Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland

de Hert, Paul; Parlar, C; Thumfart, Johannes

Published in:
New journal of European criminal law

Document version:
Publisher's PDF, also known as Version of record

Publication date:
2018

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright, please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland

Paul de Hert
Vrije Universiteit Brussel (LSTS), Belgium; the University of Tilburg (TiLT), the Netherlands

Cihan Parlar
FIRST PRIVACY GmbH, Germany; Vrije Universiteit Brussel, Belgium

Johannes Thumfart
Vrije Universiteit Brussel (LSTS), Belgium

Abstract
This contribution reflects on recent cases involving cross-border data production orders such as Yahoo Belgium, Skype Belgium and Microsoft Ireland. Cross-border data production orders are found to generally involve conflicts regarding sovereignty and enforcement jurisdiction and to frequently include voluntary cooperation of companies for which the legal framework is lacking (Introduction). The Lotus principle, which recognizes a broad extraterritorial jurisdiction to prescribe and limits extraterritorial enforcement jurisdiction, is reconsidered concerning those issues (see the ‘International law pragmatism for jurisdiction to prescribe, but not for jurisdiction to enforce’ section) and the use of mutual legal assistances, which should be the rule, is discussed with four caveats (see the ‘Four caveats to territorial sovereignty and the need for MLAs: Unclarities and politics’ section). Twelve typical arguments are identified, which are employed in courtrooms when cross-border data production orders are discussed, for example, arguments regarding territorial sovereignty, the location of servers, the virtual presence of businesses via the Internet or the nationality of the data subject (see the ‘Arguments in courtrooms in favour or against informal-based cross-border investigations’ section). Subsequently, from fourth to seventh sections, those arguments are investigated regarding their context in the cases Yahoo! Belgium (2007–2015), Skype Belgium (2012–2017), Microsoft Ireland (2013–2018) and Google in re Search Warrant

Corresponding author:
Cihan Parlar, FIRST PRIVACY GmbH, Konsul-Smidt-Straße 88, 28217 Bremen, Germany.
E-mail: mail@parlar.co
Finally, a first step to evaluate and test the strength of those arguments is undertaken (see the ‘Assessing the arguments: From logically weak, to unpractical to law enforcement utilitarianism (give us everything)’ section).

Keywords
Extraterritorial law enforcement, courts, arguments, mutual legal assistance in criminal matters, consent in international law

Introduction – Cross-border law enforcement ‘questions’: Voluntary cooperation?

Because electronic communication makes up a larger and larger part of our lifeworld, and crime is, of course, a part of our lifeworld as well, more and more crimes are committed online or are at least somehow facilitated by a computing device such as a mobile phone, tablet or PC. Therefore, today almost all criminal investigations involve electronic evidence. This creates a number of fundamental problems, enforcement and sovereignty among them. As Woods puts it:

The fact is that the vast majority of the world’s Internet users are outside the United States, but they are using services headquartered in the United States. The result is that digital criminal evidence – evidence that would historically have been physically located in the same jurisdiction as the crime – is now very often stored in the cloud, and often with a service provider that is foreign.

While a state’s jurisdiction is limited to a certain territory, data traffic via the Internet is a priori designed to ignore borders. And the rise of cloud computing has led to a significant increase in cross-border data traffic. Between 2005 and 2012 alone, during the dawn of cloud computing, cross-border Internet traffic grew 18-fold. The clash between ubiquitous data and the territorial limits of state sovereignty is evident and forces prosecutors and other law enforcement agencies, together with courts, to make delicate decisions.

When law enforcement agencies approach providers to produce data, the respective service provider might be established abroad or storing the data sought after outside the investigating state’s territory. Usually, this extraterritorial aspect should require the use of the official channel of investigation, mutual legal assistance (MLA). This procedure, however, is regarded as being

---

burdensome and slow, especially when the establishment of the service provider abroad or data storage abroad is the only cross-border element of a case. Law enforcement agencies in the European Union (EU) have therefore developed other scenarios or ways to proceed, the most common being to approach providers in other countries directly with a request or order to produce certain data.

This approach or method is now so common that it has practically become a standard procedure in certain cases. It is impossible to assess precisely how many times law enforcement authorities in the EU have requested access to individual data held by Internet firms in the past, but these firms have started to produce transparency reports that give a flavor. From these reports, we gather that requests of EU law enforcement authorities amount to half of the total requests companies like Microsoft and Google, both based in the United States, receive.

This direct approach method clearly challenges some of our rule of law understandings: requests are sent to companies whose decisions to disclose the data can be considered to fall under another jurisdiction and access to the data would entail legal responsibility there. Moreover, the practice lacks consent by the requested state and any mediation by independent judicial authority.

Boulet and Hernanz speak about a scheme of voluntary cooperation, but immediately warn the reader that this voluntary mechanism creates a serious burden for private companies. Also difficult to reconcile with the voluntary nature of this method of cooperation is the reality of ‘bargaining’ between law enforcement authorities and private companies. Law enforcement authorities try to massage the information technology (IT) firms to be more cooperative. One of


6. For example, both the perpetrator and the victim of a crime committed in France could be French citizens and residents. The investigation will be carried out by French police and French prosecutors. However, they might have to acquire certain electronic evidence from a non-French service provider.

7. On the distinction between mediated and unmediated practices, see S. Carrera, G.G Fuster, E. Guild, et al., Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights (Brussels: Centre for European Policy Studies, 2015), pp. 6–9. Unmediated access practices are practices, whereby an authority in the requesting foreign country communicates its demands directly to the private company holding or controlling the data.

8. See for a discussion of several reports, G. Boulet and N. Hernanz, Cross-border law enforcement access to data on the Internet and rule of law challenges in the EU, Sapient, Deliverable 6.6, 2013, p. 16, 5–8.

9. Carrera, Fuster, Guild et al., Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights, p. 6. See also about challenges to the privacy rights of the individual, Boulet and Hernanz, Cross-border law enforcement access to data on the Internet and rule of law challenges in the EU, pp. 14–16.

10. Boulet and Hernanz, Cross-border law enforcement access to data on the Internet and rule of law challenges in the EU, p. 8.
their strategies is to insist on the rather innocent nature of their request by distinguishing two types of data: the content and the metadata, and by arguing that the latter is less sensitive and therefore more easy to hand over.\textsuperscript{11}

Anna-Maria Osula speaks about ‘informal’ mechanisms for accessing and obtaining extraterritorial data by law enforcement agencies characterized by a certain degree of ‘sidestepping’ the central role of the state and the principle of territorial jurisdiction as the determining factor for the location of the data.\textsuperscript{12} Walden, equally, speaks about informal mechanisms not regulated in relevant international law (for instance, the Cybercrime Convention of the Council of Europe) with a ‘voluntary’ nature.\textsuperscript{13} Interesting is his short discussion of the possible responses of IT firms when confronted with these requests. All the big players have developed internal policies. Numbers have shown that there is no standard ‘no’ or ‘yes’ practice. Sometimes requests are declined and referred to official channels to try again, but ‘any multinational cooperation is likely to be mindful of any impact that an adverse decision might have on the position of its domestic entity’ (in the country of the requesting law enforcement authority).\textsuperscript{14} Walden then subtly refers to Council of Europe guidelines and practices going back to 2008, clearly showing how states try to create a culture of cooperation between service providers and law enforcement authorities, encouraging the former to respond favourably to requests of the foreign law enforcement authorities.\textsuperscript{15} Similar political massage is to be found in EU programmes, Commission communications and European Parliament resolutions of the last decade.\textsuperscript{16}

Any precise analysis of the legal framework for these kinds of collaborations is lacking in these documents\textsuperscript{17} deliberately, because a legal framework is simply lacking. Article 18 of the 2001 Council of Europe Cybercrime Convention\textsuperscript{18} calls for drafting legal provisions in the Member States to make ‘their’ service providers cooperate (national production orders),\textsuperscript{19} but consciously avoids to regulate in clear terms international production orders sent to Internet service providers (ISP) and other IT players outside the country. With a majority of these players established in the

\textsuperscript{11} Op. cit., p. 15.
\textsuperscript{12} A.M. Osula, ‘Remote search and seizure in domestic criminal procedure: Estonian case study’, \textit{International Journal of Law and Information Technology} 24(343–373) (2016), pp. 344–345. There are other examples of informal extraterritorial practices. Next to directly contacting the service provider, examples that come to mind are accessing publicly available data and undertaking investigative measures such as remote search and seizure.
\textsuperscript{14} Op. cit., p. 301.
\textsuperscript{17} Boulet and Hernanz, \textit{Cross-border law enforcement access to data on the Internet and rule of law challenges in the EU}, p. 11.
\textsuperscript{18} CETS No. 185, entered into force 1 July 2004.
\textsuperscript{19} \textit{Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: […] (b) 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 (Article 18 (1) b).
United States, it therefore comes as no surprise that (data) production orders with a cross-border dimension have been the source of high-tension litigation as well as political discussions in Europe and the United States.

In the following, we will discuss the international law context of cross-border orders and the distinction between the very broad jurisdiction to prescribe and the more strict jurisdiction to enforce (see the ‘International law pragmatism for jurisdiction to prescribe, but not for jurisdiction to enforce’ section). In the light of this strict regime surrounding extraterritorial law enforcement, we then wonder why MLA in criminal matters that should be the rule is not taken seriously (see the ‘Four caveats to territorial sovereignty and the need for MLAs: Unclarities and politics’ section). No less than four caveats need to be made regarding territorial sovereignty and the need for MLAs. Because MLAs are bypassed in practice, controversies arise producing many court cases. In the next section (see ‘Arguments in courtrooms in favour or against informal-based cross-border investigations’ section), we identify 12 arguments heard and used in courtrooms in favour or against informal cross-border investigations. From fourth to seventh sections, we then take a closer look at Yahoo! Belgium (2007–2015), Skype Belgium (2012–), Microsoft Ireland (2013–2018) and Google in re Search Warrant (2017). In the final part, we will undertake a short, albeit in no way exhaustive, first step to evaluate and test the strength of those arguments (see the ‘Assessing the arguments: From logically weak, to unpractical to law enforcement utilitarianism (give us everything)’ section).

Our analysis of court cases will be parallel to short observations about the arguments to introduce legislation. In the ‘The arguments in their context: Microsoft Ireland Case (2013–2018)’ section, the US Clarifying Lawful Overseas Use of Data (CLOUD) Act will be mentioned. In our final section, we turn to the European Commission proposal of 17 April 2018 regarding a European Production Order as well as Preservation Order, and a directive which aims at obliging service providers to designate a legal representative in the Union, to whom orders can be addressed. We conclude that law enforcement utilitarianism explains the choice of final arguments in these texts, with only minor attention to the sovereignty interest of states and of individuals. By avoiding or slimming down the most controversial aspects of going extraterritorial via production orders and by using dangerous alternatives to the MLA system, such as threatening with punishment (contempt of court or fines), courts and magistrates have paved the way for a system where direct contact between magistrates and IT companies outside the territory became a reality, awaiting only some domestic framework arranged by the lawmaker to give a sign of ‘consent’ to these extraterritorial law enforcement practices.

International law pragmatism for jurisdiction to prescribe, but not for jurisdiction to enforce

An interesting late 20th-century criminal law–related development is the one towards the increasing use of provisions in national bills providing for enlarged jurisdiction in areas connected to human rights, such as terrorism, hostage taking, child pornography and human trade.20 States

---

20. See H. Osofsky, ‘Domesticating International Criminal Law: Bringing Human Rights Violators to Justice’, *The Yale Law Journal* 107 (1997), pp. 191–226. International law recognizes five grounds upon which states can base their jurisdiction: territorial jurisdiction stems from wrongs occurring within a nation’s territory; nationality jurisdiction is based on an offender being a national of the state taking jurisdiction; passive jurisdiction occurs when a victim is a national of the state; protective jurisdiction is based on the acts impinging upon important state interests of national security; and universal jurisdiction stems from the notion that some international prohibitions are so important that a
commonly incriminate or punish acts committed abroad. The growing entanglement of the world community apparently brings states to a growing recognition and acceptance of the enlargement of jurisdiction.\textsuperscript{21}

The logic and coherence of a presentation of criminal law in terms of territorial jurisdiction or of territorial sovereignty is therefore misleading. Indeed, the traditional limitation of criminal law upon territorial jurisdiction is (only) of pragmatic nature. No principle of international law forbids the enlargement of jurisdiction (jurisdiction to prescribe)\textsuperscript{22}: states can enact legislation binding upon their nationals abroad and even enact laws applicable to other facts or forms of conduct engaged in abroad and considered prejudicial to the state.

There is less pragmatism and there are more prohibitive rules when it comes to extraterritorial law enforcement (jurisdiction to enforce). Key here is the 1927 \textit{Lotus} judgment, in which the Permanent Court of Justice took the view that states have a broad margin when deciding upon substantive prescriptive jurisdiction, but that they violate sovereignty when their prosecution officers undertake actions on the territory of another country without permission. \textit{Lotus}, in a nutshell, gave us the rule that the \textit{jurisdiction to enforce} or the penal enforcement power should normally be confined to acts committed on the state’s territory. This type of jurisdiction ‘cannot be exercised by a state outside its territory except by virtue of a permissive rule derived from international custom or from a convention’.\textsuperscript{23} States can consent to the extraterritorial activities of other states, even implicitly,\textsuperscript{24} but this role for consent strengthens, rather than weakens the role of territory in international public law that protects states against all kind of extraterritorial material acts of other states.\textsuperscript{25}


22. See below.

23. See for a discussion of recognized prerogatives of sovereignty in international law, such as territorial integrity, right to non-intrusion and the principle of jus excludendi alios that protect against material violations of borders, B. Schotel, \textit{On the Right of Exclusion: Law, Ethics and Immigration Policy} (Oxon: Routledge, 2013), chapter 2.
international public law and no possibility for extraterritorial law enforcement unless a legal basis exists.

This insistence in international public law on territorial sovereignty with regard to law enforcement acts explains why supranational cooperation in criminal justice investigations and proceedings has been developed in international treaties which have taken the shape of MLA agreements. The fact that cooperation of foreign authorities has to be requested and that states cannot ‘serve themselves when possible outside their borders’ is a confirmation of the territorial sovereignty principle.²⁶ Carrera et al. phrase it as follows:

MLA represents the classical treaty-based mechanism allowing for foreign law enforcement cooperation and assistance in ongoing criminal investigations and proceedings, while respecting the notions of jurisdiction and national sovereignty in criminal justice matters. It constitutes the most important legally-binding tool that provides the rules through which third-country authorities can lawfully issue requests for assistance in relation to the gathering of evidence from foreign jurisdictions.²⁷

In the next section, we will discuss several caveats to this stricter regime for law enforcement actions abroad.

Four caveats to territorial sovereignty and the need for MLAs: Unclarieties and politics

Primo, there is the role of consent with regard to extraterritorial law enforcement. States can consent to the extraterritorial activities of other states, even implicitly.²⁸ One way of consenting is by drafting relevant treaty provisions. In the past, there were few examples of such arrangements, but their number is on the rise.²⁹ A real breakthrough in this regard is to be seen in the EU. After modest innovations in the 1960s with cross-border hot pursuit in the Benelux area, the EU followed with more arrangements in the 1990 Schengen Convention and in the 2000 EU Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the EU.³⁰ The latter allows direct sending by post of procedural documents intended for persons who are in the territory of another state (Article 5); the establishment of joint investigation teams that could, on the basis of mutual consent, carry out criminal investigations in one or more of the participating states (Article 13); and covert investigations in other states provided that there is agreement between the states involved (Article 14). Most striking is the provision allowing ‘without prejudice to the general principles of international law’ and ‘in the course of criminal investigations’ to intercept communications in other states ‘from which no technical assistance is needed to carry out the interception’ granted that the intercepting state informs the state of the interception when possible (Article 20). The EU Convention furthermore allows for more flexible bilateral

²⁸. A striking example of explicit consent can be found in the 1903 US-Cuba Lease of Lands for Coaling and Naval Stations Treaty stating that ‘(t)he Republic of Cuba consents that during the period of occupation by the United States ( . . . ) the United States shall exercise complete jurisdiction and control over and within said areas’. See for a detailed discussion of consent, Klip, ‘Soevereiniteit in Het Strafrecht’, pp. 145–149.
arrangements for the purpose of facilitating the exploitation of present and future technical possibilities regarding the lawful interception of telecommunications (Article 22).

All these provisions were copy pasted in the 2014 European Investigation Order Directive\(^{31}\) intended to replace and reinforce the EU Convention (without annulling it). These developments point at a diminishing attachment to sovereignty in the area of law enforcement in the Union. Member States agree that certain material acts can be done by others, even without consent and prior notice. Klip rightly sees in this a sign of growing trust and more confidence in correct behaviour of others who are not expected to abuse these new powers.\(^{32}\)

At the global level, there are less examples to be found of such arrangements, although a development in this direction is to be expected, perhaps not so much as a sign of growing trust, but as a result of necessity due to the omnipresence of borderless working technologies. We will discuss the US CLOUD Act below.

Consent between states via legal arrangements is only one aspect of current state practices. Implicit consent, as a result of convergence of views or power relations, is the most frequent practice. Klip discusses several examples (some will be discussed below) and points at the many unclarities surrounding this kind of consent: Who within the state apparatus can give consent (the legislator? the individual? the magistrate? the executive?)? What are the effects of a posteriori consent? Does it legitimize evidence gathered unilaterally? Assuming that the individual needs to consent, can he raise a violation of sovereignty as a defence in a criminal court?

Second, there is more unclarity, this time at a more general level about the scope of the *Lotus* prohibition on extraterritorial law enforcement actions. ‘You can incriminate behavior elsewhere, but you cannot send the police’, says *Lotus*. But what does that mean in light of today’s law enforcement options? Does the prohibition only regard physical actions and trespassing of borders, or is sovereignty violated every time some actions happen, even when carried out digitally?

There is clearly a need for a new *Lotus*, this time in cyberspace, clarifying digital extraterritoriality. Kaspersen, a key expert in discussions about extraterritorial computer searches without consent, simply sees no guidance in international public law for these and other more intangible actions. He refers to discussions in the 1980s about remote sensing by satellites. Since observed states cannot do anything about it and are usually not aware of it, these discussions simply withered away allowing further deployment of these satellites.\(^{33}\) In the ongoing discussions about a more contemporary practice, computer searches by magistrates, Kaspersen identifies at least three competing interpretations or views proposed by state authorities.\(^{34}\) Surprisingly, few defend the view that all searches of remote systems violate the exclusive jurisdiction and sovereignty of states. The opposing view is that these searches are to be understood as no more than virtual acts that, contrary to material acts, need no consent under international law. Most state representatives


adhere to a middle position: sovereignty can be endangered by remote searches, but magistrates do not always realize that their search has extraterritorial dimensions or cannot always avoid extraterritorial searches, so it is better to go for some legal arrangement.

Strictly legally, this middle position cannot satisfy to any degree, but its pragmatism probably best explains the rather hesitating attitude of states in these affairs, which brings us to the next loophole in the sovereignty story about law enforcement.

Third, territorial sovereignty is said to be important, but there is no established legal sanctioning system when states or individuals feel offended by extraterritorial law enforcement and very little development on this front is to be seen. On the contrary, Cassese quotes American, Israeli and British cases in which national judges have asserted jurisdiction over persons in custody, but who had been kidnapped by either American, Israeli or British state officials abroad contrary to international law principles on sovereignty.\footnote{A. Cassese, \textit{International Law}. 2nd ed. (Oxford: Oxford U.P., 2005), pp. 50–52, with reference to US v. Alvarez-Macain, Dominguez v. State, Eichmann and Regina v. Plymouth Justices, ex parte Driver.} In the \textit{Eichmann} case\footnote{Op. cit., pp. 50–52 with reference to US v. Alvarez-Macain, Dominguez v. State, Eichmann and Regina v. Plymouth Justices, ex parte Driver.} (kidnapped in Argentina in 1960 by Israeli agents posing as private individuals and taken to Israel), Argentine, not content with the apology offered by Israel, took the case to the UN Security Council, which called upon Israel to pay adequate compensation.\footnote{Op. cit., p. 52 with references.} The UN warning – a kind of soft political sanction – did not dissuade Israel from prosecuting Eichmann.\footnote{District Court of Jerusalem, \textit{The State of Israel v. Eichmann} [1961] 36 \textit{International Law Reports} (1961–62), 18; Supreme Court of Israel, \textit{Eichmann v. the State of Israel} [1962] 36 \textit{International Law Reports} (1961–62), 277.}

In many other examples furnished by Cassese, the reactions equally are often only of a political nature, with only a minor role for legal sanctions or conflict solving. Klip discusses the ambivalent position of the United States in this matter. On the one hand, they have no objections against their forces kidnapping persons in other countries, even in violation of extradition treaties, and on the other hand there is no sign that the United States would tolerate kidnapping by other countries on its own territory and there is more reluctance by the United States to kidnap persons in befriended European countries.\footnote{Klip, ‘Soevereiniteit in Het Strafrecht’, pp. 141–142.} Power, more than legal concepts, seems to determine the weight given to sovereignty. Powerful nations take more liberty with sovereignty interests of nations and rules seem to count more for countries that undergo extraterritorial actions than countries that undertake them.\footnote{P. B. Heymann, ‘Two Models of National Attitudes toward International Cooperation in Law Enforcement’, \textit{Harvard International Law Journal} 31(1) (1990), pp. 99–107.} Already in 1990, Heymann argued that states seek no rule uniformity but prefer flexibility: informal relations with compatible states and more formal relations with less compatible states (strong legal and political differences): a prosecutorial approach between compatible states with effectiveness as a priority; a more legal, international law approach between less compatible states, based on precise legal treaty obligations respecting sovereignty, but less focused on efficiency.\footnote{Heymann, ‘Two Models of National Attitudes toward International Cooperation in Law Enforcement’, p. 102. See also N. Boister, \textit{An Introduction to Transnational Criminal Law}. 2nd ed. (Oxford: OUP, 2012), p. 23.}

Woods adds another layer to the political analysis: Not using MLA is not only a question of lacking capacity, Woods observes, but also of simply not being willing to:

\begin{itemize}
\end{itemize}
Law enforcement agents, and more importantly political leaders, resent the idea that they must request legal assistance from another country in order to access evidence that relates to a crime that occurs on their soil. This is an entirely understandable reaction. Why, national leaders ask, should we have to ask the United States for legal assistance when the company in charge of the evidence is operating on our soil, making money on our citizens? In a world where 90 percent of global Internet users are outside the United States, yet Internet services are dominated by American firms, international politics matter a great deal.  

Some authors therefore rightly speak about objections about the alleged inefficiency of the MLA procedure, insisting on independent and critical analysis of available evidence.

The foregoing teaches us that in international law, there is only recourse to political sanctions because of the role of politics. No better illustration for this than espionage among nations. Authors see as an intrusion into one state’s internal data by another state, and thus a violation of the principles of state sovereignty and non-intervention. However, there has been little interest among states to regulate espionage at the international level, as nearly all states actively practice it and apart from a few international rules limiting the scope of espionage, neither customary international law nor international treaties explicitly prohibit it. To illustrate the priority of politics in the area of law enforcement, Klip points at US Supreme Court case law on kidnapping, and we could add the US Supreme Court dual sovereignty theory, the theory that the exclusionary rule does not apply in cases where evidence is illegally obtained in another country. Exclusion is not applied, in other words, to the domain of

---

43. Carrera, Fuster, Guild et al., Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights, p. 2: ‘Arguments alleging that MLA agreement models are inefficient are not substantiated by the available evidence or statistics on their uses and practical operability. While there exist certain obstacles affecting their practical implementation, this study argues that they can be overcome through a combined approach focused on bilateral case consultations, day-to-day contacts, stronger political commitments, more effective use of existing tools and sound financial, technological and human resources investments in their implementation’.
45. Maša Kovč Dine, 265 with ref.; R. Buchan, ‘Cyber Espionage and International Law’, in N. Tsagourias, ed., Research Handbook on International Law and Cyberspace. (Cheltenham: Edward Elgar Pu, 2015), pp. 168–190; Buchan, Cyber Espionage and International Law, 2018, p. 208. In both contributions, Buchan discusses a number of general principles of international law that indirectly regulate cyber espionage: territorial sovereignty, non-intervention and the prohibition of unlawful use of force apply to cyber espionage and equally a number of principles that could justify espionage such as the doctrines of self-defence and necessity. In his monograph, attention is also given to the role of diplomatic and consular law, international human rights law and the law of the World Trade Organization in addressing cyber espionage. He concludes with a plea to develop an international law of espionage which, as lex specialis, contains rules that are specifically designed to confront the growing threat posed by cyber espionage.
48. U.S. Supreme Court, United States v. Balsys [1998] 118 United States Supreme Court Reports (U.S.) 2218. The Supreme Court based itself on the following line of thought: the sovereign of one country cannot let itself be bound by the rules of the sovereign of another country, even if basic rights are at stake. See also U.S. Supreme Court, Heath v. Alabama, [1995] 474 United States Supreme Court Reports (U.S.) 82. See, critically, S. Winger, ‘Denying Fifth
international judicial cooperation because it is assumed that the prosecuting country cannot blame the other country for negligence. 49

The absence of firm sovereignty-supporting judgments is also striking at the European side. We know of no cases where the European legal system has responded adequately against actions such as spying, kidnapping for criminal law purposes, satellite spying of other countries, and Echelon. Moreover, we see no willingness on the part of the European legal system to condemn violations of sovereignty by law enforcement officials abroad. Illustrative is the case law of the European Court of Human Rights. 50 In principle, states are held responsible by the Court for human rights violations in areas outside their national territory when they exercise effective control, but the application of these principles in Öcalan v. Turkey 52 is less convincing. The applicant was kidnapped by Turkish agents in Kenya and brought to Turkey. Kenyan officials denied having played any part in the arrest or having been informed by the Turkish forces. The Court agreed that from the moment Abdullah Öcalan was in Turkish hands, the European Convention on Human Rights applied (para 91) and that an arrest made by one state on the territory of another state, without the consent of the latter, affects the arrested person’s individual rights to security (para 85). 53 But then the Court goes on with a political stand on the danger of safe havens for fugitives ‘undermining the international system’ and the observation that there is no real proof that Kenyan sovereignty was violated contrary to international law and concludes that there was no human rights violation in the case at hand. 54

52. ECHR 12 May 2005, Öcalan v. Turkey.
53. Cooperation between states, within the framework of extradition treaties or in matters of deportation, for the purpose of bringing fugitive offenders to justice, is perfectly possible within the framework of the European Convention on Human Rights, provided that it does not interfere with any specific rights recognized in the Convention (para 86). This Convention is also the yardstick by which to measure extradition arrangements or, in the absence of a treaty, extradition practices between states when one is a party to the Convention and the other is not (para 87).
54. See the crucial ‘political’ stand by the Court in para 88: Inherent in the whole of the Convention is a search for a fair balance between the demands of the general interest of the community and the requirements of the protection of the individual’s fundamental rights. As movement about the world becomes easier and crime takes on a larger international dimension, it is increasingly in the interest of all nations that suspected offenders who flee abroad should be brought to justice. Conversely, the establishment of safe havens for fugitives would not only result in danger for the State obliged to harbour the protected person but also tend to undermine the foundations of extradition. On this basis, the Court arrived at a hands-off approach: ‘Subject to its being the result of cooperation between the states concerned and provided that the legal basis for the order for the fugitive’s arrest is an arrest warrant issued by the authorities of the fugitive’s state of origin, even an atypical extradition cannot as such be regarded as being contrary to the Convention’ (para 89). Irrespective of whether the arrest amounts to a violation of the law of the state in which the fugitive has taken refuge – a question that can only be examined by the Court if the host state is a party to the Convention – the Court requires proof in the form of concordant inferences that the authorities of the state to which the applicant has been transferred have acted extraterritorially in a manner inconsistent with the sovereignty of the host state and therefore contrary to international law (para 90). To reach its conclusion, the Court ignored the official denial of Kenyan officials (see above). The existence of a Turkish arrest warrant disseminated through the Interpol machinery and the ‘fact’ that
To the foregoing, one should add the case law of the European Court with regard to the exclusionary rule. *Schenk v. Switzerland*\(^{55}\) concerned the illegal gathering of evidence in another country: telephone calls involving a private person were illegally recorded in France and subsequently handed over to Swiss judicial authorities, but the Court found no harm in that. The example shows that Europe is not wholly unaffected by the American dual sovereignty theory and also that a solid system of legal remedies for violations of sovereignty is lacking. We refer to our observations about the role of consent under our first caveat. Courts seem hesitant to recognize a role for the affected individual to point at violations of sovereignty. Klip refers to the Israeli *Eichmann* case and the German *Dost* case: like in *Öcalan* the baseline seems to be that there is no autonomous right to call for sanctions in this matter. Only the concerned state can object in court to violations of sovereignty.\(^{56}\)

*Fourth*, territorial sovereignty can be made redundant by what Woods calls ‘dangerous’ alternatives to the MLA system understood as the best guarantee for state sovereignty (and individual rights):

If domestic law enforcement cannot conveniently access criminal evidence held by American Internet companies, it might 1) demand that data be held on local servers, where it can more easily be accessed (and surveilled); 2) deploy covert surveillance efforts to access the data (and perhaps demand a way around the service provider’s encryption); and/or 3) assert extraterritorial jurisdiction over the foreign-held data, throwing Internet companies into an unfortunate conflict of laws.\(^{57}\)

The last option consists more precisely in enforcing draconian state law when foreign Internet companies do not comply with local law. Woods gives the only half hypothetical example of Brazil seizing Google’s assets, arresting Microsoft’s employees and shutting down Facebook and Twitter because the company refuses to comply with a production order from a Brazilian court outside the existing MLA regime.\(^{58}\) Later on, we will discuss Belgian examples of straining foreign firms with criminal law sanctions.

---

\(^{55}\) In the 1988 judgment *Schenk*, the person charged had been criminally convicted in his own country, partly on the grounds of the recording of a telephone call made by him. *Pierre Schenk v. Switzerland*, ECHR 12 July 1988, Series A, No. 140. See in the same sense *Lidí v. Switzerland*, ECHR 15 June 1992, Series A, No. 238, para 43; *Vidal v. Belgium*, ECHR 22 April 1992, Series A, No. 235-B, para 33; *Dombo Beheer v. The Netherlands*, ECHR 27 October 1993, Series A, No. 274, para 31; *Scherler-Zgraggen v. Switzerland*, ECHR 24 June 1993, Series A, No. 263, para 66. Rather than dwelling on the lawfulness or unlawfulness of evidence, the Court looks to see whether the procedure as a whole has been carried out honestly and whether the judges have guarded themselves against prejudice. In Schenk’s case, Article 6 European Convention on Human Rights had not been violated (see paras 47–48 and 51 of the judgment).


Political unwillingness to go via MLA, objective and less objective frustrations about current MLAs and the existence of ‘dangerous’ alternatives to MLA explain the rising number of court cases, often including Internet firms that have not lived up to the demands of law enforcement authorities working outside the realms of MLA. Before discussing some of these cases more in detail, we first present an inventory of arguments used in courtrooms.

**Arguments in courtrooms in favour or against informal-based cross-border investigations**

We have found the following arguments being employed by judges and the parties in front of them in the aforementioned cases:

1) **The strict sovereignty argument**: This line of argument deals with the basic problem of everything discussed in this article. It denies the legitimacy to access extraterritorial data because the unilateral exercise of a state’s sovereignty outside of its borders implies a violation of another state’s sovereignty.\(^\text{59}\)^

2) **Servers are abroad argument**: This line of argument – storage location of the data as a connecting factor – regards the location of the server, on which the data are stored, as decisive. When data relevant to a case are physically stored in another territory, then, the argument goes, this data can only be obtained by law enforcement authorities by extra-territorial means.

3) **There are MLAs argument**: If, because of arguments (1) and (2), a cross-border element of a case is given, then, this argument goes, one should use an MLA.

4) **Our virtual actions are harmless or there is no physical presence abroad argument**: If law enforcement authorities do not need to physically enter another territory for obtaining information stored, they do not violate another state’s sovereignty by their actions. In those cases, this argument goes, an MLA is not needed.

5) **Your business is established on my territory argument**: This line of argument – use the location of the seat as a connecting factor – sees the establishment of a business on a territory as a necessary and sufficient condition for the possibility to obtain its data by the respective law enforcement authorities in a unilateral way. In a more flexible approach (from the viewpoint of law enforcement agencies), any domestic business presence (even when formally not an establishment) could be used as a connecting factor.

6) **Your business is virtually present argument**: If a company is participating in a national market only via the Internet and without maintaining a physical presence on its territory, it nevertheless has to comply with the laws concerning data production orders of the territory in whose market it participates. The participation in a market has also been understood as maintaining a virtual presence on a territory.

7) **Your business is a data controller and you are on my jurisdiction, and therefore so are all your data in my jurisdiction argument**: This is a variation on the fifth and sixth arguments. If a company present in one way or another on a given territory controls data, regardless of whether these data are stored abroad or domestically, it has to comply with data

production orders concerning these data according to the laws of the territory on which it is established.

8) *We can punish you wherever you are, if you are not cooperating argument*: This is one of the 'dangerous' alternatives to the MLA system discussed in the previous section (enforcing draconian state law when foreign Internet companies do not comply with local law). We discussed as an example Brazil seizing Google’s assets or arresting Microsoft’s employees, and promised to discuss Belgian examples of straining foreign firms with criminal law sanctions, where the argument is hidden after the less brutal-sounding argument of applicability of Belgian criminal jurisdiction over the investigated offence (see below). The US Nova Scotia case is an older example, and it is illustrative for the broad American discretion to obtain evidence available in other countries through the use of subpoenas and compelled consent. A subpoena from the Florida District Court Grand Jury obliged this Canadian bank with presence in Florida and the Bahamas to hand over client data available in the Bahamas subsidiary. After refusal of the Bank with the argument that the data were confidential in the light of banking law provisions of the Bahamas, the Bank of Nova Scotia was convicted for *contempt of court* with the argument that 'US criminal investigations must (not) be thwarted whenever there is a conflict with the interest of other states'.

9) *Nationality of data subject argument*: Rather than all previous ways to determine the territorial reach of data production orders, the nationality of a data subject should be decisive: it makes a difference when law enforcement requests are about data of a national of the requesting state.

10) The *nobody controls technology (technological reality) argument*: This argument is the most radical. It claims that it does not necessarily make sense to think of data as something that occupy a territory at all. Google, for example, breaks up its emails and stores them on different servers all over the world. To optimize performance, reliability and efficiency, the data are also automatically moved from one location to another. The company itself therefore cannot fully determine where each and every part of an email is actually stored at any given moment in time.

11) Linked to the foregoing argument: the *need to counter sophisticated transnational crime argument*. This argument is about the importance of territorial borders diminishing over time, not only owing to rapid technological development, but also due to the need to counter sophisticated transnational crime. It is essentially a non-legal argument, but our discussion of Öcalan v. Turkey (above) revealed that it is far from being a weak argument.

---


62. On how cloud services operated by global Internet companies frustrates local law enforcement authorities, see Woods, ‘Mutual Legal Assistance in the Digital Age’, p. 662 (stressing the obstacles created by US privacy laws) and Walden, ‘Law Enforcement Access to Data in Clouds’, pp. 287–289 (focusing on frustrations due to the technical inability to establish location (‘loss of location’).

63. Compare Osula, ‘Remote search and seizure in domestic criminal procedure’, pp. 346 and 366 about this argument used by Belgian magistrates.
in court. A similar argument was used in the very recent case *Centrum foûr raûttvisa v. Sweden* where a bulk surveillance system of electronic signals in Sweden for foreign intelligence purposes was deemed compatible with the human rights convention. Given the present-day threats of global terrorism and serious cross-border crime, the Court argued, as well as the increased sophistication of communications technology, that states have large discretion in setting up such systems of bulk interception.  

12) *Some data are harmless so I can ask for it argument*. All kind of data types are recognized in the legal systems of the world and all kind of consequences are attached to these typologies. Below in the *Yahoo!* case, we will discuss Article 46bis of the Belgian Code of Criminal Procedure (CCP), allowing public prosecutors to order operators of networks and providers of electronic communications services to hand over data such as the identification of the subscriber or regular user of an electronic communications service. For data about the content, a judicial warrant is needed.

Influential, both as a model and as a practical reference point in all data requests sent to the United States, is the Electronic Communications Privacy Act (ECPA) that distinguishes between content data and metadata. ECPA – especially when combined with privacy policies drafted by the IT players to protect customers – serves as a blocking statute for non-US law enforcement authorities. ECPA only allows the American Internet firms to share content (such as emails) when an MLA procedure has been followed to obtain a warrant issued by a US judge (that demands for probable cause). ECPA does allow American firms to produce metadata in response to non-US law enforcement demands, but ‘those firms are often unwilling to hand over metadata on the grounds that doing so is inconsistent with their terms of service or would otherwise anger civil liberties groups or threaten customer privacy’.

Walden rightly observes that around the world, similar types of data can be subjected to different authorization procedures. Neither the United States nor Europe requires that only judicial authorization procedures are adopted (although, in principle, the exercise of law enforcement powers should be entrusted to the supervisory control). In the United Kingdom, a judicial warrant is needed for stored data, an executive warrant for the interception of communication content and an administrative warrant for access to communications data. In the United States, there is the ECPA requirement of a judicial warrant for communication data, there is nothing for metadata and there is the flexible executive authorization procedure for the interception of foreign communications.

The point with regard to our 12th argument is the following: law enforcement people tend to agree that content data are more sensitive but have a hard time to agree with privacy concerns about metadata, especially basic subscriber information and location data, and when they want this from

---

66. Woods, ‘Mutual Legal Assistance in the Digital Age’, p. 662: Content refers to the contents of emails, photographs and other uploaded files, while ‘metadata’ refers to basic subscriber information such as user identification, as well as location and time data (known as communications data in the United Kingdom).
Google in California, they are not inclined to ask for MLA from the United States.\(^{69}\) The position of the IT firms, however, is not unreasonable. There is a growing awareness, also in courts, that the sharing of metadata cannot be accepted without proper guarantees.\(^{70}\)

Our presentation of 12 possible arguments in court is of course an author’s pick. Other arguments could possibly be identified, and some variations could be imagined. Several of these arguments are formulated from the viewpoint of the prosecution, and in court can and are adapted by other parties to further their interest. In the Belgian cases below, the fifth argument (your business is established on my territory) will be reversed by the respective IT firms arguing that since they have no establishment on Belgian territory, MLA should be used.

Woods proposes a similar list of elements that serve as jurisdictional hooks: the more arguments one can build up in favour or against an MLA approach, the stronger the case at least in political perception and perhaps also legally in court.\(^{71}\) A Commission document (discussed below) speaks about ‘connecting elements’. After a discussion of the arguments used in our selected court cases, we will come back to the respective weight of the arguments in our concluding section.

### The arguments in their context: Yahoo! Belgium Case (2007–2015)

The Yahoo! Belgium Case is a pertinent example of the complexity that surrounds production orders with a cross-border element and a fine example of an application of We can punish you wherever you are, if you are not cooperating (argument (8)). The context is of course that Belgium is a small country known for its activist prosecutors for whom location is outdated and also for its provisions in the CCP, introduced in 2000, are among the first in the world to allow the investigation judge to carry out remote digital searches abroad, with the weak obligation to inform competent authorities of other states ‘if possible’.\(^{72}\) Consequently, unilateralism is not alien to the Belgian DNA, at least of the judiciary.

The Yahoo! Case itself is an atypical case that raised many interpretative questions and therefore was brought no less than three times before the Supreme Court (Court of Cassation), in 2011,

---


70. See for instance European Court on Human Rights, Benedik v. Slovenia, 24 April 2018, application no. 62357/14 (The police request to an ISP and their use of the subscriber information leading to the applicant’s identification amounted to an interference with Article 8 (right to privacy) because of a lack of a legal basis with appropriate safeguards). A. Chatzinikolaou, ‘Benedik v Slovenia: Police need a court order to access subscriber information associated with a dynamic IP address’, blog published 1 June 2018. Available at: https://strasbourgobservers.com/2018/06/01/benedik-v-slovenia-police-need-a-court-order-to-access-subscriber-information-associated-with-a-dynamic-ip-address/ (accessed 12 September 2018).

71. Woods, ‘Mutual Legal Assistance in the Digital Age’, p. 674: ‘Another way to think about this is to consider each possible jurisdictional hook as further proof that the state has a compelling interest in the case in question. So the easiest cases are those we might call “wholly local” – where the crime is British, the suspect and victim are British, and every other aspect of the case is British but for the domicile of the company that controls the digital evidence in question. It seems least controversial to say that in these cases the British government can ask Google or Microsoft to hand over digital data in their possession if it meets whatever due process standards apply locally for relevance. In other words, digital data would be no different from physical data in these cases. The case for asserting a state interest – and therefore for justifying direct access to data – is incrementally more controversial as you remove each jurisdictional hook’.

Among the questions to be answered were the following two: Can Yahoo! be qualified as a provider of electronic communications services in the sense of Article 46bis of the Belgian CCP – that foresees a duty to cooperate \(^74\) – and thus be subjected to the obligation to cooperate with law enforcement authorities? Second, can a Belgian public prosecutor validly send a request to cooperate and provide personal user and communications data to a foreign provider of electronic communications services that has no presence in Belgium?

In 2007/2008, the public prosecutor of the city of Dendermonde requested the US-based service provider Yahoo! to disclose data such as IP addresses and subscriber information belonging to several email accounts hosted by the service provider. The request was sent directly by the Belgian prosecutor to Yahoo!’s offices in the United States. The order was based on Article 46bis CCP that, as we saw above, obliges electronic communication service providers to disclose identification data to prosecutors upon their request. Although Yahoo! is established in the United States and has no branch or office in Belgium, the public prosecutor was of the opinion that Yahoo! is to be considered such an electronic communications service provider and is consequently obliged to comply with his request. It is useful to quote the full text of Article 46bis CCP:

\(\text{§1 When tracking crimes and misdemeanors, the Public Prosecutor can [. . .] based on any information in his possession or by means of access to the customer files of the operator [of an electronic communications network] or of the provider [of an electronic communications service] proceed or order to proceed to: 1 the identification of the subscriber or regular user of an electronic communications service.}\)

\(\text{§2 (...) Refusal to communicate the information will be punished by a fine of twenty-six euro up to ten thousand euro.}\)

Yahoo! among other things claimed not to be a provider of electronic communications services in the sense of Article 46bis CCP and also that the requesting prosecutor would extend Belgian jurisdiction extraterritorially and thereby infringe the territorial sovereignty of the United States (\textit{strict sovereignty} (first argument)), since the company was physically not established on Belgian soil (\textit{business is (not) established on my territory} (fifth argument)) and therefore should address its requests via the official channel of MLA (third MLA argument).\(^75\) The prosecutor countered that Yahoo! was reachable from Belgian soil by email addresses it explicitly provided and furthermore would at least be ‘virtually present’, in the sense that it offers its service to Belgian customers (\textit{business is virtually present} (argument 6)).\(^76\) Based on the second paragraph of 46bis CCP, the


\(^{74}\) On the basis of said section, public prosecutors can issue requests to providers of electronic communications services to provide them with personal and communications data of their subscribers, such as identification data, IP addresses and communication logs. \textit{See below.}


\(^{76}\) Op. cit., p. 293.
prosecutor brought a legal challenge against Yahoo! before the Belgian criminal court of Dendermonde for failure to cooperate.

The case took a challenging road through the courts starting in 2009 at the Criminal Court in Dendermonde, being subsequently appealed at the Court of Appeals in Ghent in 2010, running further up the judicial ladder to the Court of Cassation (2011), from there being referred to the Court of Appeals in Brussels (2011), again up to the Court of Cassation (2012), from where it was finally referred to the Court of Appeals in Antwerp (2013) and ultimately brought in front of the Court of Cassation for the third and final time in 2015.

The Court of Cassation (2015) ultimately rejected Yahoo!’s argument and upheld the lower court’s decision to fine the service provider for not obeying the production order. The judges agreed with Yahoo! on the principle that a state, by imposing a coercive measure on the territory of another state, appropriates itself an extraterritorial jurisdiction that violates the sovereignty of that state (first argument). However, the Court of Cassation found that, contrary to Yahoo!’s argument, there was no issue of extraterritorial jurisdiction at stake. Indeed, according to the Court, the request for disclosure to an operator or provider active in Belgium does not imply any intervention outside the territory of Belgium, such as sending civil servants abroad. The whole affair was no more than an affair of territorial jurisdiction. It is possible to view that a state implements a coercive measure purely within its own territory, and not extraterritorially, as long as there is a sufficient territorial link between the measure and the territory in question.

Which territorial link is required in a given case is to be determined among other things by the nature and extent of the coercive measure at hand, but in this case the following four criteria or elements were relevant in the eyes of the Court: (1) virtual presence of the service provider in Belgium, (2) the quality or type of data sought, (3) applicability of Belgian criminal jurisdiction over the investigated offence and (4) no physical presence or act of Belgian law enforcement authorities outside Belgian territory.

Based on these criteria, the Court determined that (1) Yahoo! was virtually present by offering its service to Belgian customers, (2) the quality of data sought was identification data and thus of lesser personal relevance, (3) the respective data were sought in connection with a criminal offence investigation into apparent acts of fraud conducted from Belgian territory, which falls within the jurisdiction of Belgian law enforcement authorities and finally (4) the requested data are to be provided by Yahoo! to the Belgian law enforcement authorities in Belgium, whereby no physical presence or act by these law enforcement authorities abroad is needed.

The justices ultimately concluded that the production order at hand only constitutes a coercive measure which does not require intervention outside the Belgian territory. Any conviction of a

---

81. See respectively our 6th argument, 12th argument, 8th argument and 4th argument.
foreign service provider failing to comply with such an order is thus only carried out in Belgium and therefore no exercise of extraterritorial jurisdiction exists.  

**The arguments in their context: Skype Belgium Case (2012–2017)**

We encounter a similar line of reasoning in the more recent Skype Belgium Case. In this Skype Case, the Belgian investigator directed a request to Skype established in Luxembourg. Unlike the Yahoo! Case, the investigator ordered the service provider to provide technical assistance to intercept a suspect’s communication according to sections 88bis (2) and 90quater (2) CCP, instead of disclosing subscriber information as in the aforementioned case.

The request was sent by the Belgian prosecutor on 7 September 2012. Skype replied in several emails addressed to the Belgian authorities that it would not be able to disclose content data, since all communication is encrypted, and it does not store such data. However, it offered to provide subscriber information on a voluntary basis. It did not per se address the request for technical cooperation to intercept, but Skype – using arguments such as *there is MLA* (third argument) and *strict sovereignty* (first argument) – pointed out that any further compliance would need to be requested by the Belgian authorities through official MLA processes with Luxembourg, thereby challenging the Belgian authorities’ enforcement jurisdiction.

Subsequently, the prosecutor brought the case before the Criminal Court in Mechelen arguing that Skype, by refusing to collaborate, is liable for sanctions in the form of a punitive fine prescribed under sections 88bis (2) and 90quater (2) CCP, which function similar to the criminal sanction included in Article 46bis CCP used in the Yahoo! Belgium Case.

The Mechelen Court in its late 2016 decision ruled in favour of the prosecution.  

It addressed Skype’s argument that the request for cooperation could not be considered valid, since among other things it was not sent through the official channel of MLA and thereby exceeded the Belgian authorities’ jurisdiction. The Court by quoting the above-mentioned Court of Cassation Decision 2015 affirmed that a state implements only a coercive measure within its own territory, and not on foreign territory, as long as there is a sufficient territorial link between the measure and the territory in question (eighth argument). The Mechelen Court briefly declared, in the line of *Yahoo!*, that the respective request for interception did not require the presence of Belgian investigators nor any other material action abroad (fourth argument), but unfortunately did not further elaborate on the type of data argument used in *Yahoo!*, here content. Based on the figure of ‘virtual presence’ (sixth argument), the Court, like the Court of Cassation (2015) in *Yahoo!*, pointed out that Skype was present on Belgian soil by actively participating in the economic life in Belgium and therefore saw an ‘adequate territorial link’ to be established.

Skype brought the case in front of the Court of Appeals in Antwerp, which on 15 November 2017 upheld the Mechelen Court’s decision. This court in its decision emphasized that the

---

87. See Yahoo! Belgium Case in section I.1. of this Article.
88. Criterion 1 in the Yahoo! Belgium Case (see above), established by the Court of Cassation Decision 2015, Op. cit.
business is virtually present (sixth argument) and pointed out that economic presence transcends mere virtual presence in the form of a (passive) website and hence presents a sufficient territorial connecting factor to Belgium, regardless of the fact that Skype is physically not established on Belgian soil. According to the judgment, a company is already economically active in Belgium when it has the intention to enter into agreements with Belgian customers. Finally, the Court argues, since the requested cooperation has to be performed by Skype in Belgium, no investigatory measure by the Belgian State has to be performed in Luxembourg (fourth argument) and therefore an MLA procedure in the case at hand would be superfluous. Accordingly, a conflict between the aforementioned sections 88bis (2) and 90quater (2) CCP with Article 2 of the UN Charter in regard to the sovereign equality of the contracting States would therefore also not be in question.

The arguments in their context: Microsoft Ireland Case (2013–2018)

The Microsoft Ireland Case began in December 2013, when a magistrate judge at District Court for the Southern District of New York granted a warrant for search and seizure of information belonging to an email account hosted by Microsoft. The magistrate ordered the service provider to hand over a variety of data, including content, belonging to the aforementioned email account.

Microsoft produced all relevant subscriber information and non-content data, which were hosted on servers based in the United States, but went on and tried to vacate the warrant concerning the disclosure of content data, which were hosted on a server abroad in Ireland. The service provider argued that a US judge had no authority to issue a warrant for data stored abroad (location of server (second argument)) and must rather seek MLA from Ireland (there are MLAs (third argument)).

The aforementioned magistrate did not share this view and rejected Microsoft’s motion to vacate in April 2014. Similar to the Belgian court cases, the judge used no physical presence abroad (fourth argument) by pointing out that, since the search only occurs within the United States after the data are handed over to law enforcement authorities, it does not involve the presence of US investigators abroad. Different from the Belgium cases, the Microsoft Case does not circle around the service provider’s establishment but rather concerns the location of the server on which the sought data are stored.

Microsoft unsuccessfully appealed to the District Court for the Southern District of New York. The company used strict sovereignty (first argument) to challenge no physical presence abroad.
(fourth argument) by stressing that the seizure of the content data in the form of emails actually takes place abroad.\textsuperscript{98} The opposing US attorney’s office, in line with the district court judge, countered that the warrant only requires Microsoft to disclose data under its control regardless of where the data are stored (\textit{data controller} (seventh argument)).\textsuperscript{99} The attorney’s office went on to point out that the “warrant is served upon the provider [within the US]; the provider must produce its records to a law enforcement agent [within the US]; and if the provider fails to do so, the provider is subject to court sanction imposed [within the US]”, and thus any jurisdictional limitations challenged by Microsoft are “completely inapposite”.\textsuperscript{100} The attorney’s office thereby made use of the \textit{business on my territory} – (fifth) argument, which, since Microsoft is established in the United States, here works to the benefit of the prosecution.

The case went on to the Court of Appeals for the Second Circuit (2nd Circuit).\textsuperscript{101} The 2nd Circuit decided that a warrant is unenforceable when a service provider, such as Microsoft, stores the data outside US territory (affirming \textit{server is abroad} (second argument)).\textsuperscript{102} It argued that the respective provisions do not explicitly permit the issuing of a warrant with extraterritorial reach and therefore can only be used to issue domestic warrants.\textsuperscript{103} Notably, the justices point out that it is “difficult to dismiss” the interests of the foreign state Ireland to regulate the behaviour of service providers within its state borders “on the theory that the foreign sovereign’s interests are unaffected when a United States judge issues an order requiring a service provider to ‘collect’ from servers located overseas and ‘import’ data into the United States, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States” (connecting \textit{strict sovereignty} (first argument) with \textit{server is abroad} (second argument)).\textsuperscript{104}

In his concurring opinion, Judge Gerard E. Lynch additionally reasons that “we live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours, and their own legitimate interests. The attempt to apply U.S. law to conduct occurring abroad can cause tensions with those other countries” (\textit{strict sovereignty} (first) argument). The same judge points the finger where it hurts when he states that “the Irish government and the European Union would have a considerable grievance if the United States sought to obtain the emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland” but that the “case looks rather different, […] to the people and officials of Ireland and the E.U. […] if the American government is demanding from an American company emails of an American citizen resident in the U.S., which are accessible at the push of a button in Redmond, Washington, and which are stored on a server in Ireland only as a result of the American customer’s misrepresenting his or her residence, for the purpose of

\textsuperscript{98} Microsoft’s objections to the Magistrate’s Order denying Microsoft’s motion to vacate in part a search warrant seeking customer information located outside the United States, 13 Mag 2814, 6 June 2014, p. 2 ff. and 7 ff. Available at: https://www.eff.org/document/microsofts-objection-magistrates-opinion (accessed 29 June 2017).
\textsuperscript{99} Government’s Brief in support of the Magistrate Judge’s Decision to uphold a warrant ordering Microsoft to disclose records within its custody and control, 13 Mag 2814, 9 July 2014, p. 4 ff. Available at: https://www.eff.org/document/governments-brief-support-magistrates-decision (accessed 29 June 2017).
\textsuperscript{100} Op. cit., p. 20 f.
\textsuperscript{101} U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016), 14 July 2016.
\textsuperscript{102} Op. cit., p. 6 f.
\textsuperscript{104} Op. cit., p. 42.
facilitating domestic violations of American law, by exploiting a policy of the American company that exists solely for reasons of convenience and that could be changed, either in general or as applied to the particular customer, at the whim of the American company”.  

In this last observation, Judge Lynch ultimately affirms business is on my jurisdiction, and so are all its data (seventh argument), but goes beyond and softens the argument, by pointing out different sovereignty interests, from which especially the nationality of the target or data subject (introducing the ninth argument) stands out.

The US Department of Justice (DOJ) petitioned for rehearing, which was denied by the 2nd Circuit on 24 January 2017. Judge Dennis Jacobs, in his dissenting opinion to the denial of rehearing, questions the reasonableness of any argument based merely on the location of the sought data (second argument). He states that a “warrant can reach what their recipient can deliver” and therefore everything that is accessible from US soil through the respective service provider, even when stored abroad, should be considered to only constitute an act of the state within its state borders (affirming the fourth and seventh arguments, mixed with eight argument). According to Judge Jacobs, hence, “[I]ocalizing the data in Ireland is not marginally more useful than thinking of Santa Claus as a denizen of the North Pole”.

In its last attempt to challenge the decision, the DOJ asked the Supreme Court to hear its appeal in June 2017. The Supreme Court granted certiorari in October 2017 and heard the case in February 2018.

However, before the justices could hand down a judgment, the US Congress passed in March 2018 the CLOUD Act, which allows US law enforcement authorities to compel all companies based in the United States to provide the requested data, regardless of the data’s place of storage. As a result of this, the DOJ in March 2018 requested to vacate the case and obtained a new warrant under the CLOUD Act. The Supreme Court in response vacated the case and remanded the case to the Court of Appeals for the 2nd Circuit.

112. See section 5 of the CLOUD Act amending the Stored Communications Act (18 U.S. Code Chapter 121) by adding § 2713: ‘A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States’. (accentuation by the authors).  
In passing, we note that section 105 of the CLOUD Act sets the parameters for foreign governments to enter into executive agreements with the United States, based on which US companies will be enabled to respond to cross-border data requests.

The arguments in their context: Google in re Search Warrant (2017)

In Google in re Search Warrant, a magistrate judge ordered Google in February 2017 to comply with two warrants aimed at the production of foreign-stored email content. Google had previously refused to comply with the warrants issued in August 2016, relying on the rationale established in the Microsoft Ireland Case, especially server is abroad (second argument).

However, instead of storing an email in its entirety on a specific server such as Microsoft does, Google breaks up its emails and stores them on different servers all over the world. In order to optimize performance, reliability and efficiency, the data are also automatically moved from one location to another. Google itself therefore cannot fully determine where each and every part of the email is actually stored at any given moment in time: technological reality (10th argument). Additionally, and also different from the Microsoft Case, Google does not foresee access to email content for its subsidiaries abroad. The data can only be accessed directly from the Google headquarters in the United States, where the two respective warrants were served upon Google.

The magistrate, similar to the lower courts in Microsoft Ireland Case and Belgian courts before, makes use of no physical presence abroad (fourth argument). The judge furthermore challenges there is MLA (third argument) by pointing out that an already cumbersome MLA process with a foreign state would become impossible, since, in the case of Google, the data can only be accessed from within the United States, which would make any MLA request superfluous and therefore ultimately impossible to effectively access the sought data (10th argument). He argues that “Google’s cloud technology makes it uncertain which foreign country’s sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process.” Since the data are also automatically moving while potential MLA requests are pending, it might well be that the data will have already changed its location before foreign authorities could actually address the request properly.

Assessing the arguments: From logically weak, to unpractical to law enforcement utilitarianism (give us everything)

As one can conclude from the different, contradicting nature of the 12 arguments currently employed by courts when facing problems relating to trans-border data traffic and data production orders, it is difficult to predict the nature of a coherent solution to the problems discussed in those cases. Due to the fundamental incongruousness between the global scope of data traffic and the territorially limited understanding of sovereignty at one hand, and the need for finding fast ways to obtain data in some cases, however, it is probable that an international normative framework will

---

have to be established that grants faster and easier extraterritorial access than MLAs. It is sure that such a normative international framework on extraterritorial access to evidence, still to be developed, will in some way relate to the arguments laid out here.

Much more difficult than such general predictions and a mere exposition of those 12 arguments is the evaluation of their validity. The fourth argument (*no physical presence abroad*) seems to be the weakest since it seems to ignore the physical basis of contemporary digital communication and represents law enforcement utilitarianism at its worst, opening the gates to unilateral actions, weakening the rule of law and possibly causing stress on international relations. In fact, a district court in the United States has already refuted that argument in 2013 with surprising conceptual clarity:

> “Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location. Before that digital information can be accessed by the Government’s computers in this district, a search of the Target Computer must be made. That search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name”.119

Nevertheless, most courts seem to ascribe special importance to this *no physical presence abroad* argument when countering the *strict sovereignty* argument and justifying unilateralism.

Surprisingly though, none of the aforementioned courts addresses the question if not already the mere sending of a production order in the form of a letter or email accounts to an exercise of power in the territory of another state (the main idea behind the first, second and third arguments). This is unfortunate, since it is precisely the request in the form of an email or letter which carries the compulsory weight. Such law enforcement utilitarianism seems also to be the driving force behind the reasoning in the *Google in re Search Warrant*.

Of course, it cannot be denied that a fossilized understanding of territoriality is confronted by technological advancements, which will ultimately force the legal system to adapt. A justification of unilateralism on the grounds of efficient and effective battling of crime though (11th argument) does not live up to the rule of law and risks to undermine the causal dependency of effective fundamental rights protection from state sovereignty.

Other arguments are much more difficult to evaluate. It seems safe to say that service providers are more inclined to disclose subscriber information on a voluntary basis than content data.120 For the latter service, providers respond with *there is MLA* (third argument), as particularly seen in *Skype Belgium*, *Microsoft Ireland* and *Google in re Search Warrant*.

Essential to the cross-border discussion of production orders is the divergent scenarios in Europe and the United States. In the two Belgian cases, the service providers was physically not established within the investigating state’s borders, whereas in the United States cases, Microsoft and Google headquarter on US soil but store their data abroad. We have seen that Yahoo! as well as Skype used *business is not established on your territory* (fifth argument), whereas the Belgian authorities countered with *you are virtually present* (sixth argument).


120. This is often owed to provisions, preventing a disclosure of content data to foreign law enforcement in the first place, such as Article 48 of the GDPR (also known as the ‘anti-FISA clause’) or in the United States within the Stored Communications Act 18 *U.S. Code* § 2702 and § 2703.
In the United States, Microsoft as well as Google relied on servers are abroad (second argument) which was challenged by your business is a data controller and you are on my jurisdiction, and therefore so are all your data in my jurisdiction (seventh argument), an argument the judges in the United States, against all odds, seem to favour.

Jennifer Daskal in her analysis sees a location-driven approach (to determining enforcement jurisdiction) at work in Microsoft Ireland and a give us everything approach in the Belgian cases.121 Both approaches have a range of unintended consequences.122 The problems regarding the location-driven approach have to do with the MLA system. Interesting is Daskal’s critique of the Belgian approach she rightly points out that:

“[t]he Belgian courts […] endorsed an entirely new and potentially infinitely expansive ground for determining territoriality – based on where data is received, even if the relevant provider is not physically located in the receiving state’s territory.”123

Indeed, we saw how these courts dismissed business is not on the territory (fifth argument) and strict sovereignty (first argument), basing their argumentation on we can punish you if you are not cooperating wherever you are, so there is a territorial link and we are competent (eighth argument), established by the Belgian Court of Cassation in its 2015 ruling (and formulated in less brutal-sounding terms of ‘applicability of Belgian criminal jurisdiction over the investigated offence’ (see above)).

This resonates with the proposal Belgian policymakers brought forward during the expert process launched by the European Commission following the Council Conclusions in June 2016.124 Belgium, in line with its Court of Cassation ruling, proposed to qualify a production order as having an extraterritorial and therefore relevant cross-border aspect, depending on, first the sensitivity of the data sought after,125 with subscriber data being less sensitive than content data, and second on the geographical location of the target:

- When law enforcement authorities (only) seek subscriber information, such a production order would then be regarded as only “domestic”.
- When law enforcement authorities seek content, the key factor seems to be where the intrusion of privacy actually takes place.126 It does not immediately become clear though which criterion is determining the place of intrusion. The determining factor could be the location of the service provider,127 location of data128 or, quite intriguing, the intrusion

123. Different from Microsoft Ireland, the service provider in the Belgian cases is physically not present in the investigating state, and therefore can actually not access the data from Belgian soil.
125. Twelfth argument and criterion 2 established by the Court of Cassation Decision 2015 in the Yahoo! Belgium (see above).
127. In that case, the ‘Data Controller Argument’, (seventh argument) introduced in the Yahoo! Belgium Case, would prevail.
128. In that case, the ‘Data Location Argument’, introduced in the Microsoft Ireland Case, would prevail.
could be evaluated upon the target’s (data subject) residence or nationality, which seems to be the direction Belgium is actually promoting.\textsuperscript{129} The latter criterion also resonates very well with \textit{nationality of data subject} (ninth argument) raised by Judge Gerard E. Lynch in his concurring opinion in \textit{Microsoft Ireland}.

Belgium thus seems to promote direct production orders to foreign-established service providers but considers sovereign interests of states in which the target is residing in when it comes to more sensitive data, such as content.\textsuperscript{130} This underlines the Belgian court’s viewpoint, in that the state in which the service provider is established should be presumed to have no sovereign interest at stake.

The above sketched complexity boils down to several battlegrounds, from which one especially stands out. Legal frameworks regulating the access to electronic evidence through production orders are ambiguous and deviate from each other as to “what constitutes a ‘cross-border’ situation”.\textsuperscript{131} The European Commission, in its recently published Technical Document,\textsuperscript{132} points out that some laws use the storage location of the data\textsuperscript{133} in question as a connecting factor, others use the location of the seat of a potential addressee of an order\textsuperscript{134} and yet others rely on a domestic business presence of the potential addressee.\textsuperscript{135} This nebulosity is furthermore blurred by the lack of a harmonized and universal understanding of electronic evidence, in particular how to categorize specific types of data.\textsuperscript{136}

Finally, the Council of the EU in its efforts to improve criminal justice in cyberspace, concluded that the European Commission should explore possibilities for a common EU approach on enforcement jurisdiction in cyberspace in situations where existing frameworks are not sufficient, for example, “situations where relevant e-evidence moves between jurisdictions in short fractions of time”.\textsuperscript{137} The Commission was especially requested to determine which connecting factors can provide grounds for enforcement jurisdiction in cyberspace and “whether, and if so which investigative measures can be used regardless of physical borders”.\textsuperscript{138}

The Commission on 17 April 2018 proposed new rules in the form of a regulation, which foresees a European Production Order as well as Preservation Order, and a directive which aims at obliging service providers to designate a legal representative in the Union to whom orders can be addressed.\textsuperscript{139} An order can be issued to any service provider, ranging from classical Internet

\textsuperscript{129} In that case, the ‘Nationality of Data Subject Argument’ raised by Judge Gerard E. Lynch in his concurring opinion in the Microsoft Ireland Case.

\textsuperscript{130} According to an interview conducted with a legal advisor in the Federal Public Service Justice of Belgium.

\textsuperscript{131} Op. cit.


\textsuperscript{133} Op. cit. (emphasis added by authors).

\textsuperscript{134} See \textit{business is in my jurisdiction, so all its data too} (seventh argument) introduced in the Microsoft Ireland Case.

\textsuperscript{135} See also \textit{applicability of domestic criminal jurisdiction over the investigated offence} (eighth argument) introduced in the Yahoo! Belgium Case.

\textsuperscript{136} See also \textit{business is virtually present} (sixth argument) introduced in the Yahoo! Belgium Case.


\textsuperscript{139} Op. cit., conclusion point 11.

services, to social networks to online market providers, as long as the service is offered in the EU. This is the case according to Article 3 (4) (a) of the regulation, when the service provider is enabling “persons in one or more Member State(s) to use the services” and when, according to Article (4) (b), cumulatively “a substantial connection to the Member State(s)” exists. Recital 27 of the proposal clarifies that mere accessibility of a website or of an email address and of other contact details in one or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.

Recital 27 exemplifies that such substantial connection to the EU exists where

1. the service provider has an establishment in the Union, meaning “the actual pursuit of an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or a stable infrastructure from where the business is managed”, or
2. “the existence of a significant number of users in one or more Member States” or
3. “the targeting of activities towards one or more Member States”, which could be assessed on factors such as the use of language or currency, the possibility of ordering goods and services, availability of an app, providing local advertisement and providing customer services in the language generally used in the respective (targeted) EU Member State.

In perspective to the 12 arguments identified in this contribution, elements (2) and (3) clearly depict presence on the territory, formal or virtual (fifth and sixth arguments), whereas element (1) relates to the we have the data controller, hence all his data too (seventh argument), when considering the territory of all Member States, backed by the principle of mutual recognition, as a common territory. The pure we have the data controller argument is, however, watered down in that Recital 26 clarifies that services offered exclusively outside the Union are not in the scope of this Regulation, even if the service provider is established in the Union.

Additionally, Articles 15 and 16 of the regulation foresee a review procedure in case of conflicting obligations based on fundamental rights and other grounds of a third (non-EU) country. Article 17 (effective remedies) dictates that the ordering State is supposed “to ensure that information is provided about the possibilities under national law for seeking remedies and ensure that they can be exercised effectively”.

We conclude that, although the Commission proposal seems to at least recognize the importance of fundamental rights protection, the overall discussion on extraterritorial access to evidence via production orders is dominated by law enforcement utilitarianism arguments. Only minor attention is paid to sovereignty interest of states and of individuals.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.