Global Views on Internet Jurisdiction and Trans-Border Access

By
Cristos Velasco·, Julia Hörnle· & Anna-Maria Osula·

Abstract

This paper offers insights and perspectives on the jurisdiction of law enforcement authorities (LEAs) under international law and reviews current approaches to the territoriality principle and trans-border access to data for LEAs to conduct criminal investigations; controversial topics that are currently in the center of discussions, both at the international and national level. The views and perspectives offered in this paper seek to contribute to the international debate on cross-border access to data by LEAs and how the principles on internet jurisdiction should evolve in order to turn the administration of the criminal justice system more efficient, dynamic and compliant with the needs to obtain and secure evidence while respecting data protection safeguards.

Keywords: Internet Jurisdiction, Cross-border Access, Extraterritoriality, Mutual Legal Assistance, International Law, Data Protection

1. Introduction

'Jurisdiction' has different meanings depending on the context that the term is used, whether in the context of international law, private international law or criminal law and also depending on the legal system and tradition of a country. The scope of jurisdiction may vary widely from one state to another, however the term *'jurisdiction'* usually includes two main aspects. The first aspect is connected to state sovereignty and designates the power of a state and its agents over the territory, country, region, state or province. The second aspect concerns the exercise of authority and powers of a national court or judicial authority to apply and execute national procedural laws that are within their sphere of competence in order to attract and investigate a particular case based on existing principles, legislation and precedents or jurisprudence in a certain area of law.[1]

· Founder and Manager Protección Datos México (ProtDataMx) http://protecciondatos.mx and Ciberdelincuencia.Org http://ciberdelincuencia.org

· Professor in Internet Law at the Queen Mary School of Law, University of London.

· Researcher at NATO CCD COE Law & Policy Branch. This contribution contains the opinion of the respective author only, and does not necessarily reflect the policy or the opinion of NATO CCD COE, NATO or any agency or any government.

[1] Velasco, Cristos. *La Jurisdicción y Competencia sobre Delitos Cometidos a través de Sistemas de Cómputo e Internet*. (Tirant lo Blanch 2012), 207-209. For a perspective on the classification and types of jurisdiction under public international law, see pp. 209-215.

Internet jurisdiction has been one of the most controversial areas of Internet Governance[2] fundamentally because there is no *'one size fit all approach'* for each state to resolve the cross-border problems of the inherent in the use of ICTs and the internet. Internet jurisdiction intersects with different areas of law and a number of national courts around the world have issued landmark judgments and jurisprudence in order to resolve legal issues regulating the activities of companies with internet presence or individuals located in different territories that have experienced damage or loss of property or assets as result of their interaction and use of internet.[3]

It is well known that the internet is borderless and it has no geographic boundaries. However, laws and policies are still mostly subject to the territory and scope of the national boundaries of each state and the judgments issued by national courts usually – unless under very specific exemptions and circumstances – have no extra-territorial effects in other countries as further discussed in this paper. This is one of the main reasons why there is a wide number of legal approaches regarding the application of national laws to conduct in cyberspace.[4]

For instance, one of the main problems in the area of criminal law is to know the exact place and time where the crime was perpetrated and the location of the party or parties involved in the commission of such crime; a situation that is by all means uncertain on the internet, precisely because of the ubiquity of that medium, the difficulty to collect and secure electronic evidence by law enforcement authorities (hereinafter LEAs), as well as the availability of technologies and means used by perpetrators to conceal their identity[5], situations which make it extremely difficult for LEAs to know the exact geographical location of perpetrators to launch a particular criminal investigation.

This paper provides views and perspectives on some of the jurisdictional challenges discussed during the panel on *"Internet Jurisdiction and Law Enforcement"* at the Computers, Privacy and Data Protection 2015 Conference in Brussels.[6]

---

[2] For a perspective of internet Jurisdiction in the context of internet Governance, see: Kurbalija, Jovan. *Internet Governance*. (Diplo Foundation 2014), Section 3 Jurisdiction, pp. 92-96.

[3] For instance in the area of internet content and freedom of speech, see: *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme (LICRA)* 433 F.3d 1199 (9th Cir. 2006) http://law.justia.com/cases/federal/appellate-courts/F3/433/1199/546158/ and in the area of internet defamation *Down Jones & Company Inc v. Gutnick, Joseph* [2002] HCA 56 10 December 2002, full text of the High Court of Australia available at: http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html

[4] For national perspectives on cybercime jurisdiction, see: Bert- Jaap Koops and Susan W. Brenner. *Cybercrime and Jurisdiction. A Global Survey* (Asser Press 2006). For a perspective on cyberspace jurisdiction under public international law, see: Henrik Spang-Hansen. *Cyberspace and International Law on Jurisdiction* (DJOF Publishing 2004).

[5] See for instance the Tor network https://www.torproject.org/

[6] The video of this session is available at: https://www.youtube.com/watch?v=NL4nNlzyqmQ&feature=youtu.be

The views presented in this paper are mainly academic and do not neither represent consensus on the subject matter nor official views, opinions or policies of the institutions, organizations affiliated with each of the authors.

2. The Principle of Territoriality and Trans-Border Access

The territoriality principle is a fundamental principle of international law and effectively limits LEAs' powers to act within the territory of their state.[7] However it is argued here that it is not entirely clear what the territoriality principle means in the modern internet connected world.[8] An example where the legal boundaries of the principle of territoriality become especially blurred is when LEAs need for investigation purposes access data that is located extraterritorially.

All measures used and employed by LEAs to access data extraterritorially must be in accordance with the legal limits as set in both national and international law.[9] Notably, according to the established principle of jurisdiction to enforce, also known as the Lotus principle, established by the International Court of Justice (ICJ), states are prohibited to "*exercise its power in any form in the territory of another state" unless there are specific grounds to do so deriving from international custom or agreements.*[10] This may include, for example, the general prohibition of conducting an investigation on the territory of another state. Failure to do so may be considered as a breach of the sovereignty of the other state, and may lead to undesired escalation of retaliation activities.[11]

This concurs with the fundamental presumption against the extraterritorial expansion of enforcement powers based on national, domestic law. The consequence of the territoriality principle has been that a state who required intelligence or evidence stored abroad in the context of criminal investigations or prosecutions would have to use recognized international co-operation procedures, such as *letters rogatory* or Mutual Legal Assistance (MLA), the latter of which is based on bi-lateral or multi-lateral treaties.[12]

As an indication of states attempting to keep up with the territorial limits of jurisdiction to enforce, it has been reported that 70 per cent of the cases where there is a need to access

---

[7] Malcolm Shaw *International Law* (5th edition Cambridge University Press 2003) 579-584.
[8] Uta Kohl *Jurisdiction and the Internet* (Cambridge University Press 2007) 96-102.
[9] See Article 15 of the *Convention on Cybercrime*
[10] S.S. Lotus, Fr. v. Turk., 1927 P.C.I.J. (ser. A) No. 10, at 4 (Decision No. 9), 45 (Permanent Court of International Justice 1927).
[11] For a more detailed analysis of the Lotus Case, see: Paul de Hert, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace-Whose Sovereignty is at Stake?" in *Cybercrime Jurisdiction. A Global Survey*. Edited by Bert- Jaap Koops and Susan W. Brenner, pp. 97-98.
[12] Susan Brenner *Cybercrime and the Law* (North Eastern University Press 2012) 171-188.

evidence located extraterritorially, mutual legal assistance mechanisms have been used.[13] At the same time, recent studies have concluded that the format and procedures involved in mutual legal assistance treaties are not suitable for the volatile nature of digital evidence.[14] There are many reasons for this. MLA is usually considered slow and bureaucratic as it depends on the workings of diplomatic channels and is frequently hampered by political considerations and the principle of reciprocity.[15]Oftentimes the mutual legal assistance does not contain the required clauses to be considered valid or the lack of mutual legal agreements entered and ratified among the countries involved.[16]

It has therefore been argued that traditional MLA does not fit for the internet age, where cybercrime crosses borders on a massive scale and cloud computing[17] means that data is stored and controlled remotely. Thus, the internet age causes massive challenges for law enforcement. LEAs exercise coercive powers domestically to force the disclosure of communications data and/or the simultaneous interception of data in transit, both in respect of content data and meta-data[18] but the extraterritorial application of the same powers may become problematic.

In addition to MLA treaties (that may sometimes cover regions such as the European Union), informal cooperation with the foreign LEAs, or using the 24/7 points of contact networks may also be a way for obtaining relevant data.[19] However, there are two approaches to accessing extraterritorially located data that have recently been most actively discussed: first, access to data based on specific agreements such as the Council

---

[13] UNODC, *Comprehensive Study on Cybercrime*, February 2013. <http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

[14] Council of Europe Cybercrime Convention Committee (T-CY), *The mutual legal assistance provisions of the Budapest Convention on Cybercrime*. Adopted by the T-CY at its 12th Plenary (2-3 December 2014) e.g. p 123. <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf>.

[15] For further views on Mutual Legal Assistance and cooperation provisions in international and regional cybercrime instruments, see UNODC, *Comprehensive Study on Cybercrime*, *Op. cit*. 13. pp. 197-208.

[16] For a comprehensive overview, see *Ibid*.

[17] For views on cloud computing and cybercrime jurisdiction see: Cristos Velasco. *Jurisdictional Aspects of Cloud Computing* (Paper presented at the Octopus 2009 Conference on Cooperation against Cybercrime of the Council of Europe February 2009) available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf and Council of Europe. *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?* (Council of Europe 31 August 2010), available at: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

[18] This paper will not discuss the details of domestic powers and different categories of communications data.

[19] For a good overview, see Ian Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent* (Rochester, NY: Social Science Research Network, 14 November 2011) <http://papers.ssrn.com/abstract=1781067>.

of Europe Convention of Cybercrime facilitating the cooperation between its Parties[20]; and second, obtaining data through contacting the Service Provider. Latest developments regarding these two options will briefly be commented below.

2.1. Council of Europe Convention of Cybercrime

Despite current ongoing proposals seeking to amend mutual legal assistance treaties to better satisfy the needs of modern cyber crime investigations[21] and coordination and cooperation between regional judicial and police enforcement bodies like EuroJust and EuroPol[22], countries are seeking alternative approaches. For example, an explicit need to explore other options besides traditional MLA occurs in situations where it simply is not possible to identify the location of the data, like when the perpetrator makes use of anonymising or techniques to conceal their identity or data storage service features offered by cloud service providers, which may include storing data simultaneously in several databases, or distributed storage platforms worldwide.[23]

Transborder access has been the subject of analysis of an ad-hoc working group of the Cybercrime Convention Committee (TC-Y) of the Council of Europe since 2001. Perhaps the most well-known example of the "exception of the traditional territoriality principle"[24] is the Council of Europe's Convention of Cybercrime that includes a separate article on "Transborder access to stored computer data with consent or where publicly available" (Article 32). Article 32 of the Council of Europe Convention on Cybercrime allows the access to data located extraterritorially without the authorisation of another Party if it is publicly available (open source) or if the data is located in the territory of another Party and the Party seeking to obtain access to such data obtains "lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system." Old debates over the scope and exact meaning of said provision of the Convention on Cybercrime have led to explore a proposal for an Additional Protocol to further outline options for accessing data extraterritorially.[25] However, the limits of the scope of interpretation of Article 32 have not fully been agreed upon among the states that ratified the Budapest Convention, and the prospect of the

---

[21] *Ibid*. pp 128-134.
[21] *Ibid*. pp 128-134.
[22] See Joint Investigative Teams, EUROPOL, <https://www.europol.europa.eu/content/page/joint-investigation-teams-989>.
[23] *Supra* note 29, p 3.
[24] Cybercrime Convention Committee (T-CY) Ad-hoc Subgroup on Transborder Access and Jurisdiction Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)', (December 2013) < http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)7REV_GN3_transborder_V12adopted.pdf>.
[25] Council or Europe, *(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data*. Proposal prepared by the Ad-hoc Subgroup on Transborder Access, (9 April 2013) <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2914transb_elements_protocol_V2.pdf>.

adoption of an Additional Protocol has been halted due to the lack of consensus among state governments and other relevant stakeholders.[26]

There is ambiguity and legal uncertainty regarding the extraterritorial powers of law enforcement authorities to access data remotely in other countries in order to collect and secure evidence for purpose of criminal investigations. The scope of interpretation and the application limits of Article 32 of the Convention are very broad and countries have implemented this provision very different on a practical basis. The lack of consensus to create an Additional Protocol to the Budapest Convention will not prevent the regulation of transborder access to data in other countries. However, we strongly believe that the traditional concept of jurisdiction to enforce and its territorial application should evolve and be transformed by the states through the adoption of modern legal frameworks and transborder access to data practices that offer both, certainty and transparency for the states involved in cross-border investigations.

2.2. Direct Communication with Service Providers

Given the relative inflexibility of the MLA mechanisms as well as the ambiguity deriving from the interpretation of the Convention of Cybercrime, states are looking for alternatives. The pressing question today is whether LEAs should have the power to request communications data directly (i) from foreign service providers (i.e. those established or headquartered in a foreign country) or (ii) from local service providers (i.e. those established on domestic soil), where the data is physically stored remotely on a foreign server.

The former scenario arose when the Belgian Public Prosecutor requested Yahoo Inc. in 2008 to disclose subscriber data in relation to Yahoo email accounts supposedly used to commit and execute computer fraud and forgery affecting local residents located in Belgium.

The latter scenario arose in 2014, when Microsoft was ordered by a US court warrant to disclose content data physically stored on a data center located in Ireland operated by a wholly owned subsidiary of Microsoft.

Such powers to request communications data would be governed by the LEA's domestic law. For some states the exercise of these powers is restricted by statute for others it is not. This immediately raises serious concerns about the data subject's privacy, as privacy protections for communications data vary enormously between countries.

---

[26] Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access to data and jurisdiction: Options for further action by the T-CY. Report prepared by the Ad-hoc Subgroup on Transborder Access on Jurisdiction*. Adopted by the 12th Plenary of the TC-Y (2-3 December 2014) <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf>.

Therefore it is important to consider what the territoriality principle means for networked computing (in particular cloud computing) and law enforcement. The question to be answered is which is the most appropriate link to a territory to determine jurisdiction and it is argued here that there are four basic possibilities (with additional variations), which are illustrated in the following chart:

Data Subject's Country A	Territory of the person whose data is requested	Based on: -location when sending/transmitting -location when data is sought -domicile -nationality	Arguably accords with data subject's expectations of protection, but would restrict LEAs activities to local data subjects, which is an extremely narrow interpretation of the territoriality principle – may mean that privacy-friendly jurisdictions become a haven for cybercriminals, encouraging cross-border cybercrime providing victims with no protection	May be same as Country C or at least the same region as Country C; in a cloud computing environment data is frequently stored as local to users as possible in order to deal with data latency issues
Service Provider(s) Country B	Territory of establishment of the person/entity effectively controlling the data (being able to access and disclose)	May be more than one in different countries; in a cloud computing environment there may be a chain of different service providers May be none, if the data is encrypted by user	The data controller has *de facto* ability to control the relevant data; data subject may have a contractual relationship with that service provider (not always, eg sender of email stored by recipient's service provider); data controller may have to comply with data subject's law (eg EU Data Protection Directive 1995/46/EC)	May provide some protection for data subject, but in many scenarios it will not; service provider may be in any jurisdiction as services are provided remote; data subject/user may not be aware of location of service provider
Data Storage Country C	Territory of the location where the data is physically stored	May be single location; but also possibility that data spread over several server locations; sometimes impossible to	This is the traditionally recognized territorial link, since in the offline world control was at the	Likely to be close to the data subject and hence likely to provide~~r~~ better protection to the data subject than Country B

		determine even by the service provider	place of storage. Some element of control still exists at the physical location of a server (to put it drastically: that country could move in with bulldozers), but not necessarily direct access to data & disclosure	
Law Enforcement Authority Country D	Territory of the state investigating & prosecuting a crime; gathering intelligence	LEA proceeds under local domestic law; may be politically motivated, discriminatory or in breach of internationally recognized human rights standards	This has never been a recognised principle of territoriality and is the classic example of extraterritorial application of the law	Insufficient protection for data subject (the LEAs domestic protections, if any, may or may not apply to the data subject);- most efficient for law enforcement purposes and prevention of cross-border cybercrime

Having presented the different *theoretical* possibilities for law enforcement jurisdiction and potential connection factors to territory, the next section will briefly describe three case examples where either the courts have sanctioned direct law enforcement access to foreign communications data or the national legislation provides for direct law enforcement requests to foreign service providers.

The *Belgian Yahoo case* has been widely discussed and criticized.[27] This case concerned a criminal prosecution of fraud committed through the use of Yahoo email accounts. The Public Prosecutor requested subscriber information from Yahoo under Art 46bis of the Belgian Code of Criminal Procedure to identify the perpetrators of the fraud. Yahoo refused to comply with the request, arguing that the request must be served by US authorities under the Electronic Communications Privacy Act (ECPA). [28]

At the time, Yahoo did not have an office or-establishment in Belgium. At first instance, the Dendermonde Court ordered Yahoo to disclose the information requested in 2009 and resolved to levy a fine of EUR 55,000 and a EUR 10,000 penalty for each day of non-compliance. The Belgian Court found jurisdiction on the basis of commercial presence: Yahoo was commercially present in Belgium through the provision of internet services to

[27] See for example http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters and P de Hert, M Kopcheva, "International Mutual Legal Assistance in Criminal Law Made Redundnant" (2011) 27 *Computer Law & Security Review* 291-297

[28] For a synthesis of the scope of *ECPA*, see the website of the United states Department of Justice, Office of Justice Programs, available at: https://it.ojp.gov/default.aspx?area=privacy&page=1285.

persons located in Belgian territory. Yahoo appealed the case and after long and complex appealing proceedings, the Belgian Supreme Court[29] found on 4 September 2012 that the direct order requesting subscriber information sent by the Belgian Public Prosecutor had been validly made to Yahoo (upholding the original decision of 2009).[30]

In the final judgment of the Court of Appeals of Antwerp of November 20, 2013, the justices confirmed the opinion of the Court of First Instance of Dendermonde and found: (i) that Yahoo had a territorial presence in Belgium, (ii) that Yahoo is and should be considered a provider of electronic communications services within the meaning of Article 46 bis of the Code of Criminal Procedure, and therefore, (iii) that Yahoo should collaborate with investigative authorities in the facilitation of the information requested and (iv) levied a penalty of 44,000 euros against the company.[31]

In *Re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp*[32] the Magistrate ordered by way of a warrant under the Stored Communications Act[33] that Microsoft disclose the content of emails in connection with a criminal investigation, even though the emails were stored on a data center in Ireland by Microsoft's wholly owned subsidiary.[34] The court order was affirmed by the Federal District Court for Southern District of New York. Microsoft had already disclosed meta-data stored on its servers in the US but had refused to disclose content data physically stored in a data center located in Ireland, citing presumption against extraterritorial reach of laws. The Federal District Court did not accept this argument and held that this was not an extraterritorial application of the law, as it was sufficient that Microsoft had (remote) control over the data in the US.[35] A distinction was made between a "normal" search & seizure warrant which was limited by its nature to US territory[36] and a warrant under the Stored Communications Act which allows for electronic disclosure and is therefore more akin to a subpoena for the disclosure of documents which is not limited to US territory.[37]

Microsoft appealed the judgment of the Magistrate Judge of the United States District Court for the Southern District of New York on December 18, 2014 and the matter is yet pending to be decided in the United States Court of Appeals for the Second Circuit.[38]

---

[29] Supreme Court, September 4th, 2012, A.R. P.11.1906.N/2

[30] There was also an issue as to whether *Yahoo* was an electronic communication service provider, but this is not relevant for purposes of this paper.

[31] As of the time of the publication of this paper, the final judgment of the Court of Appeals of Antwerp is not final and it is still pending to be enforced against Yahoo in Belgium.

[32] 15 FSupp 3d 466 (S.D.N.Y 2014)

[33] 18 U.S.C. §§2701-2712

[34] 15 FSupp 3d 466, 477 (S.D.N.Y 2014)

[35] 15 FSupp 3d 466, 472 (S.D.N.Y 2014)

[36] Rule 41 Federal Rules of Criminal Procedure

[37] 15 FSupp 3d 466, 471 (S.D.N.Y 2014); see also Case Review in 128 *Harv. L.Rev 1019*

[38] See: Brief for Appellant in the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation on Appeal from the United states District Court for the Southern District of New York, (14-2985-cv December 18, 2014), available at: http://digitalconstitution.com/wp-content/uploads/2014/12/Microsoft-Opening-Brief-120820141.pdf

In the UK, new data retention legislation was passed in 2014. Section 4 of *the Data Retention Investigatory Powers Act* (DRIPA) provides for express extraterritorial powers for LEAs to make a direct request to foreign communication service providers without going through MLA procedures. These direct requests can be made in respect of interception of content, interception capabilities and meta- data. This legislation was rushed through the UK Parliament just before the summer break of 2014 and its provisions have been heavily criticized.[39] The government claims that the existing law already contained a power to request communications data from foreign service providers providing services to the UK and that this new Act only clarifies the position (for the protection of the participating communication service providers).[40]

As a matter of the analysis made in this section, we can conclude that there are sufficient legal precedents for LEAs to request communications data directly from foreign service providers or from local service providers where the data is stored on a foreign territory. Some states accept this practice while others differ and avoid conducting such practice, in other words there is not a uniform established accepted practice on cross-border access to data.. We strongly believe that there is a need to make a more detailed analysis of the conformity of this practice under the scope of international law and particularly, to consider the creation of an international standard or additional safeguards to protect privacy and data when LEAs deal with or conduct direct access to data in other countries.

The questions raised above suggest reviewing the traditional jurisdictional approaches from a more fundamental perspective. As one possible solution to these issues, the final section of the paper suggests considering alternative perspectives on jurisdiction.

3. Final Remarks

The use of Mutual Legal Assistance Mechanisms continue to generate controversy since most of those instruments are subject to the reciprocity of states, the cooperation of government authorities which is usually slow, and often delay or hampered the investigation for not having immediate access to data that could be used as evidence in a criminal investigation.

---

[39] See: The Guardian. *"Academics: UK 'Drip' data law changes are 'serious expansion of surveillance"* (15 July 2014) available at: http://www.theguardian.com/technology/2014/jul/15/academics-uk-data-law-surveillance-bill-rushed-parliament

[40] *Ibid*. See also Response by the Interception of Communications Commissioner Office (24 July 2014), available at: http://www.iocco-uk.info/docs/IOCCO%20response%20to%20new%20reporting%20requirements.pdf

Cross-border access to data and jurisdictional approaches are complex and difficult issues. Given the examples contained in this paper, it seems unlikely that states reach a mutually agreeable solution in the near future. The development and consensus on an Additional Protocol on Cross-Border Access to Data to the Convention against Cybercrime will be a lengthy process, and at its current stage of ambiguity, we do not believe that such instrument would help to improve the current practices of law enforcement authorities for accessing and securing data in foreign countries. One option to take these matters further is to provide additional guidance on the scope of interpretation of Article 32 of the Convention against Cybercrime with full attention to both, the operational needs of law enforcement as well as respect of fundamental human rights of privacy and data protection.

Examples of case law on LEAs' requests to foreign service providers shown in this paper suggest that States have a wide spectrum of possibilities to assert jurisdiction under international law, the national constitutional framework and local laws. The views hereby presented are real and may encourage states to combine and apply jurisdictional principles according to their own needs and not only focus solely in the application of the territoriality principle. We strongly believe that there is a need for a more detailed analysis of the legal limits of LEAs' requests to foreign service providers under the scope of international law. In particular, states should consider the creation of an international standard or a set of additional safeguards to protect privacy and data when LEAs deal with or conduct direct access to data in other countries.

The cross-border access to data debate will continue in the following years since it involves a number of controversial regulatory aspects for the states namely, national sovereignty issues, the use of MLA channels, conflicts of laws in the field of data protection and the protection of the fundamental right to privacy pursuant to the current international and regional instruments in the subject matter. With this in mind, we hope that the views presented in this paper will be helpful for further debates, and in particular to states, that need to be prepared to confront these issues on a more proactive and expeditious basis.