Sofie Depauw[*]

Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0?

Abstract

This article aims to analyse the recent developments with regard to the collection for criminal justice purposes of electronic evidence, and more precisely, content data, in Europe. Firstly, a brief historical overview of the EU's action in the context of judicial cooperation in criminal matters (both in general and with regard to evidence) is provided. Secondly, electronic evidence itself and the legislation as it stands today will be discussed, followed by an assessment of the actions that have been taken by both the Council of Europe (CoE) and the European Union (EU) to overcome the difficulties faced by both public (law enforcement authorities) and private actors (service providers). The article evaluates the extent to which current discussions and proposals can be considered a step forward in light of the technological and judicial reality.

I. The EU's good governance responsibility applied to electronic evidence gathering

Ever since Giscard d'Estaing launched the idea of an 'espace judiciaire européen' in 1997, judicial cooperation in criminal matters in the EU has not been the same. Despite a few cracks in the pavement,[1] the 1990 Schengen Implementation Convention gave way for the first provisions on mutual legal assistance in criminal matters.[2] The free movement ideal that promoted border crossing was no longer a mere economic term,

* Sofie Depauw is a PhD-researcher at the Institute of International Research on Criminal Policy (IRCP, Ghent University). She focuses on the development of minimum standards for criminal investigation measures in the field of forensics (including electronic evidence) in order to ensure admissibility of investigation results as evidence in court. This paper was presented at the International conference: "Freedom Under Pressure", at the occasion of the 200-year anniversary of Ghent University. It was discussed during the panel session "Free movement and cross-border crime and criminal justice" organized by Prof. dr. Wendy De Bondt.

1 The agreements related to (1) the application of *non bis in idem* (1987), the transfer of sentenced persons (1987), the transmission of extradition requests (1989), the transfer of prosecution (1990) and the enforcement of foreign judgments (1991) never fully entered into force. None of these instruments thus related to mutual legal assistance.

2 Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Ger-

DOI: 10.5771/2193-5505-2018-1-62

but required the inclusion of a crime-fighting aspect. With the 1997 Amsterdam Treaty[3] that the idea of establishing EU level minimum standards to streamline cross-border crime-fighting was introduced. These minimum standards were considered acceptable to the extent approximation of domestic laws was necessary to avoid legal safe havens.[4] Initially the EU approximation competence was limited to substantive criminal law, i.e. adopting minimum rules regarding the constituent elements of certain offences and sanctions. It was not until the adoption of the Lisbon Treaty that the scope was broadened.[5] The Treaty allowed for the adoption of minimum rules concerning the mutual admissibility of evidence between member states "*to the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension*".[6] In doing so, the concept of free movement of evidence found its origin: not only people, capital and services should be able to move freely through the EU without being hindered by the national borders, the same should be true for evidence collected in the course of a criminal proceeding. The minimum standards regarding evidence gathering were considered necessary to ensure the mutual admissibility thereof; when collected in line with the minimum standards, the evidence would be admissible in all EU member states.

Despite the option foreseen in the Lisbon Treaty, and the despite the logic that all efforts to gather evidence may prove pointless if their admissibility is not ensured, the realisation of the idea proved exceptionally difficult. As it turned out, the sensitivity of the national character of legal rules on the gathering and use of evidence, together with the differences in legal systems and traditions, has hindered the establishment of an approximation instrument. Nevertheless, the thought of a free movement of evidence

many and the French Republic on the gradual abolition of checks at their common borders, OJ 2000 L 239/19.

3 Treaty of Amsterdam of amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ 1997 C 340/115.

4 Stockholm Programme – An open and secure Europe serving and protecting citizens, OJ 2010 C 115/14 (hereafter Stockholm Programme).

5 Treaty on the functioning of the European Union, 13 December 2007, Lisbon (hereafter TFEU).

6 Art. 82.2 TFEU.

continued to intrigue both scholars[7] and European institutions[8]. Following the 2010 study conducted at Ghent University, new light was shed on mutual admissibility of evidence. More specifically, it was concluded that the consensus on this admissibility depended on the inclusion of member states' fundamental principles of law in the minimum standards. From a judicial point of view, as argued before, these fundamental principles had to comprise, on the one hand, the procedural rules limiting states' competences to execute an investigative measure, and on the other hand, the procedural safeguards for the individual involved when the measure was executed.[9] For house search and telephone tapping, this led to a great variety of rules on limitations with regard to, amongst others, who could execute the investigative measure (limitation *ratione auctoritatis*) and the geographical scope of the measure (*ratione loci*).[10] In this context, *Kusak* also shed light on the interpretation of important procedural safeguards, such as the right to be notified and the right to legal remedies.

In 2010, the Stockholm programme linked the idea of minimum standards for mutual evidence admissibility to the forensic field, stating that a more effective European law enforcement cooperation was necessary "*to combat forms of crime that have typically a cross-border dimension*", and on the other hand that the Commission should "*agree on common quality standards within the forensic field, inter alia, to develop best practice for crime scene investigations*".[11] One of the forensic evidence types with a clear cross-border dimension is electronic evidence. A number of recent events (cf. discussions with Apple and Yahoo)[12] pointed out that there is need for a more solid framework on the collection of electronic evidence in criminal matters. Policy-makers

7 *L. Bachmaier Winter*, European investigation order for obtaining evidence in the criminal proceedings. Study of the proposal for a European directive, Zeitschrift für Internationale Rechtsdogmatik, 2010, p. 580 et seq.; *J.R. Spencer*, The Green Paper on obtaining evidence from one Member State to another and securing its admissibility: the Reaction of one British Lawyer, Zeitschrift für Internationale Rechtsdogmatik, 2010, p. 602 et seq.; *S. Allegrezza*, Critical remarks on the Green Paper on obtaining evidence in criminal matters from one member state to another and securing its admissibility, Zeitschrift für Internationale Rechtsdogmatik 2010, p. 569 et seq.; *S. Depauw*, A European evidence (air)space? Taking cross-border legal admissibility of forensic evidence to a higher level, European Criminal Law Review, 2016, p. 82 et seq.; *M. Kusak*, Mutual admissibility of evidence in criminal matters in the EU. A study of telephone tapping and house search, 2016, Maklu p. 17 et seq.

8 Consideration 3.3. Stockholm Programme; Paragraph 1, 4 Communication of 20 April 2010 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions –Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme, COM (2010) 171 final (hereafter Action Plan on the Stockholm Programme); Report on data protection in gathering and using electronic evidence, 2015, http://www.evidenceproject.eu/the-activities/deliverables.html, p. 135 et seq. (hereafter Report on data protection).

9 *S. Depauw* (fn. 8), p. 82-98.

10 *M. Kusak* (fn. 8), p. 17 et seq.

11 Consideration 4.3.1., para 1 and 3, 7th – Stockholm Programme (fn. 5).

12 https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone; see also https://www.stibbe.com/en/news/2014/july/court-of-appeal-of-antwerp-confirms-yahoos-obligation-to-cooperate-with-law-enforcement-agencies.

share the point of view that cybercrime is a core priority requiring immediate various EU level actions, varying from cooperation with the private sector to the exchange of best practices between actors involved.[13] Recent action plans to respond to the current terrorism threats also address the need for support for the law enforcement and judicial authorities.[14]

Despite the wide range of issues with electronic evidence, this article will only focus on the obstacles in procedural rules and safeguards for free movement of electronic evidence. More specifically, this relates to tackling of issues of competent jurisdiction and rules on access to evidence obstacles to criminal investigations on cybercrime.

II. E-evidence today: Windows '98 of judicial cooperation

A. Increased/renewed attention for electronic evidence

In recent years, both the EU and the CoE have identified electronic evidence as a priority to be tackled. On an EU level, the European Commission did so in the 2015 Agenda on Security, stating that gathering electronic evidence and ensuring its admissibility in court are key issues, and that clear rules are necessary.[15] The reiteration thereof by the European Commission[16] was confirmed by the Council[17] and experts.[18] The

13 See amongst others the Communication of 28 April 2015 on a European Agenda on Security, COM (2015) 185 final, p. 13 and 19-20 (hereafter 2015 European Agenda on Security); Non-paper of 22 May 2017 on improving cross-border access to electronic evidence: findings from the expert process and suggested way forward, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (hereafter 2017 non-paper).

14 Communication of 18 October 2017 from the Commission to the European Parliament, the European Council and the Council – Eleventh progress report towards an effective and genuine Security Union, p. 8 (hereafter 2017 Progress report on Security Union).

15 2015 European Agenda on Security (fn. 14), p. 19.

16 Communication from the Commission to the European Parliament, the European Council and the Council delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, 20 April 2016.

17 Council conclusions on improving criminal justice in cyberspace, 9 June 2016, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en (hereafter 2016 Council Conclusions).

18 The Commission summarised the results of the expert consultation in the 2017 non-paper (fn. 14). The results of the expert process were described in more detail in the Technical document "Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace" of 22 May 2017 (hereafter 2017 Technical Document).

challenges of electronic evidence continue to be addressed,[19] and the European Commission has even announced that legislative proposals can be expected in early 2018.[20]

The CoE had, in fact, already put electronic evidence back on the agenda some time before this. In fact, an ad-hoc subgroup on Transborder Access, founded in 2011 in the leap of the Cybercrime Convention Committee, already concluded in 2014 that the negotiation of an additional Protocol to the Budapest Convention would not be feasible.[21] Already then, the Transborder Group emphasised that this should be reconsidered in the future. The reconsideration process started with the recommendation of the Cloud Evidence Group (another subgroup) to draft the protocol,[22] which led to the adoption of terms of reference to guide the drafting process in midst 2017[23] and referred to the creation of an ad-hoc Drafting Group. The draft Additional Protocol is expected to be prepared and finalised by December 2019.

B. Terminology: e-evidence and content data

Despite the overall presence of electronic evidence in everyday society, and the need for a common approach on what can be collected, exchanged and preserved in and by member states,[24] there is no common and binding definition of the term on an EU level. That electronic evidence does not necessarily relate to electronic crime, cybercrime or e-crime, however, seems self-evident. Though cybercrime is also named one of the EU's priorities,[25] electronic evidence does not necessarily aim to prove the existence of cybercrime. This is to some extent already illustrated by the 2001 Convention on Cy-

19 For example, the Commission has also conducted an impact assessment in August 2017 and organised a public consultation with regard to cross-border access to electronic evidence, which implied that all interested stakeholders could fill in the questionnaire made available online.

20 Joint press conference by Marlene Bonnici, Maltese Permanent Representative to the EU, and Věra Jourová, Member of the EC, 8 June 2017.

21 *Ad-hoc Subgroup on Transborder Access and Jurisdiction*, Transborder access to data and jurisdiction: Options for further action by the T-CY, 3 December 2014, https://rm.coe.int/16802e726e, p. 12-14 (hereafter Transborder Options for further action). The Ad-Hoc Group adopted a document on the possible elements of the additional protocol in another report. See *Ad-Hoc Subgroup on Transborder Access and Jurisdiction*, (Draft) elements of an additional protocol to the Budapest Convention on cybercrime regarding transborder access to data, 9 April 2013, https://www.coe.int/en/web/cybercrime/tb.

22 *T-CY Cloud Evidence Group*, Criminal justice access to data in the cloud: recommendations for consideration by the T-CY. Final report of the T-CY Cloud Evidence Group, 16 September 2016, https://rm.coe.int/16806a495e, p. 40 (hereafter Cloud Evidence Group Final Report).

23 *T-CY Cloud Evidence Group*, Terms of reference for the preparation of a draft 2nd additional protocol to the Budapest Convention on Cybercrime, 9 June 2017, https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b. (hereafter Cloud Evidence Group Terms of Reference).

24 *T. De Zan*, Improving criminal justice in European Union cyberspace, in T. De Zan and S. Autolitano (Eds.), EUnited against crime: Improving criminal justice in European Union cyberspace, Istituto Affari Internazionali, 2016, p. 82.

25 European Agenda on Security (fn. 14), p. 2.

bercrime adopted in the leap of the CoE, where some provisions regarding all types of crime are included as well.[26]

Attempts to define electronic evidence have been taken at both CoE and EU level. In the Electronic Evidence Guide, which resulted from a joint CoE and EU-project, electronic evidence is defined as "*any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings*".[27] The EU (by way of the European Commission) emphasizes that an electronic device must be involved, as it refers to "*any information (comprising the output of analogue devices or data in digital format) of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device*".[28] Whereas in its Recommendations, the CoE refers to "*evidence in the form of data generated by or stored on a computer system*", it can be assumed that the mere reference to computer systems is rather influenced by the context and that in light of the entirety of their documents, they also agree on the possibility of multiple electronic evidence sources.[29] The definition of Mason and Seng refers to the variety of possible electronic evidence sources, defining 'electronic evidence' as "*evidence derived from data contained in or produced by any device the functioning of which depends on a software program or from data stored on or communicated over a computer system or network*".[30]

Similar to the lack of binding definition of 'electronic evidence', none of the instruments adopted by EU actors or of the CoE define 'content data'.[31] However, one of the Cybercrime Convention groups refers to content data as "*communication content of communication; i.e., the meaning or purpose of the communication, or the message or information being conveyed by the communication (other than traffic data)*" such as emails, text messages, images, movies, music and documents.[32] On an EU level, the proposal for a Regulation on Privacy and Electronic Communications refers to content data or 'electronic communications content' as "*the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound*".[33] Despite that content data refer to the content of communications, and traffic data to data relating to the communication, there are some discussions regarding the distinc-

26 Articles 14-21 Convention on Cybercrime of 23 November 2001, ETS No. 185 (hereafter Budapest Convention).
27 *Cybercrime Division Directorate General of Human Rights and Rule of Law*, Electronic Evidence Guide: a basic guide for police officers, prosecutors and judges, 2014, www.coe.int/cybercrime, p. 11.
28 Report on overview and categorization of electronic evidence, http://www.evidenceproject.eu/the-activities/deliverables.html, p. 18.
29 Cloud Evidence Group Final Report (fn. 23), p. 6.
30 *S. Mason and D. Seng*, Electronic evidence, 2017, Institute of Advanced Legal Studies – University of London, p. 353.
31 The Budapest Convention only contains a definition of traffic data (art. 1 d).
32 Cloud Evidence Group Final Report (fn. 23), p. 12.
33 Art. 4.3 b) Proposal for a Regulation of 10 January 2017 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, COM (2017)10 final.

tion between both types of data. More specifically, as traffic data can sometimes also reveal content (cf. a standard search engine request),[34] discussion can rise with regard to the applicable legal regimes, especially in light of the broad definition of 'personal data' and 'private life' applied by the EU legislator[35] and the European Court of Human Rights[36]. The lack of clarity is also reflected in member states' legislations, as results of a 2016 EU questionnaire show that only nine member states use a definition of content data.[37]

C. Cross-border collection of electronic evidence: how the system works today

Though both the CoE and the EU intend to adopt legislative instruments addressing electronic evidence, the gathering and exchange of e-evidence cannot entirely be situated in a judicial vacuum today. More specifically, both with respect to the legal framework governing mere domestic as well as cross-border collection of evidence, some European guidance has been given.

a) Cross-border jurisdiction: delineating investigative powers in cyberspace

When it comes to both the search and seizure and the interception of electronic evidence, the Budapest Convention prescribes under which conditions law enforcement authorities can gather electronic evidence within their territory. With regard to content data, distinction is made between the search and seizure (art. 19) and interception (art. 21). Moreover, the Convention also contains a 'production order'-provision (stipulat-

34 *C. Goemans and J. Dumortier*, Enforcement issues – Mandatory retention of traffic data in the EU: possible impact on privacy and on-line anonymity, in: C. Nicoll, J.E.J. Prins and M.J.M van Dellen (Eds.), Digital anonymity and the law: tensions and dimensions, 2003, TMC Asser Press, p. 162 et seq.

35 Art. 3, (1) Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119/1.

36 See amongst others Figueirdo Teixeiro v. Andorra, where the Court said that listing the incoming and outgoing calls from a telephone are also considered personal data (*données personnelles*). Therefore, these can also amount to an intrusion with the private life. See *Figueiredo Teixeiro v. Andorra*, Application no. 72384/14, Judgment 8 November 2016, margin no. 38.

37 *European Commission*, Questionnaire on improving criminal justice in cyberspace – Summary of responses, 2016, https://webcache.googleusercontent.com/search?q=cache:NMaVxaqx5C0J:https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf+&cd=1&hl=nl&ct=clnk&gl=be&client=firefox-b-ab, p. 3 (hereafter: 2016 Questionnaire).

ing that a service provider can be forced to hand over content data to law enforcement authorities), but this remains a mere domestic measure.[38]

Despite the strict honoration of the territoriality principle, already in the Explanatory Memorandum to the Budapest Convention, it was questioned whether unilateral action of member states could be allowed and, if so, under which circumstances. The lack of agreement on comprehensive, legally binding regime in this context made the drafters abstain from such stipulation.[39] The 'lack of concrete experience' with such situations, another argument expressed, does not seem to be valid anymore today; however, member states are still bound by the provision. Therefore, without violating the Convention, some member states have stretched the possibility of unilateral action as much as possible. In Belgium, for example, the search in a computer system can be extended, even across the national borders, as long as the 'extended territory' does not belong to another contracting party.[40]

In addition, the need to expand the *ratione loci* competence of member states depends on how localisation within the national territory is decided and in doing so the territorial scope of the competence of law enforcement authorities delineated. Already in 2014, *Conings* criticised the differences in territorial approaches with regard to search and seizure of stored computer data and interception of content data.[41] For stored content data, reference is made to the location of the data.[42] Whereas reference is made to the possibility to compel for example system administrators to give information to enable the search, there are no jurisdictional limitations with regard to which system administrators can be asked to do so.[43] The only restriction is that the provision of information is limited to what is 'reasonable'. For interception however, states' competence to intercept is limited to "*communications in its territory transmitted by means of a computer system*".[44] This is the case if either one of the communicating parties is located in the territory, or if the computer or other communication means through which the communication passes can be located there.[45] *Conings* refers to a combination of the subject- and object-oriented approach.[46] As was the case with search and seizure, other actors can also come into play here, as article 21 states that a service provider can be compelled to collect the content data. In this respect, the Ex-

38 To this extent, art. 18, 1 a) Budapest Convention requires that 1) the criminal justice authority has jurisdiction over the offence, 2) the service provider is in the possession or control of the data and 3) the service provider is in the territory of the party.

39 Explanatory Memorandum to the Convention on Cybercrime, Budapest, 23 November 2001, ETS No. 185, p. 53 (hereafter Explanatory Memorandum).

40 Art. 39bis Belgian Code of Criminal Procedure. In the Explanatory Memorandum to the Belgian Code of Criminal Procedure (*Memorie van Toelichting)* there is talk of limited, almost exceptional circumstances (p. 119 et seq.).

41 *C. Conings*, Locating criminal investigative measures in a virtual environment. Where do searches take place in cyberspace, 2013, B-CCENTRE End Report, p. 43 et seq.

42 Art. 19, 1 Budapest Convention (fn. 27).

43 Explanatory Memorandum (fn. 40), p. 33-35.

44 Art. 21, 1 Budapest Convention (fn. 27).

45 Explanatory Memorandum (fn. 40), p. 38.

46 *C. Conings* (fn. 42), p. 43 et seq.

planatory Memorandum specifies that the obligation 'generally' applies to service providers having some physical infrastructure or equipment on that territory, which does not necessarily imply that the main operations or headquarters should also be situated there.[47] Following the lack of clear stance, member states appear to apply different criteria when it comes to distinguishing domestic from foreign service providers: whereas some member states refer to the main seat of the service provider, other use the place where the services are offered and the place where the data are stored, or even a combination of alternatives.[48] Qualifying a service provider as residing in national territory has, therefore, already led to discussions. Though *Yahoo! v. Belgium* for example related to disclosure of technical assistance to get to other than content data, the Court of Appeal judged on the geographical conditions that should be fulfilled before Yahoo! had to cooperate with the Belgian law enforcement authorities. For coercive measures with a limited scope (*in casu*, this implied that no intervention outside the Belgian territory was required), a sufficient geographical starting point was required, which was the case, as Yahoo! offered its services in the Belgian territory and thus actively participated to the economic life in Belgium.[49] Localisation gains even more importance when it comes to production orders. After all, only the 'competent' authority can order a 'domestic' service provider to submit content data.[50]

The CoE refers to 'cloud computing' to indicate that data are less held on a specific device or in closed networks, but rather are distributed over multiple providers and locations.[51] Cloud evidence can be related to remote emails services (such as Gmail) or to remote data storage and sharing systems (such as Google Docs).[52] In fact, the electronic evidence thus becomes independent of any location. In this way, determining jurisdiction, especially when this is determined on the basis of the location of the data (for example with regard to search and seizure) becomes hard when this location is unknown. Therefore, there is sometimes talk of 'loss of (knowledge of) location'.[53]

b) Mutual legal assistance between judicial authorities

In case of a cross-border collection of content data, the existing formal mutual legal assistance instruments should be kept in mind. However, some problems arise.

47 Explanatory Memorandum (fn. 40), p. 38.
48 2016 Questionnaire (fn. 38), p. 2.
49 The Court did not deem it necessary for Yahoo! to have its seat or a branch in Belgium. See YAHOO! Case 2012/CO/1054 Yahoo! Inc (Court of Appeal of Antwerp, 12th chamber for criminal cases 2013), https://www.stibbe.com/en/news/2016/january/court-of-cassation-definitively-confirms-yahoos-obligation-to-cooperate-with-law-enforcement-agenci.
50 Art. 18, 1 a) Budapest Convention (fn. 27).
51 Cloud Evidence Group Final Report (fn. 23), p. 7.
52 *B-J. Koops and M. Goodwin*, Cyberspace, the Cloud and Cross-border Criminal Investigation, The limits and possibilities of international law, Tilburg Institute for Law, Technology and Society, 2014, p. 27.
53 *J. Spoenle*, "Cloud computing and cybercrime investigations: territoriality vs. the power of disposal?", 31 August 2010, https://rm.coe.int/16802fa3df.

On the one hand, one can question how it can be established that there is a situation of 'cross-border' evidence collection. The distinction between domestic and cross-border evidence collection is not always clear, especially since there are no legally binding criteria for location establishment. Whereas the Budapest Convention refers to the data location for the application of mutual legal assistance,[54] this criterion has not only been outdated by everyday reality,[55] but is also incompatible with the *ratione loci* stipulations in the context of content data collection. Whereas for interception the Budapest Convention seems to give the territoriality principle a quite broad interpretation (see also *supra* in a)), this approach seems to be in contradiction with the EU MLA provisions. According to the 2000 Convention, mutual legal assistance comes into play when the subject is no longer present in the national territory of the requesting member state.[56] The European Investigation Order does not refer to scope of mutual legal assistance. However, the Directive states that if mutual legal assistance is sought for the interception and if more than one member state can provide technical assistance, it prioritises the member state where the subject is located to send the EIO to.[57] From a data protection point of view, other criteria apply to determine which rules a service provider needs to comply with.[58] The Cybercrime Convention Committee refers to "*different layers of jurisdictions for various legal aspects related to its service at the same time*".[59]

On the other hand, the value of the existing instruments with regard to cross-border collection can also be questioned. Whereas the European Investigation Order allows for obtaining evidence in another member state, it does not provide any indication on how the collection, preservation and exchange of electronic evidence should take

54 Art. 31, 1 Budapest Convention refers to computer data that are stored and can be located within the territory of another Party. According to the Evidence Project, there are three scenarios which could be addressed by law: (1) the cloud service provider and/or data centre are located in a (known) foreign country, (2) both are located in one country, but the suspect is located in a foreign country, and (3) the physical storage location of the data is unknown. See Report on data protection (fn. 9), p. 104.

55 Research has also proven that data storage normally takes place outside the control of the state on whose territory these data are stored. See 2017 Technical Document (fn. 19), p. 30.

56 Art. 18, 2 of the 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 2000 C 197/1 (hereafter 2000 Council Act on MLA).

57 Art. 30, 2 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ 2014 L 130/1 (hereafter European Investigation Order). This also implies that it is not necessarily the member state where the subject is located in, that is competent to intercept the content data.

58 See amongst others *Court of Justice of the European Union* (CJEU), 13.5.2014, case 131/12 (*Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*).

59 Cloud Evidence Group Final Report (fn. 23), p. 7-8.

place.[60] On the level of the CoE, the Budapest Convention itself also comprises an MLA provision.[61] However, the exchange of content data through the mutual assistance channel is considered too lengthy and formal, especially given the "*volatile and fast moving nature of electronic evidence*"[62]. Whereas the MLA process is already considered inefficient in general, the Cybercrime Convention Committee believes this is in particular so with regard to obtaining electronic evidence.[63] Moreover, as MLA provisions can only be invoked when the location is known, these are useless in the 'loss of location'-context.

c) Direct cooperation with service providers

Beside the MLA instruments, direct access options are also included in the Budapest Convention. With regard to accessing content data in another member state (for domestic situations, the production order can be used, but only article 18, 1, a) for content data), and if not accessed based on the public availability of the content data, the Budapest Convention prescribes that another member state may "*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.*"[64] However, some problems occur in applying this provision, which is actually a combination of direct cooperation and widened access rights. For example, it is required that the data can be located, which in present times is not that self-evident.[65] Moreover, it also requires that the service provider has the lawful authority to disclose the data, which is questioned from a data protection point of view.[66] Therefore, informal assistance between law enforcement authorities and service providers appears to have become the main channel for obtaining cross-border access to the electronic evidence, at least for non-content data.[67] In fact, with regard to cloud evidence, statistics show that requests

60 Report on legal issues – status quo assessment and analysis of primary challenges and shortcomings, 2015, http://www.evidenceproject.eu/the-activities/deliverables.html, p. 22 (hereafter Report on legal issues).
61 Art. 31, 1 Budapest Convention (fn. 27).
62 Report on legal issues (fn. 61), p. 33.
63 *Cybercrime Convention Committee (T-CY)*, T-CY assessment report: the mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3 December 2014, https://rm.coe.int/16802e726c, p. 123 (hereafter 2014 MLA Report).
64 Art. 32, b) Budapest Convention (fn. 27). In this situation, no authorisation of another party is required.
65 Cloud Evidence Group Final Report (fn. 23), p. 27. For most US providers, the actual location seems to be of limited relevance. For access to subscriber information, whether or not there is access to this information seems to be determined by (a) the location of the service provider and the regulations that govern the service provider, and (b) whether the requesting law enforcement authority has jurisdiction over the offence investigated. See Cloud Evidence Group Final Report (fn. 23), p. 27.
66 Cloud Evidence Group Final Report (fn. 23), p. 33.
67 2017 Technical Document (fn. 19), p. 10-11.

sent to US service providers are answered by (partial) data disclosure in at least 60 percent of the requests.[68] However, when it comes to EU service providers, this is far from the case, mainly because most legislation does not seem to cover or allow service providers to respond to these requests.[69] Beside the national differences, this form of cooperation remains unregulated (or regulated only bilaterally[70]) and, therefore, arbitrary.[71] The EU questionnaire also reveals that it is not even possible in all member states to request content data directly from service providers.[72] Together with the lack of clear definition of the different types of data sought, it is no wonder these legal lacunae hamper the cooperation of international law enforcement.[73]

d) Conclusion: time for an update of the electronic evidence framework

Taking a look at the regulations in place for gathering of electronic evidence/content data and mutual legal assistance, one cannot but conclude that these are far from adequate to deal with cross-border access to electronic evidence. Whereas the procedural rules lack a clear delineation *ratione loci* to collect content data, mutual legal assistance instruments seem outdated (if not contradictory to the procedural rules), and direct cooperation too arbitrary. It is time for the European legislator to keep up with the technological developments and adapt the antiquated rules on collection of content data in order to meet the wish of both law enforcement authorities and service provider.

III. Food for thought: the EU's and CoE's solutions for the problems faced

Given the challenges of electronic evidence collection, both the EU and the CoE have put the topic back on the agenda. Though there have also been many discussions with regard to encryption and the possibilities (also given the wordings of the Budapest Convention) to compel service providers to give law enforcement authorities access to certain data,[74] it is preferred to exclude this discussion from the scope of this article. In the next paragraphs, the article will discuss the extent to which the current proposals might resolve the problems that are now faced when collecting content data. In doing so, these proposals will also be measured up against the results and recommendations

68 *T-CY Cloud Evidence Group*, Criminal justice access to data in the cloud: cooperation with 'foreign' service providers, 3 May 2016, https://www.coe.int/en/web/cybercrime/ceg. With regard to content data, most of the service providers discussed require a search warrant issued upon showing probable cause. Sometimes (Microsoft and Yahoo) an actual MLA request is necessary.

69 2016 Questionnaire (fn. 38), p. 3.

70 For example, the US and the UK plan on concluding such bilateral agreement.

71 2017 Technical Document (fn. 19), p. 11.

72 2016 Questionnaire (fn. 38), p. 2-3.

73 *M.A. Biasiotti*, A proposed electronic evidence exchange across the European Union, Digital Evidence and Electronic Signature Law Review, 2017, p. 10.

74 For more information on this, see for example 2017 Progress report on Security Union (fn. 15).

of the Evidence Project, a study conducted with the aim to, amongst others, create a Common European Legal Framework.

According to the Evidence Project, adapting the MLA procedures to everyday reality is one of the short-term solutions. In doing, so, the study refers to the need for promotion and support of internationally coordinated investigations and JITs.[75] Strange enough, the modernisation of international law, the scope under which the study puts the creation of a sound legal basis (definition of electronic evidence, discussing possibilities for modernising international law and draft amendments), is considered a long-term solution, *i.e.* that will be addresses within the ten (!) upcoming years.[76]

A. Solving the challenges of cloud computing: extended or remote access?

The first method applied by law enforcement authorities to collect electronic evidence, is search and seizure or interception of the content data. As was mentioned above, over the years, some member states have widened their authority *ratione loci*, which can lead to conflicts.

Both on an EU and CoE level, the issue of extended access has already been discussed quite thoroughly. On the one hand, the EU specified in its non-paper that a legislative solution to facilitate direct access should be accompanied by the adoption of EU level common conditions and minimum safeguards for direct access in cross-border situations and mitigating measures such as notifications to other possibly affected countries.[77] Reference was also made to considering this option in situations where the storage place of the data is unknown or is located outside of the EU.[78]

In some of the policy documents, a subject-oriented approach to determine the substantial connection was proposed. This could for example imply that "*the nationality or the habitual residence of the suspect or accused or the location of the person affected by the crime*" or 'the power of disposal' function "*as a connecting factor*" for establishing enforcement jurisdiction.[79] The subject-oriented approach confirms the position taken by some scholars.[80] In the actual Conclusions, however, the EU only stresses the need to discuss on possible solutions for investigations in cyberspace where the location of data is not (yet) known, and the connecting factors for enforcing jurisdiction in cyberspace should be reviewed, but this is not explicitly linked to a wider possibility of

75 Road map for a Common European legal framework for electronic evidence, 2016, http://www.evidenceproject.eu/the-activities/deliverables.html, p. 40 (hereafter Road map).
76 Road map (fn. 76), p. 70-71.
77 2017 Non-paper (fn. 14), p. 5.
78 *European Commission*, Inception Impact Assessment on Improving cross-border access to electronic evidence in criminal matters, 3 August 2017, https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en, p. 3 (hereafter Inception Impact Assessment).
79 *Council of the European Union*, Improving criminal justice in cyberspace – Preparation of the Council debate (Justice Ministers), 12 May 2016, p. 5.
80 *C. Conings* (fn. 42), p. 43 et seq.

'extraterritorial' access.[81] The results of the questionnaire launched end of 2016 and subsequent countries' responses do not seem to give way for an explicit stance of the approach that needs to be taken with regard to jurisdiction.[82] This led to the Commission not taking a stance with regard to the factors determining member states' jurisdiction for the gathering of electronic evidence, in the 2017 Public Consultation everything is questioned again, *i.e.* not only whether a common EU Framework for this situation is needed, but also whether it should be accompanied by certain procedural safeguards and rules (double criminality, notifications, …). Some organisations (such as CCBE and DigitalEurope) have indeed raised their concerns in this regard, as they believe a distinction should be made between extended and remote access in that misuse of 'legal hacking' should be prevented by clearly spelled out safeguards and limitations.[83] A study conducted by the Directorate General for Internal Policies on legal frameworks for hacking by law enforcement show that member states' compliance with both procedural rules and procedural safeguards should be regarded more closely.[84]

From the CoE's point of view, the Recommendations put forward by the Cloud Evidence Group stated that a common international solution for lawful transborder access to data is required, and that this instrument "*may focus less on the location of the data but on the person in possession or control of the data*".[85] There is also talk of the 'power of disposal' as connecting legal factor.[86] The Group also believes that the location of the victim at the time of the crime in the territory of a Party can result in transborder access to data.[87] The Groups puts notification of the other member state as one of the requirements.[88] The Terms of Reference for the preparation of the Additional Protocol included in the elements for reflection the creation of a clearer framework and stronger safeguards (including data protection requirements) when it comes to cross-border access to data.[89] Though in the first meeting of the Protocol Drafting Group, the transborder access was also discussed, it is unclear what the discussion was

81 2016 Council Conclusions (fn. 18). Whereas the Council stresses the need to discuss on possible solutions for investigations in cyberspace where the location of data is not (yet) known, this is not explicitly linked to a wider possibility of 'extraterritorial' access.

82 *Council of the European Union*, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 7 December 2016; 2016 Questionnaire (fn. 38), p. 1 et seq.

83 Privacy International however confirms that there is a need for a common framework in this regard, whereas the CCBE has no opinion on this.

84 *Directorate-general for internal policies*, Legal frameworks for hacking by law enforcement: identification, evaluation, and comparison of practices, 2017, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf, p. 69-70.

85 Cloud Evidence Group Final Report (fn. 23), p. 16.

86 Cloud Evidence Group Final Report (fn. 23) p. 45.

87 Cloud Evidence Group Final Report (fn. 23) p. 16.

88 Cloud Evidence Group Final Report (fn. 23), p. 55.

89 Cloud Evidence Group Terms of Reference (fn. 24), p. 3-4. in the Cloud Evidence Group Final Report (fn. 23) reference is made to the operational agreements concluded between Europol and a number of non-member states, where certain data protection requirements such as purpose limitation and right of access are included. See p. 46.

about and whether any progress was made.[90] Also here, it will remain to be seen whether the legislative proposals will build upon the recommendations made.

When comparing both policy levels and the (provisional) policy documents created in their leap, some similarities and differences can be noticed. Both institutions identify the need for clear rules on transborder access and criteria for such access. Whereas both stress the need for additional safeguards, it is unclear to what extent all elements mentioned in the EU Public Consultation will be included. For instance, the comment made by the CoE that a difference should be made with regard to thresholds for access rights based on the type of data[91] might be an argument for introducing a double criminality requirement or other safeguards such as the notification of other member states affected by the measure (similar to the notification requirement included in article 31 European Investigation Order?).

B. Indirect access: Mutual legal assistance vs. direct cooperation with service providers

Whereas transborder access is one way to get to electronic evidence, member states can also opt for cooperation with other actors. These actors can be service providers, in which case there is talk of direct cooperation,[92] or they can be other member states, in which case there would be talk of indirect cooperation (as the addressed member state will still have to find a way to gather the content data).

a) Direct cooperation with service providers: an international production order?

Besides looking at the possible extension of the states' powers *ratione loci*, both the CoE and the EU consider the introduction of a legal framework for cooperation between law enforcement authorities and service providers. Whereas cooperation between both actors already occurs today, the ad hoc basis of present-day cooperation leads to legal uncertainty. Important to notice is that, whereas both organisations speak of 'international production orders', their interpretation of this concept differs. On the one hand, the EU sees the international production order in the same way as the concept will be used here, *i.e.* as an investigative measure that can directly be addressed to the service provider of another member state instead of going through law enforcement or judicial authorities in another member state first.[93] The CoE on the other

90 *Cybercrime Convention Committee (T-CY)*, Summary Report of 20 September 2017 of the 1st meeting of the T-CY Protocol Drafting Group, https://www.coe.int/en/web/cybercrime/-/1st-meeting-of-the-protocol-drafting-group-on-the-second-additional-protocol-to-the-convention-on-cybercrime, p. 2 (hereafter First Meeting Report).

91 *Council of Europe*, Press Release: Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol on the Budapest Convention, 2 November 2017, https://rm.coe.int/t-cy-pd-pubsummary/168076316e (hereafter CoE Press Release).

92 *A-M. Osula*, Accessing Extraterritorially Located Data: Options for States, 2015, NATO Cooperative Cyber Defence Centre of Excellence, p. 16 et seq.

93 2017 Non-paper (fn.14), p. 4.

hand mostly[94] refers to the international production order as a way to improve MLA. More specifically, the order could then be sent by the authorities of one party to the law enforcement authorities of another Party.[95] The international production order thus is perceived as an application of the European Investigation Order to the specific situation of electronic evidence.[96] As this refers to 'upgrading' the MLA procedures, this point of view will be discussed below. However, the CoE also discusses the possibility of directly accessing service providers (albeit not by using the term 'international production order', but just by referring to direct cooperation with service providers in other jurisdictions)[97] which will be discussed here.

When it comes to the EU, the European Commission appears to be a great supporter of the idea of an international production 'order', though they are not yet sure they want to call it that. In the 2017 non-paper, the Commission mentions the creation of the production order or request as one of the solutions proposed by the experts.[98] However, the Commission also noted that the same experts believed that any improvement with regard to direct cooperation with service providers would not extend to content data, nor to non-content data situated somewhere else than in the US and Ireland (which are the only countries voluntarily cooperating).[99] In the non-paper, the ideas mentioned are just options: voluntary respond or a mandatory order combined with a sanctions regime, only compelling service providers with a presence in the EU to respond, or requiring electronic communication services and platforms providers based outside the EU to appoint a legal representative in an EU Member State,[100] etc.[101] Thought should also be given to the connecting factor on the basis of which a service provider is located in a member state.[102] Up until now, the Commission still leaves all options open. In the Inception Impact Assessment, the Commission speaks of "*a legal framework authorising authorities to directly request or compel a service provider in another Member State to disclose e-evidence processed in the Union, including appropriate safeguards and conditions. This framework can leave to the discretion of the service provider a decision on whether to provide a response ("production re-*

94 In the first meeting report, reference is however made to international production orders for subscriber information, i.e. addressing service providers.
95 2014 MLA Report (fn. 64), p. 127.
96 Cloud Evidence Group Final Report (fn. 23), p. 41.
97 CoE Press Release (fn. 92).
98 2017 Non-paper (fn.14), p. 4.
99 2017 Non-paper (fn.14), p. 4.
100 This is probably inspired by the 2000 Council Act on MLA (fn. 57), which had a similar obligation to carry out an interception through an intermediary (see article 19). However, in the European Investigation Order (fn. 58), this was no longer included. Obviously, many service providers are against the introduction of such representative, referring to the costs of translation, need for a legal basis assessment and additional efforts in providing secure communication channels (administrative and compliance costs). They believe that the obligation of a legal representative (and by extension, the order to obligate) consists of much more gains for the public sector than for the private sector.
101 2017 Non-paper (fn. 14), p. 4-5.
102 2017 Technical Document (fn. 19), p. 22.

quest") or can obligate service providers to respond ("production order"). This could also be considered with respect to service providers located outside of the Union and/or data stored outside of the Union. This system could be complemented by an obligation for service providers established in third countries but offering services in the EU to designate a legal representative in the EU for the purpose of the cooperation on the basis of production requests/orders".[103]

In the EU Questionnaire, many aspects of the international production order/request are still left open for debate. For example, it can be discussed which types of service providers (electronic communication service providers such as telecom operators, information society service providers such as cloud services and social networks, other digital service providers) relevant for investigative measures should be involved.[104] Moreover, it is unsure, given the current practices, whether the production order or request will also be adopted for content data and, even if so, whether this will apply to data stored in the EU or also to the data stored outside (apparently, the Commission forgot about the difficulty to locate the data), or whether this will depend on the location of the service provider.[105] In addition, and similar to the questions on direct access, the Commission asks for thoughts on whether certain procedural rules and safeguards should accompany the introduction of the direct cooperation. Some of those seem to recall previous legal instruments. Though relating to judicial cooperation, the European Investigation Order also foresees a dual criminality requirement, but this will not be checked if it concerns an "*offence listed within the categories of offences set out in Annex D, as indicated by the issuing authority in the EIO, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years*".[106] Moreover, the EIO foresees some kind of topping with regard to the execution of investigative measures by stating that the execution of an order may be refused if "*the investigative measure would not be authorised under the law of the executing State in a similar domestic case*".[107] Beside these procedural rules, the Commission also asks for the opinion of the public with regard to the introduction of certain safeguards. In particular, the notification of the member state(s) affected by this measure, and notification of the targeted person are integrated in the questionnaire. With regard to the notification of affected member states, the Commission stated that it would have to be determined what factors identify affected countries, and whether the member state can object and if so, within which deadline.[108] *Osula* and *Zoetekouw* indicate that there is no legal obligation as such in international

103 Inception Impact Assessment (fn. 79), p. 3.
104 Public consultation on improving cross-border access to electronic evidence in criminal matters, https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en, Question 62.
105 *Ibid.*, Question 61.
106 Art. 11, 1, g) European Investigation Order (fn. 58). Question 59 refers amongst others to limiting the possibility to address service providers directly based on the severity of the offence.
107 Art. 11, 1 c) European Investigation Order (fn. 58).
108 2017 Technical Document (fn. 19), p. 22.

law, though it might be beneficial from a diplomatic point of view.[109] In MLA instruments such as the 2000 MLA Convention and the European Investigation Order, the notification of the member state in which the intercepted person is foreseen, including the possibility to object.[110] When it comes to the notification of the targeted person, the Commission is aware of the need to consider the (modalities of the) notification of the individuals affected.[111] In this context, *Jasserand*[112] also considers that access by law enforcement authorities to personal data initially collected for other purposes should be subject to certain procedural, data-protection oriented safeguards, inspired by the case-law of the Court of Justice. Besides referring to several data-protection oriented safeguards, based on Digital Rights Ireland and Tele2 Sverige,[113] she believes that notification of the person involved inevitably follows from the considerations in Tele2 Sverige, where the Court of Justice said that the persons affected must be notified as soon as possible (in light of the investigations), in order to enable the exercise of the right to a legal remedy.[114] Despite the clear stance of the Court of Justice, the Commission, however, still asks for the opinion of the public in this respect.

On the level of the CoE, thought has also been given to possibilities to enhance cooperation with foreign service providers. Some service providers have stressed the need for a legal basis in order to avoid liability claims from the data subjects.[115] The need for enhanced cooperation with these actors has also been confirmed by the ECtHR in *K.U. v. Finland*. In this case, the Court believed it was unacceptable in light of article 8 that the Finnish law did not enable compelling the operator of the internet server to provide information on the other user, but merely provided the criminal offence of malicious misrepresentation and the possibility of bringing criminal charges or an action for damages against the server operator.[116] Though the case concerned the need for identification of the perpetrator and thus subscriber information, it is interesting that the possibility to compel the service provider to hand over information is ad-

109 *A. Osula and M. Zoetekouw*, The notification requirement in transborder remote search and seizure: domestic and international law perspectives, Masaryk University Journal of Law and Technology 2017, p. 108-09.

110 Art. 20, 2 and 4 2000 Council Act on MLA (fn. 57) and art. 31 European Investigation Order (fn. 58).

111 2017 Technical Document (fn. 19), p. 23.

112 *C. Jasserand*, Law enforcement access to personal data originally collected by private parties: missing data subjects' safeguards in directive 2016/680?, Computer Law and Security Review 2017, in Press.

113 For example, she concludes that amongst others that there should be objective criteria limiting the law enforcement access to personal data and that serious crimes should be involved. See *Court of Justice of the European Union* (CJEU) 8.4.2014, joint cases 293/12 and 594/12 *(Digital Rights Ireland and Seitlinger and others),* margin no. 62) and *Court of Justice of the European Union* (CJEU) 21.12.2016, joint cases 203/15 and 698/15 *(Tele2 Sverige AB/Post-och telestyrelsen and Secretary of State for the Home Department/Tom Watson and others)*, margin no. 119.

114 CJEU, *Tele2 Sverige* (fn. 114), margin no. 121.

115 Cybercrime Convention Committee (T-CY), Guidance Note 10 on Production orders for subscriber information, 1 March 2017, https://rm.coe.int/16806f943e.

116 *K.U. v. Finland*, Application no. 2872/02, Judgment 2 December 2008, margin no. 46.

dressed. In the MLA Assessment Report, one of the recommendations of the Cybercrime Convention Committee said that the Parties may consider addressing the practice of law enforcement and prosecution services obtaining information directly from foreign service providers, and related safeguards and conditions.[117] The member states, however, which also formulated some proposals to make MLA more efficient, limited the direct requests to non-content data.[118] In the 2016 Cloud Recommendations, the scope becomes even narrower, as the T-CY first discusses subscriber information and then refers to the content of the Protocol, clarifying *such* cooperation, thus tying itself to article 18 and clarification of the existing direct cooperation.[119] In the summary of recommendations, the direct cooperation is also limited to subscriber information.[120] In subsequent documents, the scope of the electronic evidence has not been broadened again.[121] In the first meeting report of the Drafting Group, direct cooperation with service providers is mentioned separately again, not accompanied by any limitations *ratione materiae*.[122] However, it seems that the CoE will first have to decide to what extent they will allow being influenced by actors such as service providers,[123] but also the US[124] and European member states' governments[125] in deciding on the scope of direct cooperation with service providers.

When comparing the efforts of both organisations, it seems that both the EU and the CoE are in favour of a way to come to better cooperation with service providers. On the one hand, the EU might leave to many options open for discussion, whereas the Court of Justice has already taken a stance with regard to the inclusion of several procedural rules and safeguards when it comes to access of judicial authorities to data gathered by private parties for other purposes. On the other hand, the CoE might be

117 2014 MLA Report (fn. 64), p. 127.
118 2014 MLA Report (fn. 64), p. 132.
119 Cloud Evidence Group Final Report (fn. 23), p. 44.
120 Cloud Evidence Group Final Report (fn. 23), p. 47.
121 Cloud Evidence Group Terms of Reference (fn. 24), p. 3 also refers to subscriber information, just like First Meeting Report (fn. 91), p. 2.
122 First Meeting Report (fn. 91), p. 4.
123 Agreement on Mutual Legal Assistance between the European Union and the United States of America, OJ 2003 L 181/34). This agreement has been approved on behalf of the EU in the Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ 2009 L 291/40.
124 In the US, direct requests from foreign jurisdictions to US-based service providers are not prevented, as long as the request considers non-content data. The US has indicated that they are not in favor of extending the current practices of voluntary cooperation in the context of non-content data, and prefer lawful orders or mutual legal assistance otherwise. See *Council of the European Union*, Improving criminal justice in cyberspace – Preparation of the Council debate (Justice Ministers), 12 May 2016, p. 6.
125 In fact, the 2016 Questionnaire showed that only a few member states have informal agreements with service providers, whereas the majority of the member states has not. Moreover, almost all member states do not allow or cover service providers established in that member state to respond to direct requests from another member state or third country. See 2016 Questionnaire (fn. 38), p. 2-3.

blamed for dismissing to many options in advance, whether or not influenced by the opinions of actors involved, as they currently only speak of direct cooperation for subscriber information anymore.

b) Indirect cooperation between judicial authorities: the lesser evil?

Besides the far-reaching intentions of the EU and the CoE, both have also expressed their intentions to update the formal cooperation channels. As this only concerns the improvement of already existing practices, only a brief overview of the planned improvements will be given.

The EU puts its focus on working on an electronic form and a secure platform for exchanging requests for electronic evidence.[126] Closer judicial cooperation with the US is also envisaged,[127] especially given the relatively small possibility that the US government will agree to the exchange of content data on a non-MLA basis (see also *supra*). On an EU level, the mutual legal assistance regime with the US will not be adapted through amendments to the European Investigation Order, as the US is not a party to this Directive, but will require an Agreement similar to the 2003 Agreement on MLA between the EU and the US. In the Inception Impact Assessment, however, the Commission does not mention MLA between judicial authorities as one of the legislative options.

The CoE conducted a study on the MLA provisions of the Budapest Convention and recommended there that the CoE should develop standardised, multi-language templates for MLA requests. Moreover, the Council states that enhanced direct cooperation between judicial authorities in MLA requests should be one of the elements to consider to be addressed through an Additional Protocol.[128] These recommendations have been copied in the Final Report of the Cloud Evidence Group and the Terms of Reference for the preparation of a second draft Protocol to the Budapest Convention. As in its press release, the Council, however, recommended several provisions for more efficient MLA, which amongst others imply international production orders (see *supra* for the differences in meaning between international production order from an EU point of view).

IV. Conclusion: efficient electronic evidence collection, just an update away, or does the device need to be restarted to complete the necessary updates?

Given the overall presence of electronic evidence and the rareness of specific legal instruments in this regard, the initiatives of the CoE and the EU to ameliorate e-evidence cooperation in criminal matters does not appear out of thin air. After considering the technological developments and the legal frameworks of both the EU and the CoE, it

126 2017 Technical Document (fn. 19), p. 15.
127 2017 Technical Document (fn. 19), p. 15-17.
128 2014 MLA Report (fn. 64), p. 127.

becomes clear that the legal instruments in force at present are not sufficiently advanced to meet today's challenges with regard to the collection of electronic evidence. Though both organisations aim at updating their legal tools, the EU already plans concrete action in the beginning of 2018, whereas the CoE expects a first Draft Additional Protocol to be delivered in December 2019. How the EU's legal instrument on e-evidence will look like, however still needs to become clear. Though the Commission appeared to have a very clear view on this when it initiated the update initiative, a lot of options still appear to be open for discussion. In any event, and despite the identification by the Evidence Project as something that should only be addressed in the long term, the member states are in need of clarity, not only with regard to the definition of the different types of electronic evidence, but also with regard to the localisation of actors and evidence involved. After all, all efforts to enhance cooperation based on legal concepts that are still under discussion will not be considered an update, but will rather lead to… more discussion.