nature of criminal measures; their impact on recipients; and the penalties which non-observance attracts render these two orders incomparable. This is especially true when one considers that the extra-territorial effects of criminal measures will be heightened – from the perspective of the directly affected State – by the fact that criminal justice authorities of the investigating State will be involved. In this respect, it is important to emphasize that a pivotal consideration in the context of determining whether there is an exercise of enforcement jurisdiction by one State in the territory of another is establishing *who* is involved – directly or indirectly – in such activity. If the conduct is undertaken by officials who are carrying out governmental functions (or if a private actor is authorised to carry out such public functions), then it

[66] See Guidance Note No 10, n 28, para 3.4; and the Explanatory Report, n 60, para 171.
[67] In this regard, the CEG's approach was informed by the 'long-arm anti-trust doctrine' which is observed in EU Law: see the *ICI Ltd. v EC Commission* (1972, ECJ, Case 48/69). EU:C: 1972:70 and the *Woodpulp Case* 89/85, European Court Reports 1993 I-0130. See the CEG's Report, ibid, para 49.
[68] This leap between criminal and civil jurisdiction is made the CEG's Report, ibid, paras 48-49.

is much more likely for such activity to will be attributed to the investigating State.[69] In contrast, inspection orders (and subpoenas, too) are not considered to be instances of the exercise of enforcement jurisdiction because they are not executed by public officials rather , typically, they are issued at the behest of private parties,[70] nor do they mandate private individuals to exercise governmental authority in order to bring about compliance.

The entire argument in favour of the extra-territorial applicability of Article 18 production orders is premised on accepting that the ordering State has not conducted an extra-territorial criminal investigation at all, but rather that it has merely used its coercive powers over an individual, or individuals, present within its own territory. However, it is clear that this is a flawed assumption as it fails to account properly for the extra-territorial effects of the ordering State's conduct and it ignores the way in which the extra-territorial actions of a compelled individual – the recipient of a production order – may be attributed to the ordering State in certain circumstances (especially where that person is a custodian of data belonging to another) for the purposes of establishing State responsibility.[71] In addition, it is clear that Article 18 production orders do not address the question of consent in a satisfactory way. As noted in the previous section, Article 32 permits State officials to engage in unilateral trans-border access but this provision is validated by the freely-given consent of a data owner/possessor,[72] rather than as a result of the compelled production of data at the bequest of the ordering State. Indeed, it is apparent that a data owner/possessor's consent is not a legal requirement for operation of Article 18 production orders, as mediated through national measures. However, given the general legitimizing role that consent performs in relation to the data protection regimes,[73] it is hard to accept the Cybercrime Committee's assertion that production orders are, in fact, any less intrusive than other criminal measures when all the relevant factors are taken into consideration.

[69] See section 6, below.
[70] This point is noted in the context of the operation of subpoenas in the amicus brief by International and EU Law Scholars submitted to the Supreme Court in support of the Respondent, in the Microsoft Warrant Case, 19, n 4. See section 6, below.
[71] See section 6, below.
[72] Or, alternatively, the consent of the service provider in very limited circumstances.
[73] See Bert-Japp Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law, 250.

In July 2017, the Cybercrime Committee made arrangements for the commencement of work on drafting of an additional protocol to the Budapest Convention. It is expected that the draft protocol will seek to achieve a number of objectives, including: (i) to strengthen existing MLAT processes; (ii) to facilitate direct cooperation between LEAs and service providers in other jurisdictions; (iii) to establish a legal framework for the conduct of unilateral forms of trans-border access in exceptional cases; and (iv) to establish data protection requirements in the above situations.[74] A key proposal identified, by the CEG, in this context concerns the development of Article 18 production orders. To this end, it is notable that, in its 2016 recommendations, the CEG suggested that the jurisdictional options previously recommended by the TAG should be reconsidered within the context of this initiative. Consequently, it appears that the Committee intends to revisit the jurisdictional challenges posed by unmediated trans-border access and, specifically, the loss of location problem in the foreseeable future. The broadening and deepening of Article 18 may be more palatable to institutional actors, and State parties to the Budapest Convention, because the scope of production orders may – ostensibly – be susceptible to a broad interpretation in cases where the data in issue is located beyond the territory of an ordering State. In sharp contrast, demanding content and traffic data directly from service providers remains highly contentious for numerous reasons, including data protection considerations, fundamental rights observance, and commercial sensitivity, in addition to the general problem of the exercise of enforcement jurisdiction in another State's territory. Against this background, it is suggested that the Cybercrime Committee's faith in the capacity of production orders to address the jurisdictional challenges posed by extra-territorially located data for the investigation of criminal activity by national LEAs, is fundamentally unsound. The next section will seek to illustrate the difficulties confronting the Committee's preferred means of regulating unilateral trans-border activity by reference to two recent cases, namely the Belgian Supreme Court's Judgment in the *Yahoo! Case* and, more significantly, the *Microsoft Warrant Case*.

6. Recent Cases

[74] See the CEG's Report, n 58, 35-46; and the *(Draft) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol,* n 59.

6.1. The Belgian Yahoo! Case (2013-2015)

The *Belgian Yahoo! Case* concerned a request made by the Belgian public prosecutor to Yahoo! for traffic data in an effort to establish the identity of certain persons who, allegedly, used email addresses to commit internet fraud in Belgium, in violation of Article 46(a)(2) of the Belgian Code of Criminal Procedure. Yahoo!, a US based company which was not established in Belgium, refused to provide this information. Ultimately, the Belgian Supreme Court decided that: (i) Yahoo! qualified as an electronic communications service provider; (ii) it was commercially active within Belgium; and (iii) it targeted Belgian consumers.[75] Accordingly, the Belgian Supreme Court ruled that Yahoo! had 'voluntarily' submitted to the relevant provisions of Belgian law,[76] and its refusal to provide the required information constituted a criminal offence under Belgian law.[77] In reaching this conclusion, the Supreme Court held that there was no exercise of extra-territorial jurisdiction, on the facts, because the Belgian authorities had not conducted any criminal investigations in the territory of another State.[78] In its view: 'The Public Prosecutor does not require anything in the United States from an American subject, but requires something in Belgian from an American subject offering services on Belgian territory'.[79] Consequently, it decided that the orthodox territorial requirements for the exercise of enforcement jurisdiction were satisfied.[80] However, in delivering judgment, the Belgian Supreme Court drew a clear distinction between traffic data, which it considered to be susceptible to Belgian jurisdiction because was this data was deemed to be moving through Belgian territory, and content data which may be located within another jurisdiction. It acknowledged that the Belgian State would not have jurisdiction to enforce its jurisdiction in the latter situation.[81] While the Supreme Court did not give reasons for such a distinction it may have thought that the extra-territorial dimension of such unilateral conduct was harder to justify as any reference to territoriality would necessarily be more oblique. Of course, the *Yahoo! Case* involved the issuing of a nationally-developed criminal measure, the Belgian authorities could not rely upon Article 18(1) of the Budapest Convention

[75] See *Yahoo!* Judgment, n 3, paras 7 and 8.
[76] *Yahoo!* Judgment, ibid, para 9. The Supreme Court also observed that: 'A State imposes a measure of coercion on its own territory as far as there is, between the measure and that territory, a sufficient territorial link', para 5.
[77] ibid, para 3.
[78] ibid, para 8.
[79] ibid, para 9.
[80] ibid, paras 4 and 5.
[81] ibid, para 9.

because, under that provision, a service provider can only be required to produce subscriber information whereas, in the present case, the Belgian authorities were demanding that Yahoo! turn over traffic data. The question of whether the criminal justice authorities of the investigating State can access, or obtain, content data which is located in another State, was the subject of proceedings at the US Supreme Court in the *Microsoft Warrant Case*.

6.2. The Microsoft Warrant Case: Court of Appeals Decision

As noted above, the dispute concerned the operation of a warrant, issued pursuant to section 2703 of the US Stored Communications Act 1986 (SCA),[82] which, purportedly, compelled Microsoft to disclose specified content data to the US authorities in its possession, custody or control, data that would otherwise be protected under the provisions of the Act. During the Court of Appeals proceedings, Microsoft argued that, as the sought-after data is located in Ireland, the US authorities would be undertaking enforcement activities in the territory of another State. Moreover, it contended that, given the SCA's silence as to its territorial scope, the long-standing presumption against the extra-territorial application of US statutes should be upheld.[83] According to the jurisprudence of the Supreme Court,[84] in cases where Congress has not *expressly* provided for the extra-territorial application of a statute, a court must determine the Act's focus in order to establish whether: (i) the regulated conduct has occurred in a domestic setting; or (ii) it can be shown that the relevant behaviour involves the taking of action beyond US territory, in which case the statute would manifest an extra-territorial application.[85] In applying this test, the Court of Appeals decided that the SCA's focus concerned the protection of privacy rights in the context of information technology communications.[86] In its view, such a conclusion was supported by the statute's full title – the Electronic Communications Privacy Act – and

[82] The SCA forms Title II of the Electronic Communications Privacy Act 1986.
[83] See the Court of Appeals Judgment, n 28, 5. The presumption has evolved to guard against unintended clashes between US law and the laws of other States. Also see the closely related *Charming Betsy* canon which evolved out of the analysis offered by Chief Justice Marshall in the US Supreme Court's Judgment in *Murray v the Schooner Charming Betsy*, (1804) 6 US (2 Cranch) 64. For a recent assessment of this case see William S. Dodge, '*The Charming Betsy* and *The Paquete Habana* (1804 and 1900)' in Eirik Bjorge and Cameron Miles, (eds) *Landmark Cases in Public International Law* (Hart Publishing, 2017) 11.
[84] See *Morrison v National Australian Bank Ltd*, 561 US 247 (2010), 255.
[85] See Court of Appeals Judgment in the *Microsoft Warrant Case*, n 28, 21-25.
[86] ibid, 6.

the structure of its key provisions.[87] Accordingly, it ruled that the constitutional safeguards contained in the Fourth Amendment applied to stored electronic communications.[88] In addition, it noted that, under the terms of the warrant, Microsoft was not required to hand over its own data, but rather it was required to disclose information belonging to one of its customers. In the circumstances, the Appeals Court observed that, as the custodian of its customers' data, Microsoft was subject to a special duty to protect his or her privacy rights.[89]

The Court of Appeals went on to determine the point at which the interference with the customer's privacy rights would take place in the event that the warrant was enforced. The key question, in this respect, was whether it would occur at the location where Microsoft hands over the data to the US authorities (i.e. in US territory after Microsoft had exported it there) or in Ireland, when Microsoft accesses the data stored in its Dublin data-centre, for the purposes of its retrieval. If the former was correct, then the SCA would appear to manifest a permissible domestic application whereas, if the latter were true, then the regulated conduct would involve an impermissible extra-territorial application of the SCA. The Appeals Court held that any interference with a customer's privacy rights occurs where the protected data is *stored*.[90] Therefore, as the sought-after data was kept in a data-centre located in Dublin, it resolved that the warrant's execution would infringe upon Ireland's sovereignty, if MLAT procedures have not been followed.[91]

The Appeals Court noted that the terms of the SCA warrant compelled Microsoft to search and seize specified data, data which the parties agree is located abroad. In this context, it observed that warrants are only applicable in relation to US territory and it ruled that there was nothing to indicate that Congress intended for SCA warrants to have a different territorial scope.[92] Consequently, it held that the term 'warrant' should

[87] ibid, 13-17. Section 2701 protects stored electronic communications from unauthorised interference. Section 2702 prevents service providers from divulging such communications without the data owner/possessor's consent. Section 2703 permits these communications to be disclosed pursuant to a warrant issued in accordance with rule 41 of the Federal Rules on Criminal Procedure (which requires that a warrant be issued by a court of competent jurisdiction).
[88] ibid, 13 and 14. The Fourth Amendment to the US Constitution recognises the right of persons and their property to be protected against unreasonable searches and seizures in the absence of a probable cause warrant.
[89] ibid, 31-32 and 40.
[90] ibid, 39.
[91] ibid, 42.
[92] ibid, 18-19.

be given its ordinary meaning.[93] In reaching this conclusion, the Appeals Court also dismissed the US government's claim that an SCA warrant was materially different from an ordinary warrant because it exhibited characteristics similar to those of a subpoena.[94] The government had contended that a subpoena requires a recipient to produce the required material regardless of its location, as long as: (i) he or she is in US territory; and (ii) the required information is in his or her custody or control. In support of its argument, the government claimed that an SCA warrant does not require US officials to enter an addressee's premises to search and seize property in its possession, custody and control, but rather it requires the addressee to disclose data in its possession to the US authorities.[95] In this regard, it argued that there is no physical enforcement activity carried out, by the US authorities, in an overseas location as the necessary steps required to ensure disclosure would be taken by Microsoft itself.[96] The Appeals Court was not prepared to accept this assertion, noting that the SCA's provisions did not indicate that section 2703 warrants possess a hybrid quality.[97] In addition, it observed that, contrary to the tenor of the government's claim, an ordinary warrant is not exclusively dependent on public officials for its execution. Indeed, it is well-settled that private individuals may be required to perform an active role in its enforcement.[98] Finally, and importantly for the present purposes, the Appeals Court decided that the SCA warrant required Microsoft to act as an *agent of the US government* for the purpose of enforcing the warrant in an extra-territorial location and that, in effect, its actions could be attributed to the US.[99] This responsibility would extend to the actions required in order to access and retrieve the data located in Microsoft's Irish data-centre. In the circumstances, the Appeals Court concluded that the warrant was unlawful.

6.3. *Microsoft Warrant Case in the Supreme Court*

[93] ibid, 25.
[94] ibid, 20-28.
[95] This was the conclusion reached on this point by the Magistrate Judge at first instance in the *Microsoft Warrant Case*, ibid, 40.
[96] This was the conclusion reached on this point by the Magistrate Judge at first instance, ibid, 29. The government also argued that Microsoft is able to perform the actions of accessing, retrieving and exporting the data stored in its Dublin data-centre from its HQ in the US.
[97] ibid, 28-29.
[98] ibid, 29.
[99] ibid, 39.

In its Petition to the Supreme Court in the *Microsoft Warrant Case*, the US government argued that the relevant conduct in issue would take place in the US rather than abroad.[100] Specifically, for the purpose of determining the statute's focus, it claimed that the Court should follow a provision by provision approach instead of looking at the statute's overall effect.[101] In this regard, it contended that section 2703 is concerned with the act of disclosing data subject to an SCA warrant to the government rather than on privacy protection.[102] Alternatively, the government asserted that, as any disclosure would occur in the US, the material conduct would take place within US territory and, in its view, this showed the statute's domestic application.[103] Moreover, it reiterated the argument it advanced in the Court of Appeal – that an SCA warrant is similar to a subpoena in key respects, the most significant being that it generates an obligation to produce the required data irrespective of its location.[104] It also refuted the Court of Appeal's finding that Microsoft would be acting as its agent by obtaining the data from its Dublin data-centre and turning it over to the US authorities.[105] Instead, the government claimed that Microsoft already has lawful possession of the data because its operational policy, which led to the data being stored in Ireland, did not generate any privacy rights for its customer.[106] In any event, it argued that as the act of turning over the data to the authorities would take place in the US, and because the data would be delivered pursuant to a probable cause warrant there can be no privacy incursion as the compelled disclosure was lawfully justified.[107]

In response, Microsoft argued that the Supreme Court should follow the approach adopted by the Appeals Court.[108] Relying on the reasoning adopted in that decision, it restated its argument regarding the SCA's proper focus and that the conduct in issue amounted to an impermissible extra-territorial application of the statute's provisions.[109] Further, it claimed that the government's contention that the specific focus of section 2703 is on disclosure rather than on privacy protection is

[100] US Government's Petition to the Supreme Court, n 4, 12-14.
[101] Petition, ibid, 13-17 and 21-22. It derives authority for this proposition from the Supreme Court authorities of Morrison, n 84, 267 and *RJR Nabisco, Inc v European Community*, 136 S C 2090 (2016), 2101.
[102] Petition, ibid, 16-17 and 19.
[103] Ibid, 17.
[104] Ibid, 23-24.
[105] Ibid, 20.
[106] Ibid, 17-20 and the US Government's Reply in the Supreme Court Case, n 4, 6.
[107] Ibid.
[108] Microsoft's Brief in Opposition in the Supreme Court Case, n 4, 26-30.
[109] Ibid, 10-14.

flawed.[110] Instead, Microsoft observed that sections 2701 and 2702 together provide the general position (i.e. that stored electronic communications are protected by privacy entitlements) while 2703 provides a limited exception by permitting the disclosure of stored data to the authorities when a court has issued a search and seizure warrant.[111] Consequently, it maintained that the meaning and function of section 2703 must be interpreted in the broader context of the operation of sections 2701 and 2702. In any event, Microsoft asserted that section 2703 is not engaged because the SCA's provisions can only be applied domestically and, as the relevant conduct occurs in Ireland, this provision is inapplicable, on the facts.[112] Moreover, in its reply to the US government's argument that Microsoft already lawfully possesses the data in question and, therefore, that the act of gathering it from the Dublin data-centre does not amount to an interference with its customer's privacy rights,[113] Microsoft reiterated the Court of Appeals ruling that such a claim ignores the duty that Microsoft owes as the custodian of such property.[114] It contended that the government failed to appreciate that Microsoft's control over the data in question may be regulated by data protection rules imposed by the State in which the data-centre is situated.[115] Finally, Microsoft raised the prospect that the extra-territorial activity mandated by the SCA warrant would result in a flagrant breach of international law because it would involve an intrusion upon Ireland's territorial sovereignty, without its consent.[116]

The Supreme Court proceedings were halted due to Congress' intervention. In particular, section 103(a)(1) of the CLOUD Act amended section 2701 of the SCA, by adding that:

> 'A [service 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

[110] Ibid, 6.
[111] Ibid, 6-7. See n 87 for the content of these provisions.
[112] Microsoft's Brief in Opposition, n 4, 6-11.
[113] Ibid, 32.
[114] Ibid, 12 and 33.
[115] In this respect, Microsoft relies on Article 48 of the EU's General Data Protection Regulation (EU/679/2016) which is due to enter into force in May 2018. Ibid, 17. It provides that: 'Any judgment of a court or tribunal […] of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State […]'
[116] Ibid, 16-17.

> whether such communication, record, or other information is located within or outside of the United States.'

After the CLOUD Act came into force, the US authorities sought, and obtained, a new section 2703 SCA warrant and, as a result, the parties agreed that there was no outstanding dispute. In turn, the Supreme Court ruled that the proceedings were rendered moot as a consequence.[117] Notwithstanding Congress' late intervention in the *Microsoft* litigation, the judgments of the lower courts and the written and oral arguments made to the Supreme Court in this case have considerable illustrative value. They illuminate our understanding of the challenges posed by Cloud Computing for the investigation, and prosecution, of trans-border criminal activity. Moreover, its intervention does not close down the key issues explored in this chapter rather it simply put them out of the reach of the US courts as far as the terms of the CLOUD Act are concerned. And, of course, there is no knowing how Congress' specific foray into extra-territorial jurisdiction will be treated by other States – the jurisdictional consequences of the CLOUD Act will become apparent over time.

The case's wider significance was spotted by Svantesson when he pointed out, in response to the decision of the lower courts, that the respective positions of Microsoft and the US government, as to whether their particular dispute manifests an extra-territorial dimension, were diametrically opposed.[118] To demonstrate their competing perspectives, he quote from the US government's brief prepared in connection with the Court of Appeals proceedings. It stated that:

> 'Relying on Section 432(2) of the Restatement (Third) of Foreign Relations, Microsoft argues that "[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state" […] But requiring the disclosure of records by a U.S. company does not involve any enforcement activity by government personnel on foreign territory, which is the concern of that section.'[119]

Svantesson suggests that the positions of the US government and Microsoft were, arguably, both correct.[120] In particular, he observed that:

---

[117] See the Supreme Court's judgment, 17 April 2018, n 4.
[118] Dan Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press, 2017), 51.
[119] ibid.
[120] ibid, 52.

> ‘It is true, as the Government says, that there is no enforcement activity on foreign territory. However, and this is important, there is an exercise of law enforcement functions on the territory of another state. In other words, the Government looks exclusively at the location from which jurisdiction is exercised (the United States). Microsoft also considers the extraterritorial effects and these effects occur in Ireland. In this way, the US Government gives extraterritoriality a narrow definition, while Microsoft gives it a broad definition.’[121]

Here Svantesson is expressing the view that international law has no way of resolving this difference of opinion – it ‘simply does not tell us where the conduct in question takes place in situations such as that of the Microsoft Warrant case’.[122] But while Svantesson may have accurately captured the positions of Microsoft and the US government as far as the issue of extra-territoriality is concerned, he has overlooked a serious error in the government’s understanding of the applicable law. It is correct that government officials would not necessarily be engaged in enforcement activity on another State’s territory but this is not the key test for establishing State responsibility as a matter of international law. The relevant measure was set out in Article 5 of the ILC’s Articles on State Responsibility. It provided that:

> ‘The conduct of a person or entity which is not an organ of the State […] but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance.’[123]

If Microsoft is compelled to access, retrieve and export data to the US, pursuant to the execution of a valid US warrant, this would trigger consideration of the matter of international responsibility, notwithstanding the fact that Microsoft is not an agent of the US government for other purposes.[124] And this point remains unaffected by the fact of Congress’ involved via the provisions of the CLOUD Act. The key question remains whether Microsoft would be exercising specific elements of governmental

[121] ibid.
[122] ibid, 51.
[123] Articles on the Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission, (2001) 53rd session A/56/10.
[124] See International & EU Law Scholars amicus brief, n 70, 8.

authority for a limited, or particular, purpose.[125] An important component for the attribution of conduct to a State is the requirement that the private individual concerned is 'empowered by law' to undertake the activity in question.[126] It would seem to be incontrovertible that Microsoft would be exercising governmental authority for the specific purpose of accessing and retrieving the data located in its Dublin data-centre and that it was authorised to carry out this task in accordance with US law, pursuant to a valid SCA warrant.[127] Of course, in order for international responsibility to arise, it would also be necessary to establish that the conduct in question qualifies as a breach of international law.[128] But it is hard to see how the exercise of enforcement jurisdiction in another State's territory, without its consent, would not satisfy this requirement.

Another interesting argument, which was advanced in the *Microsoft Warrant Case*, and one that connects the themes explored in this essay, is the way in which the US government sought to harness the normative essence of Article 18 production orders in support of its preferred interpretation of an SCA warrant insofar as its territorial scope is concerned.[129] In particular, the government argued that Microsoft qualified as a valid recipient of a production order for the purposes of Article 18(1)(a) of the Budapest Convention.[130] Accordingly, it claimed that Microsoft would be required to produce data in its possession, custody or under its control, even if that data is stored in an overseas location.[131] However, when a service provider is ordered to produce data, which it holds, in effect, on trust for one of its customers, Article 18(1)(a) is inapplicable as such situations are governed by Article 18(1)(b) instead.[132] This distinction is important because, as discussed above, service providers are only under an obligation to divulge subscriber information rather than content or traffic data in such cases.[133] Clearly, the US government's wide construction of Article 18 for the purpose of its argument regarding the ambit of SCA warrants has potential

[125] See James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press, 2002), 43, para 2; and James Crawford, *State Responsibility: The General Part* (Cambridge University Press, 2013), 126-132.
[126] See Crawford (2013) ibid, 132.
[127] This argument could only work if the relevant conduct occurs in Ireland.
[128] Article 2 of the ILC's Articles on State Responsibility provides that an internationally wrongful act occurs where conduct, which constitutes a breach of an international legal obligation, can be attributed to a particular State.
[129] In this respect, such an argument is used to bolster its claim that an SCA warrant shares vital characteristics with a subpoena.
[130] See Guidance Note No. 10 (Article 18), n 28, para 3.1.
[131] See the US government's Final Brief in the Supreme Court Case, n 4, 48-49.
[132] See International and EU Law Scholars amicus brief, n 70, 12 and 15.
[133] See Article 18(3) and ibid.

ramifications for the sovereignty and jurisdiction of other States – as, by and large, it would render MLAT processes redundant and Article 32 of the Budapest Convention a textual irrelevance.[134] The significance of this argument is that it illustrates the potential difficulties with the Cybercrime Committee's ambitious objective of using production orders as the foundation of a robust new regulatory regime for dealing with the jurisdictional challenges presented by transnational criminality.

The *Microsoft Warrant litigation* demonstrates – irrespective of the case's ultimate outcome – that we must view potential instances of extra-territoriality by recourse to an holistic interpretation of international law. Svantesson complains that international law does not tell us where the material conduct – the accessing and retrieving of the suspect's stored content data – occurs. Consequently, according to the thrust of his argument, it cannot determine whether the SCA is being applied on an extra-territorial basis or not. This may be a plausible reading of the situation if one looks to the international norms on jurisdiction alone. However, when we take the rules governing State responsibility into account things become much clearer as we begin to see that Microsoft would be acting as an agent of the US government for this purpose and, therefore, we are able to discern how an exercise of enforcement jurisdiction may arise in concrete cases. Unless we understand how the various rules and principles of international law work together to form a complete system of law,[135] it is easy to underestimate the extent to which international law is capable of addressing complex legal problems.[136]

7. Conclusion

This essay argued that the Cybercrime Committee's preferred *short-term* option for addressing the jurisdictional challenges posed by unilateral trans-border activity – the national production order – is misconceived insofar as it seeks to legitimize the unilateral retrieval of data located within another State's territory, in contravention of international law. In addition, the chapter showed how the US government's claims in the *Microsoft Warrant Case* created the circumstances by which the US may be accountable for the enforcement of its jurisdiction in the territory of a State, without

[134] ibid, 13 and 18.
[135] For arguments in support of the claim that international law amounts to a complete system of law see, eg, Lauterpacht, n 10.
[136] See the essay on State responsibility by Kimberly Trapp in this Handbook.

consent. It is notable that Congress' involvement, by enacting the CLOUD Act, has not diminished this risk. Finally, this essay demonstrated that current solutions to the problem of the loss of location, ones which seek to bypass the territorial conception of enforcement jurisdiction by reference to exceptional grounds, are unsustainable.

Some readers may find the approach followed in this essay to be unduly pessimistic, but I would suggest that there are good reasons to be cautious. Unilateral assertions of jurisdiction have a strong tendency to undermine international co-operation as they have the capacity to promote mistrust between States. Further, unmediated approaches to trans-border access invariably favour those States that have the power and resources to mount significant enforcement operations. Accordingly, they have, potentially negative implications for the concepts of sovereign authority and sovereign equality in general. Nonetheless, the scale of extra-territorial activity prompted by the advent of cyberspace constitutes a truly global phenomenon; consequently, territorialized approaches to the regulation enforcement jurisdiction are bound to fall short. Nevertheless, it is hard to see how unilateral approaches to a problem shared by all States will prove to be the best way forward. Clearly, multilateral solutions, or networks of bilateral arrangements, have the best chance of succeeding as they require closer co-operation between national criminal justice regimes. This kind of co-ordination can only be achieved through the development of global best practices and the conclusion of comprehensive and pragmatic treaty arrangements designed to tackle cross-border criminal activities effectively, irrespective of whether they manifest a cyber-dimension or not.