DOI 10.5817/MUJLT2015-1-4

MUTUAL LEGAL ASSISTANCE & OTHER MECHANISMS FOR ACCESSING EXTRATERRITORIALLY LOCATED DATA

by

ANNA-MARIA OSULA*

This article discusses the role of Mutual Legal Assistance (MLA) and other established mechanisms of international cooperation in the fight against cyber crime. The analysis is limited to mechanisms facilitating access to extraterritorially located data. After a brief account on the legal prerequisites of successful fight against cyber crime, the article proceeds to exploring both traditional as well as alternative cooperation mechanisms for transborder data access. Given the realistic assessment that the amount of digital evidence to be accessed extraterritorially will only increase with time, the article focuses on the difficulties in accessing data under the current MLA procedures. The article reiterates that States are in need for more time-effective measures for transborder data access. Unless the identified inefficiencies pertaining to MLA are addressed, the traditional focus on territoriality, and assuming the other State being the primary counterpart for carrying out investigative measures requiring transborder access to evidence, will continue to gradually shift to more operational mechanisms that do not necessarily require the prior authorisation of the State where the data is located.

KEY WORDS

Mutual Legal Assistance, Council of Europe, Convention of Cybercrime, Transborder Access, Cybercrime Investigations

* Anna-Maria Osula, PhD candidate at Tartu University Faculty of Law, Estonia; researcher at NATO CCD COE, Estonia; lecturer at Tallinn University of Technology, Estonia.

The views expressed herein are those of the author and do not reflect the policy or the opinion of any other entity.

1. INTRODUCTION

Cyber crime investigations are increasingly faced with complex jurisdictional puzzles where the victim, the perpetrator, the Service Provider (SP) and evidence may easily all reside in different jurisdictions.[1] Law enforcement agencies have long realised that the success of such cross-border investigations relies to a great degree on up to date legal and procedural frameworks as well as functional mechanisms for international cooperation. In particular, and not only for the fight against cyber crime but increasingly for any crime with transnational character or if involving evidence stored abroad, there is a need for timely measures accessing evidence that is located in foreign jurisdiction.

This article discusses the role of Mutual Legal Assistance (MLA) and other established mechanisms of international cooperation in the fight against cyber crime. The analysis is limited to mechanisms facilitating access to extraterritorially located data. After a brief account on the legal prerequisites of an effective fight against cyber crime, the article proceeds to exploring both traditional (such as MLA) as well as alternative cooperation mechanisms for transborder data access. Given the realistic assessment that the amount of digital evidence to be accessed extraterritorially will only increase with time, the article focuses on the difficulties in accessing data under the current MLA procedures. The article reiterates that States are in need of more time-effective measures for transborder data access. At the same time, these measures need to be in accordance with both national and international legal frameworks.

2. LEGAL PREREQUISITES FOR FIGHTING CYBER CRIME

An efficient fight against cyber crime requires a well-working interplay between a number of legal aspects. Foremost, successful investigation and prosecution rely on harmonised and up to date substantial and procedural criminal law. To that end, international attempts to harmonise different national criminal laws continue to be important in order to avoid situations where behaviour rendered legal in one jurisdiction is illegal in another, and

[1] According to United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf., "between 50 and 100 per cent of cybercrime acts encountered by the police involve a transnational element." xxv, 117–118.

thus may hinder prosecuting the case.[2] Equally, national law needs to empower law enforcement with necessary tools for carrying out modern investigations. In the case of more intrusive measures such as surveillance,[3] conditions for further authorisation of a competent authority must be regulated in a clear and transparent manner and undertaken in accordance with law in order to be admissible in court.

The investigative measures relevant for the purposes of this article pertain to obtaining extraterritorially located evidence. Channels for obtaining data located extraterritorially may be built on formal or informal relationships but must at all counts be in line with international law as well as supported by domestic legislation and accepted procedures. Among other restrictions, these measures need to take into account the boundaries set by jurisdiction that reflect the extent of a State's right to regulate the conduct or the consequences of events.[4] In the context of cyber crime, the interpretation and implementation of jurisdictional principles play a role in establishing jurisdiction for both prosecuting the offence (prescriptive jurisdiction, adjudicative jurisdiction) as well as for specific cross-border investigatory measures (jurisdiction to enforce). Although jurisdiction is primarily territorial, there may be grounds for its extraterritorial application.

While over the years a lot of research has been undertaken regarding the limits of prescriptive jurisdiction, the territorial scope of jurisdiction to enforce has received undeservedly little attention. In fact, it is the interpretation of the latter that is especially relevant for outlining the rules for accessing and obtaining data in foreign jurisdictions. This is because, according to international law, the exercise of jurisdiction to enforce on the territory of another State is permitted only if the latter provides consent to such behaviour (such as a based on a bi- or multilateral agreement) or such a right would be deriving from international customary law.[5] States failing to acquire consent for any 'exercising [of] power' on the foreign territory

[2] Marco Gercke, Understanding Cybercrime: Phenomena, Challenge and Legal Response (International Telecommunication Union, 2012), 82–83, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

[3] E.g. Estonia, Code of Criminal Procedure, Chapter 3 - Surveillance Activities, RT I, 29.06.2012, 2, entry into force 01.01.2013.

[4] L. Oppenheim, Oppenheim's International Law, 9th ed (London; New York: Longman, 1996), 456.

[5] The Case of the 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).

would possibly be acting contrary to the principle of non-intervention[6] and may violate the sovereignty of the States concerned.[7] A common way to avoid the possible breach of another State's sovereignty, if in need of evidence located extraterritorially or other support in transnational criminal matters, is basing the cooperation on MLA treaties and another cooperation mechanisms — and thus requiring the consent (usually of the other State) before exercising jurisdiction in another State's territory.

3. MUTUAL LEGAL ASSISTANCE AND OTHER INTERNATIONAL COOPERATION TREATIES FOR ACCESSING STORED DATA

International cooperation in criminal matters that, in addition to MLA, consist of a number of other cooperative measures has been developing significantly over last decades. Drivers for these developments have mainly been international communities or groups of likeminded States. For example, due to transnational organised crime, notably drug trafficking, the demands for international law enforcement were rapidly increasing during the 1970s and resulted in the initiation of supplementing the then common process of rogatory letters[8] with more flexible MLA treaties.[9]

In conjunction with relevant national legislation, requests for accessing extraterritorially stored data are mostly based on: bi-lateral agreements on MLA; or multilateral agreements such as the Council of Europe (CoE) Convention on Cybercrime, European Convention on Mutual Legal Assistance in Criminal Matters and other Council of Europe treaties, United Nations and other international treaties; or reciprocity.[10] Depending on the

[6] United Nations, Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations, A/RES/25/2625, 1970.

[7] Pierre Trudel, Jurisdiction over the Internet: A Canadian Perspective, in Int'l L., vol. 32, 1998, 1047.

[8] As noted by one author, using letters of rogatory for acquiring evidence from abroad slowed down the process considerably. He stated that the criminal act and the investigative process were running at totally different speeds, "instantaneous versus the forever!" Read more: David J. Davis, "Criminal Law and the Internet:The Investigator's Perspective," in Crime, Criminal Justice and the Internet, ed. Clive Walker and Andrew Ashworth (London: Sweet & Maxwell, 1998), 51–52.

[9] Ethan Avram Nadelmann, Cops Across Borders: The Internationalization of U.S. Criminal Law Enforcement (University Park, PA: Pennsylvania State University Press, 1993), chap. 6.

[10] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, December 3, 2014, 31, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf.

framework to be used and the countries being requested, the exact content and conditions for submitting as well as responding to the request differ.[11]

For example, MLA requests may have to be sent to a central authorising authority such as the Ministry of Justice, they may be forwarded directly to the relevant national authorities, or other channels such as INTERPOL may be used.[12] Also, the national bodies authorising, in response to a received MLA requests, domestic access to stored computer data may vary according to the type of data to be accessed (e.g. subscriber data, traffic data or content data).[13] Some countries also provide for more expedited procedures such as "in cases of urgency, a request for assistance submitted through the International Criminal Police Organisation (INTERPOL) or a notice in the Schengen Information System may be complied with before the request for assistance is received by the Ministry of Justice with the consent of the Office of the Prosecutor General."[14]

Two examples of international organisations that have attempted to provide for more uniform approaches for MLA regarding accessing extraterritorially stored computer data are the European Union and the Council of Europe.

3.1 EUROPEAN UNION

The European Union is far from enforcing a pan-European code of criminal procedure but is increasingly covering different aspects of pre- and post-trial measures that result in a certain harmonisation of criminal procedure across Member States.[15] The EU's criminal assistance has been largely built upon the framework of the Council of Europe Convention on Mutual Assistance in Criminal Matters[16], parts of the Schengen Convention[17], the

[11] Ibid.

[12] Ibid., 38.

[13] Ibid., 31–33.

[14] Ibid., 38; Estonia, Code of Criminal Procedure, para. 462, "Processing of requests for assistance received from foreign states".

[15] Samuli Miettinen, Criminal Law and Policy in the European Union, Routledge Research in European Union Law 3 (Abingdon, Oxon ; New York: Routledge, 2013), 176.

[16] Council of Europe, European Convention on Mutual Assistance in Criminal Matters, 1959, http://www.conventions.coe.int/Treaty/en/Treaties/Html/030.htm.

[17] The Schengen Acquis - Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at Their Common Borders, Official Journal L 239, 22.09.2000.

EU Convention on Mutual Assistance in Criminal Matters[18], and its Protocol.[19]

Developing a common approach for more effective investigations has developed in stages. In 2003, the EU addressed the need for immediate mutual recognition of orders to prevent the destruction, transformation, moving, transfer or disposal of evidence and adopted a Framework Decision outlining the rules under which a Member State recognises and executes in its territory a freezing order issued by a judicial authority of another Member State in the framework of criminal proceedings.[20] However, as this instrument is restricted to the freezing phase, a freezing order is required to be accompanied by a separate request for the transfer of the evidence to the State issuing the order in accordance with the rules applicable to mutual assistance in criminal matters; and such a two-step procedure has proven to be detrimental to its efficiency and seldom used in practice by the competent authorities.[21]

In 2008, the Council Framework Decision for the European Evidence Warrant was adopted to further improve judicial co-operation by applying the principle of mutual recognition to a judicial decision for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters.[22] However, the instrument has been criticised as having a limited scope since it only applies to evidence which already exists and thus is not being as useful to the investigators.[23]

In 2009, the Stockholm Programme proposed setting up a comprehensive system for obtaining evidence in cases with a transborder dimension that would be based on the principle of mutual recognition, and

[18] Council of the European Union, Council Act of 29 May 2000 Establishing in Accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000.

[19] Council of the European Union, Council Act of 16 October 2001 Establishing, in Accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ 326, 21.11.2001.

[20] Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the European Union of Orders Freezing Property or Evidence, OJ L 196, 2.8.2003, para. 1.

[21] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 3.

[22] European Union, Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters, OJ L 350, 30.12.2008.

[23] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para 4.

would thereby tackle the EU's fragmented approach to evidence gathering.[24] Respectively, the EU adopted in 2014 a Directive on the European Investigation Order in criminal matters that outlines a framework for a judicial authority of one Member State to "have one or several specific investigative measure(s) carried out in another Member State" in order to obtain evidence.[25] In addition to the Directive, the EU Member States can also use Joint Investigative Teams.[26] The Directive is indeed a significant step forward since it indicates a gradual shift from the mutual legal assistance mechanisms (where the requested Member State has a wide discretion to comply with the request of another Member State) into a mutual recognition mechanism (where each Member State must in principle recognise and execute a request coming from another Member State).[27,28] However, in the context of transborder access, the Directive does still not solve the need for time-critical access to transborder data during an investigation because the Directive foresees 90 days as the allowed timeframe for responding to such requests.[29]

3.2 COUNCIL OF EUROPE

The only international treaty that includes provisions regarding mutual MLA, specifically in cyber crime cases, is the Council of Europe (CoE) Convention on Cybercrime. In addition to inviting its Parties to provide each other mutual assistance to the widest extent possible (Article 23 and Article 25 p 1), the Convention also outlines procedures to be used for mutual assistance requests in the absence of an applicable international agreement (Article 27 and Article 28). With the aim to address the volatile nature of electronic evidence, specific provisions also encourage 'expedited'

---

[24] European Union, "The Stockholm Programme - An Open and Secure Europe Serving and Protecting the Citizen 2010/C 115/01" (Council of the European Union, December 2, 2009), OJ C 115 4.5.2010.

[25] Importantly, as of 22 May 2017, this Directive will replaces most of the existing laws in the area of transferring evidence between Member States in criminal cases. Europan Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 1 (1).

[26]'Joint Investigation Teams (JITs),' https://www.europol.europa.eu/content/page/joint-investigation-teams-989.

[27] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 12.

[28] Steve Peers and Emilio De Capitani, 'EU Law Analysis: The European Investigation Order: A New Approach to Mutual Recognition in Criminal Matters,' Blog, EU Law Analysis, (May 23, 2014), http://eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html.

[29] Europan Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 12 (4).

means of communication (Article 25 p 3), use of 24/7 networks (Article 35) and sharing spontaneous information (Article 26). Notably, the Convention includes options for expedited preservation of stored computer data where the other Party is requested to preserve information stored in its territory before the mutual assistance request has been formally submitted (Article 29). Besides allowing for the provision on expedited disclosure of preserved traffic data (Article 30), the Convention also provides for 'mutual assistance regarding accessing of stored computer data' (Article 31).

Article 31 is one of the principal legal constructs informing Parties about options to access, under mutual assistance, data stored extraterritorially. It allows for requesting the other Party to 'search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29' (Article 31 p 1). Importantly, the provision also allows requests for such assistance on an expedited basis where 'there are grounds to believe that relevant data is particularly vulnerable to loss or modification' or there are other legal grounds for providing for expedited co-operation (Article 31, 3a). Unfortunately, there are currently no statistics of the frequency of the use of mutual assistance to access stored computer data amongst the Parties to the Convention; one of the main reasons for this is the increasingly decentralised nature of mutual legal assistance where a growing amount of requests are sent or received directly between relevant judicial authorities and not only via central authorities.[30]

4. ASSESSMENT OF THE MLA SYSTEM

According to the United Nations, approximately 70% of the means of international cooperation in cyber crime investigations are based on traditional MLA.[31] Although a uniform approach to MLA treaties' format, content or other requirements is lacking, in some countries only the material received via MLA, as opposed to data being obtained via alternative channels, can be used as evidence in court.[32] In others, the national legislation offers more flexibility and requires accessing only certain types

[30] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 6.

[31] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, 201.

[32] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 7.

of data (such as content data) through a formal MLA request.[33] There are also countries that do not put forward a detailed regulatory framework and only require the evidence to be gathered in accordance with the legislation of the other State and not to be in conflict with the principles of domestic criminal procedure.[34] In any case, the high percentage of the reported use of MLA is in contrast with the characteristics of the MLA procedures that generally do not satisfy the needs of modern time-critical cyber crime investigations.[35]

In the context of accessing extraterritorially stored computer data, MLA procedures have been deemed to have a number of weaknesses. According to a recent CoE study, MLA is considered "too complex, lengthy and resource intensive" and thus often abandoned.[36] Indeed, MLA may take up to months or even years for the requested evidence to reach the requesting State.[37] In addition to the inherent slowness of MLA procedures, they may always not cover required investigative measures. There may be situations where there is no MLA treaty in place, the other State is simply uncooperative, accessing the data is urgent in order to avoid it being destroyed or where it is impossible to identify the jurisdiction of the data altogether (e.g. due to the characteristics of cloud computing).[38] Further problems include refusals to cooperate for "small" offences, lack of information from the requested country about the receipt or the status of the request, problems with the content of the requests (too broad, unclear criteria for urgent requests, problems with language, terminology) and differences in legal systems.[39] Taking into account all of the above, it is no surprise that the CoE has concluded, based on responses from 39 States, that the MLA process is considered inefficient in general and with respect to obtaining electronic evidence in particular.[40] Individual States have also

[33] Ibid.

[34] Estonia, Code of Criminal Procedure, para. 65 (1).

[35] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 38–39.

[36] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 123.

[37] Ibid., 39.

[38] New Zealand and Law Commission, Search and Surveillance Powers (Wellington, N.Z.: Law Commission, 2007), 226.

[39] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 38–39.

[40] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 123.

acknowledged that current mutual assistance arrangements may not be 'sufficiently tailored to facilitate intangible evidential material being efficiently collected from other jurisdictions.'[41]

At the same time, according to the CoE, the Parties to the Convention appear not to be making full use of the opportunities offered by the Convention and other specific agreements.[42] A set of recommendations for both Parties and other relevant entities on how to improve MLA in the context of accessing stored computer data has therefore been proposed by the CoE. Keeping in mind that MLA does foresee procedures that are in the interests of the sovereign States since they allow for certain transparency and overview of the activities of law enforcement targeting data stored on foreign territory, States should show more initiative in updating bilateral MLA treaties or reaching a consensus on more effective multilateral terms. In addition to MLA, alternative cooperation mechanisms must be considered.

5. ALTERNATIVE COOPERATION MECHANISMS

It must be reiterated that States are in need of more effective investigatory mechanisms for fighting against cyber crime, and several formal and informal alternatives for transborder data access have already emerged or are currently under discussion. These approaches for accessing and obtaining data as part of an investigation from a foreign jurisdiction can be roughly divided into two groups.

5.1 ALTERNATIVE COOPERATION MECHANISMS INVOLVING THE STATE WHERE THE DATA RESIDES

The first group consists of formal and informal mechanisms that guide the cooperation between the law enforcement of two or more countries and, thus, involve formal or informal State authorisation in allowing for the requesting entity to access the data

In addition to the already mentioned MLA, informal cooperation between law enforcement of different countries is a frequent measure for sharing data related to cybercrime. Generally, law enforcement cooperation is aimed at exchanging information that could lead to the commencement of

[41] New Zealand and Law Commission, Search and Surveillance Powers, 227.

[42] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 123.

criminal proceedings even if, in many cases, the information obtained through such alternative cooperation cannot be used as evidence in criminal proceedings.[43]

States have diverse rules as to what data may be shared with other counterparts without the MLA framework.[44] For example, some countries may share specified traffic and subscriber data for investigative purposes, others may share subscriber information based on reciprocity, while there are also States that are able to share only data that can be obtained domestically by the police without compulsory measures and thus without court order.[45] It has been thus proposed that the opening of a domestic investigation following a foreign request or spontaneous information should facilitate the sharing of information without MLA, or even accelerate MLA.[46]

As also proposed by the CoE Convention, 24/7 networks are maintained and used,[47] and spontaneously disclosing information to the foreign law enforcement "where it appears relevant to conduct seemingly connected to the foreign territory, rather than waiting for the foreign LEA to commence an investigation and initiate a formal MLA request" is encouraged.[48] Also, for complex international cases, the frameworks of Europol, Eurojust or Interpol are employed, as well as joint investigation teams, or law enforcement liaison officers or networks.[49]

5.2 ALTERNATIVE COOPERATION MECHANISMS NOT INVOLVING THE STATE WHERE THE DATA RESIDES

The second group of mechanisms for accessing and obtaining extraterritorial data by law enforcement is characterised by a certain extent of "sidestepping" the State as the determining factor for the location of the

[43] It must be noted that the distinction between police-to-police cooperation and MLA is not always very clear. Read more Ibid., 7–8.

[44] Ibid., 8.

[45] Ibid.

[46] Ibid.

[47] Except for the use of MLAs, however, these methods are under-utilised and handle only approximately 3 percent of the cyber crime cased confronted by LEAs. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, xxv. About the role of 24/7 contact points pertaining to mutual legal assistance for accessing stored computer data, see Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 88–89.

[48] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 9–10.

[49] Ibid., 91.

data, and thus not always asking for nor requiring the authorisation of any of the formal State entities.

Examples of such a way forward include directly contacting the SP, accessing data publicly available, accessing data with the consent of the 'lawfully authorized entity' and directly accessing the data either knowing on unknowing its physical location. Whereas there is emerging evidence of State practice as well as developments in international organisations supporting such mechanisms, the approaches to regulating law enforcement's mandate for accessing and acquiring the data are largely divided and not sufficiently outlined in national legislation. Also, it is clear that the use of such measures decreases the control of the sovereign State over the foreign law enforcements' requests as well as activities for accessing evidence stored in its own territory.

It is not uncommon that law enforcement would directly request the foreign SP to disclose the necessary data.[50] Such cooperation can be based on the terms and conditions provided to the users that often clearly state that data may be shared with law enforcement under specific circumstances.[51] SPs may require due legal process for data disclosure, or they may under some circumstances comply voluntarily with direct law enforcement requests.[52] Some SPs such as Ebay and Facebook even have dedicated portals for facilitating such exchanges.[53] At the same time, there are on-going legal debates whether the SP is in the position to provide the foreign law enforcement the requested data or whether this would require a separate MLA request.[54]

---

[50] Ian Walden, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, November 14, 2011), 55, http://papers.ssrn.com/abstract=1781067; Micheál O'Floinn, 'It Wasn't All White Light before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe,' Computer Law & Security Review 29, no. 5 (October 2013): 611. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, xxii–xxiii.

[51] Simon Bradshaw, Christopher Millard, and Ian Walden, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services,' International Journal of Law and Information Technology 19, no. 3 (September 21, 2011): 187–223.

[52] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, xxii–xxiii.

[53] E.g. eBay Inc., "Law Enforcement eRequest System," accessed June 1, 2014, https://lers.corp.ebay.com/AIP/portal/home.do; Facebook, "Law Enforcement Online Requests," accessed June 1, 2014, https://www.facebook.com/records/x/login/ quoted in O'Floinn, "It Wasn't All White Light before Prism," 611.

[54] United States District Court, In the Matter of a Warrant to Search a Certain E-mail Account: Controlled and Maintained by Microsoft Corporation (2014); 2012/CO/1054 Yahoo! Inc (Court of Appeal of Antwerp, 12th chamber for criminal cases 2013).

The CoE's Convention of Cybercrime Article 32 is another basis for accessing extraterritorially located data with consent (Article 32 (b)) or where publicly available (Article 32 (a)). For the purposes of accessing data not publiclz available and stored extraterritorially, Article 32 (b) is especially relevant. It allows parties to 'access or receive through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.'[55] This clause in particular has whirled up a lot of controversy, leading to some countries indicating this as a reason not to join the Convention.[56] Problematically, Article 32 (b) could be interpreted as to allow for remote search and seizure,[57] albeit with a lot of confusion as to the exact conditions for such an investigative measure. Fuelling the sensitivity of this clause, the explanatory memorandum does not fully clarify the exact meaning of the terms and concepts put forward in the clause. Given that the current wording is not clear about the exact meaning of the 'lawful authority', some commentators suggest that the provision in its current wording probably contradicts fundamental principles of international law since law enforcement is not allowed to carry out investigations in another State without the consent of the competent authorities in that State.[58] It has been noted that the decision whether such investigative measures should be allowed should not be dependent on the authorisation of an individual but should remain with the States, also for purposes for overall transparency.[59] Neither have the wording or the procedures for the investigation been fully clarified by the CoE Guidance Note on the interpretation and implementation of Article 32.[60] The guidance note does, however, confirm that Article 32 (b) is an exception to the principle of territoriality in the sense

[55] Council of Europe, Convention on Cybercrime, vol. ETS No. 185, 2001, para. 32(b), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[56] Keir Giles, 'Russia's Public Stance on Cyberspace Issues,' in 2012 4th International Conference on Cyber Conflict, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (NATO CCD COE Publication, 2012), 66–67, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.

[57] Ian Walden, Computer Crimes and Digital Investigations (Oxford; New York: Oxford University Press, 2007), 319.

[58] Gercke, Understanding Cybercrime: Phenomena, Challenge and Legal Response, 277.

[59] Ibid., 278. See also Nicolai Seitz, \Transborder Search: A New Perspective in Law Enforcement,' Yale JL & Tech. 7 (2004): 40.

[60] Cybercrime Convention Committee, '(T-CY) Guidance Note #3 Transborder Access to Data (Article 32)', 3 December 2014.

that it permits 'unilateral transborder access without the need for mutual assistance under limited circumstances.'[61]

In an attempt to address MLA inefficiencies, and building on examples of national legislations allowing for transborder access (also known as 'direct access') under certain conditions, the CoE also proposed in 2013 the adoption of Additional Protocol to the Convention on Cybercrime regarding transborder access to data.[62] However, due to lack of consensus on the way forward, the CoE concluded in 2014 that the 'negotiation of a Protocol on transborder access to data would not be feasible'.[63]

6. DISCUSSION

As an increasing number of crimes involve geo-distributed electronic evidence, transborder access to data is relevant not only for cyber crime but for all crimes in general. Previous sections have introduced different cooperation mechanisms used for transborder access to evidence. Mechanisms such as MLA and the informal cooperation between law enforcement entities generally rely on the authorisation of the other State before gaining access to the data. Such mechanisms are therefore being guided by the territoriality principle that focuses, as the principal counterpart of the investigation, on the country in whose territory the data being sought resides. Thereby, the sovereignty of the other State is not being breached and the State remains in control of the investigative measures being carried out on its territory or pertaining to the data located on its territory.

Despite the frequent use of MLA, the article has indicated a number of factors that do not render the MLA framework as entirely suitable for the time-critical access to extraterritorially located data. Notwithstanding the fact that the efficiency of MLA procedures in accessing extraterritorially located data has been criticised for years, little concrete improvement can be observed. Examples of two organisations actively seeking to provide better

[61] Ibid.

[62] Council of Europe Cybercrime Convention Committee (T-CY), (Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data, April 9, 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2914transb_elements_protocol_V2.pdf.

[63] Council of Europe Cybercrime Convention Committee (T-CY), Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY, December 3, 2014, 12–13, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf.

condition for transborder access are the EU and the CoE. While the developments in both organisations such as the EU's Directive on the European Investigation Order and the option for Joint Investigative Teams as well as the CoE's work on analysing options for transborder access and carrying out an extensive study on MLA procedures must be commended, their efforts do not address the full spectrum of challenges to transborder access.

The alternative measures introduced in this article include contacting directly the SP (such as exemplified by the quoted Microsoft and Yahoo! cases) or practicing 'direct' transborder access (such as allowed by the CoE Convention Article 32 or under certain circumstances, by some national legal frameworks). In fact, it has been reported that law enforcement authorities may, in practice, either with or without the knowledge of investigators, directly access extraterritorial data without the consent of either a 'person with lawful authority' (as stated in the CoE Convention Article 32 (b)) or the SP, and in many cases not knowing in which exact jurisdiction that data might reside.[64] An example of such a case is where investigators can make use of an existing live connection from a suspect's device such as a computer or mobile phone or where investigators use lawfully obtained data access credentials to access cloud data.[65] This reality, even if not officially acknowledged or supported by the majority of governments, is reinforcing the argument that technological change, the increase in sophisticated threats and the need to redress harmful local effects of malicious offshore activities can be seen as altering the extraterritorial influence of purely territorial action.[66]

However, even if in some cases used in practice, these mechanisms do not assume the central role of the State where the data is located. Instead of focusing on territoriality, these measures prioritise quick access to the evidence. In addition to raising the obvious question of violating the sovereignty of the other State, such access may also raise data protection and privacy concerns of the individuals whose data has been accessed.

---

[64] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, 222.

[65] Ibid.

[66] Jack Goldsmith, 'The Internet and the Legitimacy of Remote Cross-Border Searches,' in The University of Chicago Legal Forum, Forthcoming, 2001, 7, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732.

Thus, since the need for more operational tools in the fight against cyber crime will not decrease, countries will have to actively look for solutions.[67] Generally speaking, countries are facing two main courses of action that do not necessarily contradict each other.

Firstly, countries may take steps towards finding consensus on the use of alternative measures for accessing transborder data, such as reflected in the work undertaken by the CoE. This would, however, require wider discussions and possibly reaching common ground on a number of interrelated issues that broadly touch upon the '(re)-conceptualization of the extent to which 'data location' can still be used as a guiding principle',[68] especially in circumstances where the exact location of the data cannot be identified. To do that, the debates on the interpretation of the limits of territorial sovereignty that would allow for, under certain circumstances, direct access to the data or the SP without the prior authorisation of the other State must be revisited. Also, the extraterritorial scope of jurisdiction must be addressed, especially as regards to examples recently adopted national legislation such as Brazil announcing its laws apply to companies that collect, store, retain or process personal or communications data whenever at least one of these activities occurs in Brazilian territory, also applying to every piece of data collected domestically as well as communication content whenever at least one of the terminals involved in the traffic is located in Brazil, and also in situations where the service is offered to the Brazilian public or when the provider has a branch in that country.[69]

Foremost, transparency is needed concerning States' official positions in such legal assessments together with examples of accepted State practice. Without sharing these with the international community, concrete agreements for further options for transborder access will be doubtful.

Secondly, and assuming that this would be the preferred choice of States keen to protect its sovereignty, States may support the reform of current MLA procedures.[70] This appears not to be an easy process since, despite the clear need for more effective investigative tools, States have largely

[67] For a comprehensive set of possible solutions, see Gail Kent, 'Sharing Investigation Specific Data with Law Enforcement - An International Approach,' Stanford Public Law Working Paper, February 14, 2014, http://ssrn.com/abstract=2472413.

[68] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, 223.

[69] Brazil, Presidency of the Republic, Law No. 12.965, April 23rd 2014, Article 11; Francis Augusto Medeiros and Lee A Bygrave, 'Brazil's Marco Civil Da Internet: Does It Live up to the Hype?' (2015) 31 Computer Law & Security Review, 127.

refrained from open discussions on how to enhance these traditional frameworks. It is unclear what the motivation of the States would be to avoid agreeing on more clear rules for more effective international cooperation. Perhaps one of the reasons could be the general lack of statistics related to cyber crime (lack of reporting, lack of initiating prosecution, lack of statistics on the use of different cooperation measures) and, hence, the insufficient underlining of the urgency of dealing with these issues. Assuming, however, that the gap in awareness will be bridged, an initiative could be taken, or efforts continue to be pursued, by international organisations such as the EU or the CoE or a group of likeminded States. Of course, such geographically restricted agreements would have their limitations regarding global cooperation but would nevertheless set an example of effective and transparent measures to other States and encourage them to follow the lead.

7. CONCLUSION

This article has discussed the role of MLA and other established mechanisms of international cooperation in the context of facilitating access to extraterritorially located data. International cooperation mechanisms for accessing extraterritorially located data were divided into two groups. Firstly, there is a group of mechanisms such as MLA, which is being used most frequently, and informal cooperation between law enforcement entities that generally rely on the authorisation of the other State before gaining access to the data. Secondly, there are alternative mechanisms such as contacting the SP or directly accessing the data that do not assume the central role of the State where the data is located but rather prioritise quick access to the evidence. As highlighted above, both of these groups of mechanisms have their own pros and cons.

However, MLA, as the most frequently used means for accessing extraterritorially located data, has proven to be largely unsuitable for the volatile nature of electronic evidence. The article concludes that unless the identified inefficiencies pertaining to MLA are addressed, the traditional focus on territoriality and assuming the other State being the primary counterpart for carrying out investigative measures requiring transborder

[70] A comprehensive list of proposals has been put forvard by Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime.

access to evidence will continue to gradually shift to more operational mechanisms that do not necessarily require the prior authorisation of the State where the data is located. However, distancing from formal MLA will bring along challenges regarding the transparency of criminal investigations and decrease the control of the sovereign State over investigations and their conditions regarding the data residing in their territory.

For finding a common ground between States, and overcoming the inconclusive state of international law, viable options and conditions for transborder access should be addressed in open discussions where States share their legal assessments together with examples of accepted State practice. These discussions could be facilitated, and continue to be supported, by international organisations such as the EU or the CoE.

LIST OF REFERENCES

Bradshaw, S., Millard, C., Walden, I., 2011. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Int. J. Law Inf. Technol. 19, 187–223.

Brazil, Presidency of the Republic, Law No. 12.965, April 23rd 2014.

Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003).

Council of Europe, 2001. Convention on Cybercrime.

Council of Europe, 1959. European Convention on Mutual Assistance in Criminal Matters.

Council of Europe Cybercrime Convention Committee (T-CY), 2014a. The mutual legal assistance provisions of the Budapest Convention on Cybercrime (No. T-CY(2013)17rev (Provisional)).

Council of Europe Cybercrime Convention Committee (T-CY), 2014b. Transborder access to data and jurisdiction: Options for further action by the T-CY (No. T-CY (2014)16 (Provisional)).

Council of Europe Cybercrime Convention Committee (T-CY), 2013a. T-CY Guidance Note #3: Transborder access to data (Article 32), Draft for discussion.

Council of Europe Cybercrime Convention Committee (T-CY), 2013b. (Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data (No. T-CY (2013)14).

Council of the European Union, Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000).

Council of the European Union, Council Act of 16 October 2001 establishing, in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 326, 21.11.2001).

Court of Appeal of Antwerp, 12th chamber for criminal cases, 2012/CO/1054 Yahoo! Inc, 2013.

Davis, D.J., 1998. Criminal Law and the Internet: The Investigator's Perspective, in: Walker, C., Ashworth, A. (Eds.), Crime, Criminal Justice and the Internet. Sweet & Maxwell, London.

eBay Inc., Law Enforcement eRequest System, available at: https://lers.corp.ebay.com/AIP/portal/home.do (accessed 11.06.15).

Estonia, Code of Criminal Procedure, RT I, 30.12.2014, 9.

Europan Union, 2014. Directive of the European Parliament and of the Council of regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014).

Europan Union, 2008. Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (OJ L 350, 30.12.2008).

European Committee on Crime Problems, Council of Europe, 1990. Computer-Related Crime: Recommendation no. R. (89) 9 on Computer-Related Crime and Final Report of the European Committee on Crime Problems. Council of Europe, Pub. and Documentation Service; Manhattan Pub. Co., Strasbourg: Croton, N.Y.

European Union, 2009. The Stockholm Programme - An open and secure Europe serving and protecting the citizen (OJ C 115, 4.5.2010).

Facebook, Law Enforcement Online Requests, available at: https://www.facebook.com/records/x/login/ (accessed 11.06.15).

Gercke, M., 2012. Understanding Cybercrime: Phenomena, Challenge and Legal Response. International Telecommunication Union.

Giles, K., 2012. Russia's Public Stance on Cyberspace Issues, in: C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012 4th International Conference on Cyber Conflict. NATO CCD COE Publications.

Goldsmith, J., 2001. The Internet and the Legitimacy of Remote Cross-Border Searches, in: The University of Chicago Legal Forum.

Joint Investigation Teams (JITs), available at: https://www.europol.europa.eu/content/page/joint-investigation-teams-989 (accessed 11.06.15).

Kent, G., 2014. Sharing Investigation Specific Data with Law Enforcement - An International Approach. Stanf. Public Law Work. Pap.

Medeiros, F.A., Bygrave, L.A., 2015. Brazil's Marco Civil da Internet: Does it Live up to the Hype? Comput. Law Secur. Rev. 31, 120–130.

Miettinen, S., 2013. Criminal Law and Policy in the European Union, Routledge Research in European Union law. Routledge, Abingdon, Oxon; New York.

Nadelmann, E.A., 1993. Cops Across Borders: the Internationalization of U.S. Criminal Law Enforcement. Pennsylvania State University Press, University Park, PA.

New Zealand, Law Commission, 2007. Search and Surveillance Powers. Law Commission, Wellington, N.Z.

O'Floinn, M., 2013. It Wasn't all White Light before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe. Comput. Law Secur. Rev. 29, 610–615.

Oppenheim, L., 1996. Oppenheim's International Law, 9th ed. Longman, London; New York.

Peers, S., De Capitani, E., 2014. EU Law Analysis: The European Investigation Order: A new approach to Mutual Recognition in Criminal Matters. Blog, EU Law Analysis, (May 23, 2014), available at: http://eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html.

Seitz, N., 2004. Transborder Search: a New Perspective in Law Enforcement. Yale JL Tech 7, 23.

The Case of the S.S. Lotus, Fr. v. Turk., 1927 P.C.I.J. (ser. A) No. 10, at 4 (Decision No. 9), 1927.

The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French

Republic on the gradual abolition of checks at their common borders, 1985 (OJ L 239, 22.09.2000).

Trudel, P., 1998. Jurisdiction over the Internet: A Canadian Perspective, in: Int'l L,32.

United Nations, 1970. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/25/2625.

United Nations Office on Drugs and Crime, 2013. Comprehensive Study on Cybercrime.

United States District Court, 2014. In the Matter of a Warrant to Search a Certain E-mail Account: Controlled and Maintained by Microsoft Corporation.

Walden, I., 2011. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (SSRN Scholarly Paper No. ID 1781067). Social Science Research Network, Rochester, NY.

Walden, I., 2007. Computer crimes and digital investigations. Oxford University Press, Oxford; New York.