Cross-Border Law Enforcement Access to e-Evidence

Why Global Problems Warrant Global Solutions

Gert Vermeulen[1]

In the global digital arena, a range of (communication) data, increasingly wanted as evidence in criminal matters, is stored, routed or otherwise processed in different places and on or through different servers or platforms by or under the control of various types of providers, often having their main establishment in foreign jurisdictions. The resulting loss of location of such e-evidence overhauls traditional jurisdictional and mutual legal assistance rules in criminal matters. Competing and conflicting interest of states, companies and data subjects are at stake. Unilateral and single-sided territorial or market (access) approaches at national, bilateral or regional level are unlikely to offer satisfactory solutions. Taking account of the complexity of the e-evidence issue, the Council of Europe's global efforts to find common ground in a second Additional Protocol to the Budapest Convention, offer the best prospects for providing an internationally acceptable and sustainable data protection backbone for transnational e-evidence gathering.

1. Introduction

The global digital arena leaves little scope for an easy e-evidence solution. The information society has prompted evidence in criminal matters to increasingly take an electronic form. A range of (communication) data – traditionally categorised as subscriber data, traffic (including geolocation) data or content data (Warken, van Zwieten & Svantesson, 2020) – is stored, routed or otherwise processed in different places and on/through a range of servers or platforms by telecom or electronic communications providers as well as over-the-top (OTT) providers. This prompts a so called *loss of location* of the data concerned and, hence, a heightened need in (even merely domestic) investigations for evidence stored across borders or controlled by providers with their main establishment in foreign jurisdictions (often the US). The issue has been amply set out and commentated and is recognised as triggering "*flaws with the straightforward application of old jurisdictional rules onto the new medium of data*" as well as "*unilateral rulemaking by powerful states*"(Daskal, 2018, p.101). The loss of location of e-evidence overhauls traditional jurisdictional and mutual legal assistance rules in criminal matters. Competing and conflicting interest of states, companies and data subjects are at stake. Unilateral and single-sided territorial or market (access) approaches at national, bilateral or regional level are unlikely to offer satisfactory solutions. Even if they won't and can't be halted, a more global effort is key, especially for overcoming diverging data protection standards, which increasingly and irreversibly interplay and interfere with traditional MLA schemes. Surely the rights of companies to freedom of establishment and the right to conduct business and offer services in a global market cannot be denied. Neither can their responsibility as data controllers or the importance of data storage location and the resulting data protection regimes. At the same time, attributing private companies a formal role in inter-state cooperation in criminal matters is a risky avenue. Taking account of the complexity of the e-evidence issue,

[1] Gert Vermeulen is Senior Full Professor of (European and international) Criminal Law and Data Protection Law, Director of the Institute for International Research on Criminal Policy (IRCP) and Director of the Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement and Surveillance (PIXLES) at Ghent University, Belgium. He is also an expert for international affairs for the Belgian Data Protection Authority, of which he formerly was a Privacy Commissioner, and a member of the European Data Protection Board's Expert Subgroup on Borders, Travel and Law Enforcement (BTLE), the Europol Cooperation Board and the Supervision Co-ordination Groups for SIS, Eurodac, VIS and CIS. Since 2018, he acts as an expert for the Committee of Convention 108 (Council of Europe) for the negotiations on a 2nd Additional Protocol to the Budapest Convention on Cybercrime, relating to (direct) cooperation in transnational e-evidence collection, i.e. the topic of the current text.

the Council of Europe's global efforts to find common ground in a second Additional Protocol to the Budapest Convention, offer the best prospects for providing an internationally acceptable and sustainable data protection backbone for transnational e-evidence gathering. It equally offers the best chances not to let alleged reasons of efficiency dictate the contours of the debate to the detriment of the data subject or person concerned.

2. National, US, EU and bilateral responses to a global problem

Whilst the cross-border gathering of evidence in criminal matters has traditionally been a matter of mutual legal assistance (MLA) in criminal matters, states have indeed turned to unilateral approaches to face the above challenges. They circumvent or bypass MLA by compelling extraterritorial providers or data controllers of extraterritorial data to cooperate directly with the competent domestic judicial or police authorities, i.e. in an asymmetrical public-private cooperation across borders.

Reference can e.g. be made to the Belgian approach: based on a stretched interpretation of traditional cooperation duties for territorial providers, international companies that offer communication services on its territory are compelled to cooperate directly with domestic investigators. Reference can be made here to the renowned Yahoo![2] (de Hert & Kopcheva, 2011; De Schrijver & Daenens, 2013; L'Ecluse & D'hulst, 2016; Miglio, 2017) and Skype[3] (Bartunek, 2017; Valgaeren, 2017) cases.

The Yahoo! case has its origin in a request by the public prosecutor addressed to Yahoo! Inc, based in California, US, to disclose the identity behind Yahoo! e-mail accounts that had been used for a fraudulent purchase of and failure to pay for electronic equipment from a shop in Dendermonde. The prosecutor's request was based on Article 46bis of the Belgian Code of Criminal Procedure Code (CCP), which provides that electronic communication services providers must disclose identification data to law enforcement agencies upon request and are criminally liable if they refuse to cooperate. The Criminal Court of Dendermonde followed the prosecutor's line of reasoning. The case was appealed against by Yahoo!, opposing the extra-territorial reach of Belgian domestic law. Following no less than three Appeals Court decisions, respectively in Ghent, Brussels and finally Antwerp (each appealed against before the Court of Cassation), the saga ended in December 2015, when the Court of Cassation confirmed the 2013 decision by the Antwerp Court of Appeal. The supreme court found that there was no issue of extraterritorial jurisdiction at stake. It held that, even if an operator or provider of electronic communications is located abroad, like Yahoo! Inc, it voluntarily submits itself to Belgian law when it deliberately participates in domestic economic life, notably by using the domain name .be, displaying ads based on the location of its users, thus targeting Belgian consumers.

In November 2017, The Antwerp Court of Appeal confirmed the position taken by the Criminal Court of Mechelen in the so-called Skype case. It held that Microsoft-owned Skype, though incorporated in Luxembourg, is under an obligation to cooperate with the domestic authorities in Belgium. Based on the above Yahoo! reasoning, Skype was found guilty of failing to give essential information and provide a wiretap on Skype VoIP calls, as ordered by a Belgian investigating judge based on Articles 88bis and 90quarter, §2 CCP. The Appeals Court found that Skype, by providing a Dutch version of its website so that Dutch-speaking Belgian users could automatically make use of its services in Dutch, actively and commercially targets potential users in Belgium and, hence, participates in Belgian economic life.

[2] Court of Appeal Antwerp 20 November 2013, 2012/CO/1054, Belgium/Yahoo! Inc; Cass 1 December 2015, P.13.2082.N, Belgium/Yahoo! Inc.
[3] Criminal Court Mechelen 27 October 2016, No. ME 20.F1.105151-12, Belgium/Skype.

By considering the targeted offering of services a sufficient territorial connecting factor with the Belgian territory, Belgian courts have thus been capable of compelling service providers having their office or establishment abroad to cooperate with the local competent authorities. The approach, if it were to be generalised, confronts international companies with requests or orders to preserve or produce data from all over the world, and undermines legal clarity at both company and user level.

The US is another example. It enacted the Cloud Act[4], thereby amending the Stored Communications Act so as to require service providers to

> *preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States* (McMeley & Seiver, 2018).

With the Cloud Act, the US wanted to counter access blocking by US-based companies to data stored overseas like in the Microsoft Warrant case[5] (Weiss, 2017). In the latter case, the US investigative authorities had issued a warrant under the Stored Communications Act in the context of a US-based drug-trafficking case in December 2013, requiring US-based Microsoft to produce subscriber information and emails associated with an account hosted by it. Microsoft provided the subscriber info, which it held on its US servers, but refused to turn over the e-mails, which were stored in its Irish data centre and consequently subject to EU Regulation 2016/679[6], i.e. the so called General Data Protection Regulation (GDPR). The Cloud Act squeezes companies concerned between two unilateral approaches, i.e. a US obligation to cooperate and an EU prohibition to cooperate, springing from Article 48 GDPR. According to the latter, a judicial or administrative third country order to transfer or disclose personal data may only be recognised or enforceable if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. In a comparable fashion, the Cloud Act makes it possible for *qualifying* governments to get access to records stored in the US that pertain to foreign citizens. A trans-Atlantic bilateral agreement between the EU and the US seems the only way out of the deadlock (*infra*, next paragraph).

Reference must equally be made to the EU's own e-evidence package[7], presented by the European Commission in April 2018. It consists of a proposed e-Evidence Regulation[8] (on

[4] Clarifying Lawful Overseas Use of Data Act 2018 (Cloud Act).

[5] *United States of America v Microsoft Corporation* US 829 F.3d 197 (2d Cir. 2016) (Lynch J); Brief of Amici Curiae Digital Rights Ireland Limited and the Open Rights Group in support of respondent Microsoft Corporation (*United States of America v Microsoft Corporation* US 829 F.3d 197 (2d Cir. 2016)); Brief of EU Data Protection and Privacy Scholars as Amicus Curiae in support of respondent (*United States of America v Microsoft Corporation* US 829 F.3d 197 (2d Cir. 2016)); Brief of Former Law Enforcement, National Security, and Intelligence Officials as Amicus Curiae in support of neither party (*United States of America v Microsoft Corporation* US 829 F.3d 197 (2d Cir. 2016)); Brief Amicus Curiae of U.N. Special Rapporteur on the Right to Privacy Joseph Cannataci in support of neither party (*United States of America v Microsoft Corporation* US 829 F.3d 197 (2d Cir. 2016)).

[6] Regulation (EU) 2016/679 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 (General Data Protection Regulation) [2016] OJ L 119/1.

[7] Council of the European Union, 'Technical document on measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace' (22 May 2017) 9554/17; Council of the European Union, 'Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward' (29 May 2017) 9677/17; European Commission, Inception Impact Assessment on 'Improving cross-border access to electronic evidence in criminal matters' (3 August 2017) Ref. Ares 3896097.

[8] Proposal for a Regulation of the European Parliament and of the Council of 17 April 2018 on European production and preservation orders for electronic evidence [2018] COM (2018) 225 final.

European production and preservation orders) annex Directive[9] (obliging providers offering their services on the EU market, even when having their HQ in a third country, to designate a legal representative in the Union for the receipt of, compliance with and enforcement of European production and preservation orders). The Commission-initiated proposals have been framed in the context of EU MLA but essentially envisage to make MLA between the Member States redundant, be it that the Council has agreed to introduce a notification duty of the judicial authorities of the enforcing Member State when it comes to content data. The EU co-decision procedure necessitates the further agreement by the European Parliament (EP), where the proposals were met with quite some – legitimate – criticism in November 2019, triggering the tabling of some 600 proposed amendments after a debate in the so called LIBE Committee based on a report by its rapporteur, Birgit Sippel[10]. One of the proposals is to include a mandatory notification to the judicial authorities of the enforcing Member State as well as of the country of residence of the person concerned. Hence, further amendments are unavoidable, with limited prospects for an agreed Council/EP any time soon, after the Covid-19 outbreak has prevented EP work on the matter to continue. Nonetheless, the EU has already initiated negotiations with the US, trying to build a bridge between the US Cloud Act and the EU GDPR and future e-evidence rules, following a negotiation mandate from Council already in May 2019[11]. The EU legislative proposals have moreover triggered ample scholarly (Biasiotti, 2018; Buono, 2019; Sallavaci, 2020; Siry, 2019; Smuha, 2018; Tosza, 2018; Vazquez Maymir, 2020) and institutional data protection attention, i.e. by the Working Party 29 and the European Data Protection Board[12].

The above national, US and EU approaches (De Pauw, 2018; Stefan and Fuster, 2018) are nothing but unilateral and single-sided territorial or market (access) *solutions*, based on new sovereignty claims in a globalized information society. Questions remain as to the privatisation of MLA, the likely excessive importance of data location and the resulting legal protection, and the lack of global legal clarity or certainty for multinational market players, let alone for the data subject, i.e. the suspect or person concerned. Bilateral initiatives such as the future EU-US agreement or the US-UK Cloud Act Agreement, signed in October 2019[13], will neither provide a solution to a global problem.

3. The Second Additional Protocol to the Cybercrime Convention: The Council of Europe's efforts towards a global solution[14]

[9] Proposal for a Directive of the European Parliament and of the Council of 17 April 2018 on laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [2018] COM (2018) 226 final.

[10] Draft report of the LIBE Committee of 24 October 2019 on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters [2019] 2018/0108(COD).

[11] Council Decision of 21 May 2019 on authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters [2019] 9114/19.

[12] Statement of the Article 29 Working Party of 29 November 2017 on data protection and privacy aspects of cross-border access to electronic evidence [2017] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610177; European Data Protection Board, 'Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)' (26 September 2018).

[13] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime. The Agreement allows law enforcement bodies from both countries direct access to electronic data stored by companies in the other country, in most cases without the prior judicial authorization required under their current MLA agreement.

[14] This part of the text is a reworked version of the opinion prepared by the author in his expert capacity for discussion by and adopted on 20 November 2019 during the 39th Plenary meeting of the Committee of Convention 108, as presented by the author on 21 November 2019 during the Council of Europe's annual Octopus Conference on cooperation against cybercrime (Vermeulen, 2019a). The adopted version of the Opinion (Opinion of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 20 November 2019 on the provisional text

3.1. Introduction

A wholly different challenge arises at international level, with the Council of Europe (hereafter: CoE) in the lead, trying to shape a solution building on the global framework for cooperation in the area of cybercrime, by drafting a second Additional Protocol to the Budapest Convention on Cybercrime.

Unlike the US or the EU, the Budapest Convention Parties are unable to pursue a single-sided territorial or market (access) solution. The 65 Parties form a complex patchwork of 44 CoE member countries and 21 non-member countries, giving the framework its global character. The data protection is triple. Whilst all 44 CoE and 5 non-CoE Budapest Parties are bound by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)[15] (hereafter: Convention 108), some key non-CoE Budapest Convention Parties like the US, Canada and Australia – all members of the so called *Five Eyes* (O'Neil, 2017; Pfluke, 2019) intelligence and surveillance alliance – are unwilling to accept the high standards of Convention 108 (or its Modernised version[16], i.e. Convention 108 as amended by Protocol CETS 223[17]; hereafter: Convention 108+) to form the data protection backbone for cross-border e-evidence gathering. The divide, however, is also witnessed at intra-European level: amongst the 44 CoE Budapest Parties are 25 EU Member States[18], which have mandated the European Commission to participate on behalf of the EU in the negotiations on the second Additional Protocol to the Budapest Convention[19]. Against the backdrop of the EU's particularly detailed and strict data protection legislation, consisting inter alia of the GDPR and of Directive 2016/680,[20] i.e. the so called Data Protection Law Enforcement Directive (hereafter: LED), the European Commission seems to feel at unease sticking to *mere* Convention 108+ standards.

3.2. Background

Drawing on work of the so called Cloud Evidence Group[21] (Segers, 2018), the Cybercrime Convention Committee (T-CY) started in 2017 to work on the drafting of a second Additional Protocol to the Cybercrime Convention[22], in view of rendering traditional MLA under the

and explanatory report of the draft Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) on direct disclosure of subscriber information and giving effect to orders from another Party for expedited production of data [2019] T-PD(2019)8FIN) differs only in few instances from the authors' draft, which built on an official expert note of his, published in Spring 2019 (Vermeulen, 2019b).

[15] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 28 January 1981, entered into force 1 October 1985) (1981) ETS No. 108.

[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 28 January 1981, entered into force 1 October 1985) (1981) ETS No. 108 as amended by 'Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (opened for signature 10 October 2018) CETS No. 223.

[17] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 10 October 2018) CETS No. 223.

[18] Note that IE and SE are no Parties to the Budapest Convention.

[19] Council decision of 21 May 2019 authorising the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185) [2019] 9116/19.

[20] Directive (EU) 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (LED) [2016] OJ L 119/89.

[21] Council of Europe Cybercrime Convention Committee (T-CY), 'Final report of the T-CY Cloud Evidence Group. Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY' (16 September 2016) T-CY (2016)5; Council of Europe Cybercrime Convention Committee (T-CY), 'Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group' (17 February 2016) T-CY (2016)7.

[22] Council of Europe Cybercrime Convention Committee (T-CY), 'Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime' (8 June 2017) T-CY (2017)3; Council of Europe Cybercrime

Convention more effective (including through the provision of video conference hearing and emergency MLA procedures) and introducing the possibility of *direct disclosure* from service providers in other jurisdictions. Such direct disclosure poses new challenges (*supra*, under 1), implying that data protection safeguards inserted in the Protocol must *also* adequately cover the scenario of direct cooperation, in addition to traditional MLA scenarios to obtain data from service providers.

In June 2018, in preparation of the 2018 annual Octopus Conference[23], the 36th Plenary meeting of the Committee of Convention 108 (T-PD) adopted *provisional answers* to the conference discussion paper on the matter[24], as prepared by the author in his T-PD expert capacity. Further inputs for the discussion were an October 2018 T-CY discussion paper on conditions for obtaining subscriber information in relation to dynamic versus static IP addresses[25] and a T-CY discussion note for a consultation with data protection experts[26], held in Strasbourg in November 2018, in which both the T-PD Secretariat and the author, in his T-PD expert capacity, participated. In May 2019, in preparation of the June 2019 T-PD 38th Plenary, the author also drafted an expert note on the inclusion of data protection safeguards relating to law enforcement trans-border access to data in the second Additional Protocol (Vermeulen, 2019b), which formed the basis for T-PD Opinion (2019)8FIN, which he also prepared and was adopted by the 39Th T-PD Plenary in November 2019[27]. The latter Opinion, which is set out below, was issued in the lead-up to the November 2019 Octopus Conference[28] in response to the related T-CY consultation[29] on its newly released provisional text and explanatory report of provisions the draft second Additional Protocol[30] and its discussion guide for consultations[31], by which it was seeking written comments from stakeholders, including data protection authorities and T-PD. Since, no new or further draft provisions of the second Additional Protocol have been officially released by T-CY.

In the Opinion, we recalled that the second Additional Protocol should adequately reflect the CoE *acquis* on fundamental rights and freedoms, particularly on the protection of personal data. We argued that it is therefore essential to ensure consistency of the second Additional Protocol with Convention 108+ which applies to all data processing carried out in the public and private sectors. The Opinion drew and expanded on a series of elements, listed hereafter, which were

Convention Committee (T-CY), 'Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime: workplan and working methods' (29 November 2017) T-CY (2017)20; Council of Europe Cybercrime Convention Committee (T-CY), 'Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime' (11 July 2018) T-CY (2018)23.

[23] Octopus Conference 2018, 'Cooperation against Cybercrime. Key messages' <https://rm.coe.int/3021-90-octo18-keymessages/16808c67bb>.

[24] Provisional Answers from the Committee of Convention 108 to the Discussion paper for Octopus Conference (11-13 July 2018) <https://rm.coe.int/draft-answers-from-the-committee-of-convention-108-to-the-discussion-p/16808b4688>.

[25] Council of Europe Cybercrime Convention Committee (T-CY), 'Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime. Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments' (25 October 2018) T-CY (2018)26.

[26] Council of Europe Cybercrime Convention Committee (T-CY), 'Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime. Consultation with data protection experts: Issues for discussion' (26 November 2018) T-CY (2018)32.

[27] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Opinion on the provisional text and explanatory report of the draft Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) on direct disclosure of subscriber information and giving effect to orders from another Party for expedited production of data' (20 November 2019) T-PD(2019)8FIN.

[28] Council of Europe, 'Octopus Conference 2019: Cooperation against Cybercrime' (Strasbourg, 20-22 November 2019) <https://www.coe.int/en/web/cybercrime/octopus-interface-2019>.

[29] Council of Europe, 'Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime' <https://www.coe.int/en/web/cybercrime/protocol-consultations>.

[30] Council of Europe Cybercrime Convention Committee (T-CY), 'Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime' (version 1 October 2019) T-CY (2018)23 (hereafter: T-CY Draft / Explanatory report).

[31] Council of Europe Cybercrime Convention Committee (T-CY), 'Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime. Discussion Guide for Consultations with civil society, data protection authorities and industry' (version 18 September 2019) T-CY (2019)28.

already raised in the T-PD provisional answers to the abovementioned discussion paper for the 2018 Octopus conference and/or in the May 2019 expert note:

a. *priority must be given to improving traditional MLA procedures, whereas direct cooperation should be kept for specific cases as an expedited procedure;*
b. *envisaged direct cooperation or expedited MLA procedures should ideally be limited to subscriber information only;*
c. *when pertaining to subscriber information, the data protection, procedural and rule of law safeguards of at least both the requesting and the requested Parties should be taken account of;*
d. *if pertaining to traffic information after all, the data protection, procedural and rule of law safeguards of at least both the requesting Party and the Party where the data subject has used the service(s) should be taken account of;*
e. *envisaged direct disclosure or expedited MLA procedures must be established on a proper legal basis, and be in conformity, as far as transfer of personal data is concerned, with Article 14 of Convention 108+, avoiding systematic reliance on derogations at all price;*
f. *any newly established cooperation regime must comply with other relevant data protection requirements, such as re the limited storage of data, subsequent use of data, processing of sensitive data, data breach notification, transparency, accountability, and effective independent oversight;*
g. *any newly established disclosure regime must either be framed in a unified data protection regime, based on Convention 108+, ideally by inviting Parties to join the latter, or in an optional data protection regime, comparable with that of Article 26.3, 2nd indent of ETS 182, allowing for the combined application of the data protection regimes of the relevant Parties, in line with their national and international data protection commitments, and reflecting compliance with a range of jointly established substantive data protection principles, in line with Convention 108+.*

3.3. Data protection lookouts for the second Additional Protocol

The below text provides the provisional T-PD position on the newly released provisional text and explanatory report of the draft second Additional Protocol regarding specifically the articles on direct disclosure of subscriber information (*infra*, under 2.3.1) respectively giving effect to orders from another Party for expedited production of data (*infra*, under 2.3.2). Provisional text of other provisions submitted to consultation fell out of T-PD's scope and are therefore not commented on.

In a note preceding the draft text and explanatory report of the articles concerned, T-CY had set out that these "*may change as the negotiations develop, depending on the outcome of* other provisions that have not yet been prepared and/or other comments received" and that they

> *should be considered by the [T-CY Protocol Drafting Group and Protocol Drafting Plenary] in order* to determine whether further changes are required […] *(in view of the unique circumstances of direct cooperation between authorities and providers) once the* ongoing work on conditions and safeguards, including with regard to data protection and privacy, *has resulted in a text and explanatory report* [emphasis added].

Consequently, we chose not to limit the opinion to the provisional text and explanatory report of both articles concerned, but to equally use it as a vehicle to provide provisional T-PD input for T-CY's ongoing/future work on conditions and safeguards with regard to data protection. Reference here is made to page 18, point 4.2, paragraph 11, *in fine*, respectively page 29, point 5.2, paragraph 19-20 of the draft explanatory report (to paragraph 2 of the draft article on direct

disclosure of subscriber information respectively paragraph 8 of the draft article on expedited production of data between traditional authorities). In these instances, T-CY explicitly envisaged to include an article in the second Additional Protocol to data protection conditions and safeguards. Of course, the T-PD opinion is in this regard intrinsically dependent on the content of that important future article, which is currently being negotiated but of which no provisional text has been officially released.

3.3.1. Direct disclosure of subscriber information

In line with the proposed scoping in the explanatory report (on pages 16-17, in point 4.2, paragraph 4) of subscriber data as potentially inclusive of both static and dynamic IP addresses:

> *Information needed [in specific cases] for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time*,

we recognised in the opinion that access to both static and dynamic IP addresses may be required in specific cases for the sole purpose of establishing the information as meant in Article 18.3 of the Budapest Convention. However, subscriber data should never be inclusive of any (other) traffic data or content data. Hence, we recommended to specify under which circumstances IP addresses could be considered as subscriber information, as meant in Article 18.3 of the Budapest Convention[32], especially paying due attention to the fact that, depending on the circumstances, an IP address may be evidence of who owns a subscriber account, but does not necessarily identify the individual user at any given time. Moreover, we only supported the potential inclusion of IP addresses under subscriber information if it is specified in the actual Protocol text (both in the articles on direct disclosure and traditional orders for expedited disclosure) as well as in the corresponding parts of the explanatory report that IP addresses are to be used solely for identification purposes and in specific cases only.

Given that some Parties, for constitutional or other principled reasons[33], treat dynamic IP address information as traffic data, T-CY has suggested, through the insertion of paragraph 9.b of the draft text, to allow such Parties to reserve the right not to apply the provision on disclosure of subscriber information to "*certain types of access numbers*"[34]. In the T-PD opinion, we expressed concerns that this proposed solution might lead to a fragmented regime for criminal cooperation and the protection of personal data, thus impacting the effectiveness of the Protocol.

Along the same lines, we noted the full opt-out possibility (in point 9.a of the draft text) for Parties not to apply the direct disclosure regime. Due to the fragmentation that is likely to arise from the variability of regimes, the *"[high] expectations set for the new Protocol*", in that it "*will need to stand the test of time in order to make a difference in terms of an effective criminal justice response with human rights and rule of law safeguards*"[35], may not be met. If introduced at all, any new direct disclosure regime should be sufficiently straightforward and binding for all ratifying Parties, sustainably building on a common commitment to shared data protection conditions, safeguards or principles (*infra*, under 2.3.5 and 2.3.6).

[32] See also: Council of Europe Cybercrime Convention Committee (T-CY), 'T-CY Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention)' (1 March 2017) T-CY (2015)16.
[33] As documented in the afore mentioned T-CY discussion paper on conditions for obtaining subscriber information in relation to dynamic versus static IP addresses.
[34] Also reflected in the proposed explanatory report on page 17, in point 4.2, para 4: 'Accordingly, paragraph 9.b provides a reservation for some Parties'.
[35] See the afore mentioned T-CY discussion guide for the 2019 Octopus Conference, *in fine*.

As concerns notification of the official authorities of the Party in which the service provider is present with which direct cooperation is established, we also urged the T-CY drafters to turn the optional notification possibility foreseen under point 5 into a mandatory notification regime.

3.3.2. Expedited production of data

Whilst the explanatory report to paragraph 4 of the proposed text on traditional orders for expedited production of data[36] rightly points out that "*under some Parties domestic laws, the production of traffic data may require further information because there are additional requirements in their laws for obtaining such data"*, we questioned in the T-PD opinion the position that the only consequence thereof is that "*additional information may need to be provided to the requested Party in order for it to give effect to the order*". The possibility of an opt-out from the regime as far as traffic data is concerned, as foreseen in paragraph 12 of the proposed text, is equally insufficient.

The mere reference to potentially higher domestic standards or the opt-out possibility for Parties in relation to obtaining traffic data does not adequately capture the principled and historical distinction the Budapest Convention has made between measures relating to subscriber data vs. measures relating to traffic data. Such principled distinction should not be sacrificed for alleged reasons of efficiency.

More fundamentally, in line with the afore mentioned T-PD provisional answers to the discussion paper for the 2018 Octopus Conference, we took the principled position in the T-PD opinion that, as a minimum requirement, a Protocol regime for disclosure of traffic data should allow for the *combined* data protection, procedural and rule of law safeguards of at least the Party of the requesting competent authority and the "*Party where the data subject was present whilst using the targeted service(s)"*, if different from the requesting Party or the Party where the service provider is present. A person who is communicating or using services in a Party's territory has a legitimate expectation of privacy under primarily the laws of that Party. As soon as it is possible to establish, based on the prior obtaining of subscriber data, where a person was while using any targeted service(s), it is key for the Protocol to make sure that the data protection, procedural and rule of law safeguards of the latter Party may be applied and complied with. If that Party is the Party where the order originates from, such assurance is implied already. Only in such case, the Protocol may suffice allowing for the *combined* data protection, procedural and rule of law safeguards of at least the *Party of the requesting competent authority* and the *Party where the service provider [or executing competent authority] is located* (as also reflected *infra*, under 2.3.5). The Protocol should moreover contain specific provisions which would guide Parties in case of conflict of laws, in that the laws offering the widest protection to the data subject will apply.

3.3.3. Insufficient criteria for service providers' territorial "presence"

Both the suggested direct disclosure and traditional cooperation mechanism pertain to the obtaining of data from service providers in another Party's territory. The related draft explanatory report to both mechanisms[37] reads as follows:

> [T]he term 'a service provider in the territory of another Party' requires that the service provider be physically present in the other Party. Under this Article, the mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not

[36] Explanatory report, p. 28, point 5.2, para. 14.
[37] See Explanatory report, respectively para 10, p. 18, and para. 5, p. 26.

constitute the service provider being 'in the territory' of that Party. Paragraph 1 requires, in addition, that the data be in the service provider's possession or control.

In the T-PD opinion, we insisted that further clarification be added, ideally in the text of the draft articles themselves, if not at least in the corresponding parts of the explanatory report, on when a service provider will be considered "physically present" in a Party's territory. Against the back-drop of the significant jurisprudential contention in the past decade around jurisdiction over service providers abroad, in which a multitude of criteria (a range of "*establishment*" criteria[38], "*offering*" criteria etc.) has passed in review, the above two criteria (negatively: that a contractual relationship does not suffice; positively: that data must be in the service provider's possession or control) seem insufficient to bring optimal clarity. Such clarity, however, is crucial for any future mechanism not to be undermined as well as to avoid forum shopping by authorities or Parties – which would be avoided if mandatory common safeguards were to be incorporated in the Protocol. Not only may the latter confront multinational service providers with parallel orders issued to its establishments or branches in several jurisdictions, it may also encourage authorities or Parties to opt for sending orders to the jurisdiction of presence of the service provider where the lowest data protection standards apply. Hence, it is of key relevance to add more clarity, e.g. drawing inspiration from the proposed criteria in the draft EU e-Evidence Regulation[39], by stipulating in the Protocol or in the explanatory report that a service provider will be considered 'physically present' in a Party's territory when it has a stable infrastructure through which it actually pursues an economic activity for an indefinite period and from where the business of providing services is carried out or managed.

3.3.4. Confidentiality

The explanatory report to paragraph 4.f of the envisaged article on disclosure of subscriber information[40] clarifies that the "*special procedural instructions*" that need to accompany a disclosure order submitted to service providers are meant to "cover, in particular, any request for confidentiality, including a request for non-disclosure of the order to the subscriber or other third parties". Even if we see no difficulty with this, we have requested in the T-PD opinion to reconsider the opening left in the further explanation given for domestic laws or discretionary policies of service providers that would not guarantee the confidentiality sought ("*Therefore, in order to avoid the risk of premature disclosure of the investigation, Parties are encouraged to be aware of applicable law and a service provider's policies concerning subscriber notification, prior to submitting the order under paragraph 1 to the service provider*"). Whilst confidentiality may be important to maintain efficiency in criminal investigations, it may equally be vital in safeguarding data protection. Hence, we favour the inclusion of a self-standing provision on confidentiality in the Protocol, for which we suggested inspiration is drawn from:

- Articles 26.2 of the Budapest Convention (ETS 185): "*Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them";*

[38] As initially accepted in Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317. See Court of Justice of the European Union, 'Press Release No 70/14' (13 May 2014).
[39] Proposal for a Regulation of the European Parliament and of the Council of 17 April 2018 on European production and preservation orders for electronic evidence [2018] COM (2018) 225 final.
[40] See Explanatory report, p. 19, point 4.2, para. 17.

- Articles 27.8 of the Budapest Convention (ETS 185): "*The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed*";
- Article 25 of the Second Additional Protocol to the Convention on MLA in criminal matters (ETS 182): "*The requesting Party may require that the requested Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting Party".*

The explanatory report to the envisaged article on traditional orders for the expedited production of data[41] clarifies that *"[u]nder paragraph 3.c, the request should also include all special instructions, including for example requests for certification or confidentiality under Article 27.8 of the Convention, at the time of transmission to ensure the proper processing of the request*". Whilst we support the reference to confidentiality and to Article 27.8 of the Budapest Convention, we have stressed in the T-PD opinion that, from the draft T-CY text as it stands, it cannot be derived that Article 27.8 of the Budapest Convention applies in a Protocol context. The reference, however, underlines the importance (*supra*) for a self-standing provision on confidentiality to be included in the Protocol itself, for both the direct and the traditional mechanism for obtaining information from service providers.

3.3.5. Data protection conditions and safeguards

In the absence of a draft text for the envisaged article on data protection (*supra*, under 2.3), we raised particular concern in the T-PD opinion regarding the non-insertion in the draft text and explanatory report of two-directional data protection conditions, including for asymmetrical transfers under the direct disclosure of subscriber information regime[42], but equally for traditional MLA to giving effect to orders for expedited production of data[43].

In the T-PD opinion, we therefore stressed the importance of making sure, at least, that data protection conditions and safeguards will be inserted in the Protocol, applicable in two directions, since the receiving entity may be:

- either a competent authority:
  - in the case of traditional MLA: both the requesting and requested authority being the recipient of personal data, i.e. of the personal data provided in the request or of the personal data transferred as a result of the execution of a request;
  - in the case of direct, asymmetrical transfers: the requesting authority being the recipient of personal data transferred by a private data controller (service provider);
- or a private data controller (service provider), which, in the case of direct, asymmetrical transfers is the recipient of personal data provided in the request.

The draft text and explanatory report as they stand, remain silent on the matter, save for a double reference in the explanatory report to paragraph 2 of the proposed draft text on direct, asymmetrical disclose of subscriber information[44], and a single reference in the explanatory report to paragraph 8 of the draft article on expedited production of data between traditional authorities.[45] The three references are exclusively targeted at "*parties that have data protection*

[41] See Explanatory report, p. 26, point 5.2, para. 8.
[42] See point 4 of the T-CY draft.
[43] See point 5 of the T-CY draft.
[44] See Explanatory report, p. 18, point 4.2, para. 11.
[45] See Explanatory report, p. 29, point 5.2, paras. 19 and 20.

requirements" (first two) or would wish to limit or refuse cooperation based on "*conditions and safeguards (including with regard to data protection)*" (third). The first reference is only a reminder to parties having data protection requirements of their obligation under domestic laws to provide "*a clear basis for the processing of personal data*" by service providers in response to an order which they directly received. The second reference relates to international data transfers, without, however, stipulating the actual safeguards that a service provider may require (from the recipient Party or authority) to be able to transfer "*responsive subscriber information*". In contrast, the explanatory text only features a blank cross-reference to a future article on data protection, whilst axiomatically stating that (a Party's implementation law for) the Protocol reflects the 'important public interest' of the direct cooperation regime (discussion continued *infra*, next para). The framing of the third reference is of concern: the explanatory report[46] warns that "*mutual assistance is in principle to be extensive, and impediments thereto strictly limited"*, so that "*accordingly, conditions and refusals should also be limited in line with the objectives of this Article to eliminate barriers to transborder sharing of subscriber information and traffic data and to provide more efficient and expedited procedures than traditional mutual assistance*". It must be stressed that labelling data protection conditions and safeguards as potential "*impediments"* and "*barrier"'* is inappropriate and does not reflect the balanced functioning of democracies safeguarding human rights and the rule of law. It is furthermore not in line with the case-law of the European Court of Human Rights. Hence, in the T-PD opinion, we emphasized that the efficiency of cooperation would be genuinely enhanced when embedded in a shared commitment to respect common data protection principles.

In claiming that the envisaged direct disclosure regime in the Protocol reflects an "*important public interest*" (*supra*, in the previous para), the T-CY proposal seeks to base the entire direct disclosure concept exclusively on the derogations provided in Article 14.4.c of Convention 108+ and, as far as EU Member States are concerned, in Articles 49.1(d) *juncto* 49.4 GDPR [emphasis below added]

> Article 14.4 Convention 108+ – Transborder flows of information
>
> *Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if: […] c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; […].*
>
> Article 49 GDPR – Derogations for specific situations
>
> 1. *In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: […] (d) the transfer is necessary for* important reasons of public interest; […].
>
> 4. *The* public interest *referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.*

Confirming the position set out in the provisional T-PD answers to the discussion paper for the 2018 Octopus Conference and emphasised in my afore mentioned expert note T-PD(2019)3, we expressed firm disagreement in the T-PD opinion with the above approach, and opposed the

[46] See Explanatory report, p. 29, point 5.2, para. 20.

envisaged structural and systemic reliance on derogations as a standardised means to allow for direct, asymmetrical transfers.

In contrast, we reiterated the position that the most straightforward, sustainable and widely acceptable way to guarantee an appropriate level of data protection under the Protocol would be the accession by the Protocol Parties to Convention 108+. As a result, an appropriate level of data protection would be generically guaranteed by all Parties to the Protocol and indirectly become a default standard also for the application amongst them of the Budapest Convention itself.

In a subsidiary manner, i.e. where the option of accession by the Protocol Parties to Convention 108+ (*supra*) would not prove feasible, we favoured the incorporation in the Protocol (as a legally binding instrument between the Parties) of common mandatory data protection safeguards [list as included *infra*, under 2.3.6], grounded in, closely aligned with and consistently interpreted in line with Convention 108+.

In an even more subsidiary manner and as an absolute minimum, in line with my expert note T-PD(2019)3, we urged T-CY to take Article 26 (pertaining to "*Data protection*") of the second Additional Protocol to the Convention on MLA in criminal matters (ETS 182) as a point of departure, thus ensuring consistency with at least the CoE's data protection *acquis* in the context of judicial cooperation in criminal matters. This would imply insertion in the Protocol (as a legally binding instrument between the Parties) of an optional regime, comparable with that of Article 26.3, 2nd indent of ETS 182:

> Any Party may refuse to transfer personal data obtained as a result of the execution of a request made under the Convention or any of its Protocols where […] the Party to which the data should be transferred is not bound by [Convention 108+], unless the latter Party undertakes to afford such protection to the data as is required by the former Party,

which would need to be rephrased, so as to enable two-directional applicability, both in the context of direct transfers and transfers between traditional competent authorities.

Further, in case the Protocol Parties were not all to accede to Convention 108+ or no new, mandatory data protection conditions and safeguards were to be inserted in the Protocol, we suggested, in order to enable and ensure (and if necessary: enforce) compliance by private data controllers (service providers) with the data protection conditions and safeguards in the Protocol (i.e. a public international law instrument, incapable of directly binding private parties), to stipulate in the latter that if a data controller or competent authority of a Party requires an appropriate level of data protection in the receiving Party, such condition shall be considered to be met if:

> *the receiving competent authority or data controller of the latter Party undertakes to process the personal data transferred subject to the conditions and safeguards under the domestic law of the former Party [ie the Party from where personal data would be transferred], including obligations upon the latter under Convention 108 and its Protocol and/or other applicable bilateral, regional or international data protection agreements or instruments guaranteeing the protection of individuals by the implementation of at least the following safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+ [list as included infra, under 2.3.6]*

In doing so, as a minimum requirement, as posited also in the provisional answers to the discussion paper for the 2018 Octopus Conference and my expert note T-PD(2019)3, a Protocol regime for disclosure of subscriber data should allow for the *combined* data protection obligations of at least the Party of the requesting competent authority and the Party where the

service provider or executing competent authority is located. This would also be a step forward into international harmonisation of data protection requirements in the field of criminal justice cooperation.

Since an undertaking as above lacks the "*legally-binding and enforceable*" character of safeguards as required under Article 14.3.b of Convention 108+, we further suggested, in line with my expert note T-PD(2019)3, to introduce an additional obligation in the Protocol for Parties to stipulate in their domestic legislation that violations of such undertaking by a receiving competent authority or data controller in their territory may give rise to all judicial and non-judicial sanctions and remedies available under their laws.

Whilst paragraph 1 of both of the draft articles on direct and traditional, expedited ordering of information limits the issuing of orders to information which is needed for the issuing Party's specific criminal investigations or proceedings, the draft text remains fully silent on the purposes for which transferred personal data can be used by the receiving competent authority or service provider. In this regard, we furthermore recommended to include explanations at least in the Explanatory Report on a commonly agreed distinction between data processing (including transfers) for criminal investigation purposes and those undertaken for national security purposes in line with the Issue paper "Democratic and effective oversight of national security services"[47], published by the CoE Commissioner for Human Rights.

We also requested in the T-PD opinion to insert clear use restrictions in the Protocol, applicable to both direct and traditional, expedited cooperation. We suggested phrasing such use restrictions based on the provisions of Article 26 of ETS 182 (*supra*), amending them *mutatis mutandis* and extending them to also cover use limitations upon a service provider to which a request is transferred. This could translate in three provisions, in which it is stipulated respectively that:

1. [*mutatis mutandis* adaptation of Article 26.1 ETS 182] personal data transferred by a competent authority or data controller of a Party as a result of the execution of an order issued under the Protocol by a competent authority of the receiving Party, may be used by the latter only:
   a. for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence within the scope of articles 14.2 and 25.1 of the Budapest Convention;
   b. for other judicial and administrative proceedings directly related to the proceedings mentioned under (a);
   c. for preventing an immediate and serious threat to public security;
2. [*mutatis mutandis* adaptation of Article 26.2 ETS 182] such data may however be used by the competent authority for any other purpose if prior consent to that effect is given by either the Party from which the data had been transferred, or the data subject.
3. [extension to cover use limitations for service providers] the request received and the information it contains can only be used by the receiving service provider for the purpose of the execution of an order issued under this Protocol.

3.3.6. Substantive data protection principles

To the extent that the option of accession by the Protocol Parties to Convention 108+ (*supra*) does not prove feasible, we urged in the T-PD opinion that the below safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+, would be

[47] Council of Europe, 'Democratic and effective oversight of national security services' [2015] <https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb> accessed 15 October 2020.

incorporated in the Protocol as mandatory common safeguards. In an even more subsidiary manner, we urged that, as an absolute minimum, the Protocol would and will allow service providers or competent authorities to require, as a precondition to transferring any personal data, the receiving competent authority or service provider to undertake to process the personal data transferred subject to the conditions and safeguards under the domestic law of the Party from where personal data would be transferred, guaranteeing the protection of individuals by the implementation of at least the following safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+ [allowing flexibility as to possible re-ordering, clustering etc.]:

a. purpose legitimacy, purpose specificity and purpose limitation;
b. lawfulness;
c. fairness and transparency;
d. necessity for and proportionality to the legitimate purpose pursued;
e. non-excessive data processing and data minimisation;
f. adequacy, relevance and accuracy of data;
g. data retention limitation;
h. accountability of controllers and processors;
i. logging, data security and data breach notification duty;
j. information security
k. specific, additional safeguards for special categories of sensitive data;
l. lawful use of exceptions and derogations;
m. enforceable data subjects' rights and effective administrative or judicial redress;
n. appropriate protection in (onward) data transfers;

3.4. free, specific, informed, unambiguous and explicit consent where consent of the data subject, having had the right to legal counsel, is the legal basis; [48]

[48] Note that the T-PD Plenary decided not to formally retain this point in the list, whilst it did recognize (see footnote 1 of the T-PD opinion) the author's point that to allow for consent of the data subject as a basis for further use could be supported in the very context of use restrictions in the future Protocol regime, as also suggested *supra*, under 3.2.5, *in fine*, under 2. Admittedly, if narrowly addressed from a data protection perspective, the consent of the data subject ought to be avoided as a ground for data processing in the context of judicial and law enforcement cooperation in criminal matters. The contemporary data protection perspective, as enshrined inter alia in the LED (recitals 35 and 37) excludes reliance on the data subject's consent as an autonomous legal ground for the processing of personal data by judicial or law enforcement authorities, arguing that consent can never be 'freely given' in such context. However, it should be stressed that the possibility of reliance on the consent of the person concerned is formally part of the contemporary *acquis* of MLA in criminal matters, both at CoE (Article 26.2 ETS 182) and EU level (Article 23.1, under (d) of the EU MLA Convention of 29 May 2000, which was not abrogated from by the 2014 European Investigation Order Directive). The possibility to rely on consent of the person concerned in fact functions here as an extra guarantee for that person in the context of the so-called specialty principle (which is the traditional correlative of the purpose limitation principle in data protection law). The specialty principle traditionally has a trust function: the requesting sate or authority ought not to use data for other purposes than the initial purposes, so as not to betray the trust put in it by the executing state or authority in sending the data concerned for those initial purposes. Since the requested state or authority might have refused cooperation or data transfer for other than the initial purposes, the specialty principle stipulates that additional consent of the executing state or authority must be sought in case of intended use beyond the initial purposes (comparable with the control principle in data protection law). The express possibility in Article 26 ETS 182 (which was copied from Article 23.1, under (d) of the 2000 EU MLA Convention) is reflective of its hybrid nature: the ability for the person concerned to agree to the surpassing of initial purpose limitations by the requesting state finds it origin in the specialty principle as it has developed in the context of extradition, surrender or the transfer of persons (supra), where the possibility for the person concerned to impact the otherwise inter-state or inter-authority cooperation process in criminal matters has only slowly made its way in. Cooperation in criminal matters had traditionally been a context in which the person concerned was only the object of cooperation instead of its subject, ie a person with its own voice and its own interests, gradually being entitled certain subjective rights, such as the right to be heard or even the right to object, the rights to legal remedies, the right to be assisted by a lawyer, the right to ask for investigative measures *à décharge*, or even the right to ask to not invoke grounds for refusal when deemed against its interest. Against this backdrop, the recognition by Article 23 that use of information beyond its initial purpose may be allowed based on the consent of the data subject functions as an extra guarantee, in that the person concerned may deliberately want such use, whilst the requested or executing state or authorities see no interest in allowing it. It marked the first recognition of a subject-triggered stretching of the specialty rule as an informational use limitation,

o. effective independent oversight.

Finally, we stressed the importance of the effectivity of the data protection safeguards and of ensuring Parties to the second additional Protocol to effectively apply and enforce them in practice. Hence, we proposed that an evaluation of the implementation of the data protection safeguards be carried out, possibly relying on the findings and recommendations of the mechanism introduced in Article 4.3 of Convention 108+ for Parties to Convention 108+, and, for other countries, on Article 23.f of Convention 108+. The articulation of the work of the T-CY and of the Committee of Convention 108+ in that regard should be further examined.

4. Conclusion

The global digital arena leaves little scope for an easy e-evidence *solution*. Competing and conflicting interest of states, companies and the data subjects/persons concerned are at stake, with traditional jurisdictional rules and MLA being overhauled. Unilateral and single-sided territorial or market (access) approaches at national or regional level, even when reaching out to one another bilaterally, are unlikely to offer a satisfactory way forward. Even if they won't and can't be halted, a more global effort is key, especially for overcoming diverging data protection standards, which increasingly and irreversibly interplay and interfere with traditional MLA schemes. Surely the rights of companies to freedom of establishment and the right to conduct business and offer services in a global market cannot be denied. Neither can their responsibility as data controllers or the importance of data storage location and the resulting data protection regimes. At the same time, attributing private companies a formal role in inter-state cooperation in criminal matters is a risky avenue. Taking account of the complexity of the e-evidence issue, the CoE's global efforts to find common ground in a second Additional Protocol to the Budapest Convention, make sense, even if it remains to be seen whether the mountain will not merely give birth to a mouse. Asymmetrical direct cooperation possibilities will surely (and luckily) remain stricter framed in an MLA context, whilst respecting the principled distinction between measures re subscriber+ data (i.e. inclusive of IP addresses, even if dynamic, where necessary for identification purposes in specific cases), traffic data and content data. Undoubtedly, the CoE level offers the best prospects for providing an internationally acceptable and sustainable data protection backbone for transnational e-evidence gathering. It equally offers the best chances not to let alleged reasons of efficiency dictate the contours of the debate to the detriment of the data subject or person concerned. The rights position of the latter will only be guaranteed properly where the option is taken to work with the *combined* data protection and procedural safeguards of at least the country of the requesting competent authority and the country where, in the case of subscriber+ data, the service provider is located, or, in the case of traffic data, the person concerned or data subject was present whilst using a given service. It's about time to put a person's legitimate expectation of privacy back at the forefront.

be it limited in scope to the use of the data subject's own personal data. On the importance of a possibility to surpass limitations and (even mandatory) refusal grounds upon the express request of the defence or person concerned, see: Sjöcrona, 1990, quoting also Nagel, 1988: 'Es liegt also nahe, eine flexibelere Handhabung der Kriterien für die Fälle vorzusehen, in denen es um die Erhebung von Entlastungsbeweisen geht'; Commissie tot bestudering van de positie van verdachten en andere belanghebbenden in de internationale strafrechtelijke samenwerking, 1993; Vermeulen et al, 2002. The latter have even proposed a fully-fledged provision on the matter in their draft Belgian code of international cooperation in criminal matters.

5. References

Bartunek, R.J. (2017, November 15). Skype loses Belgian court appeal after fails to comply with call data order. *Reuters*, retrieved from http://www.reuters.com.

Biasiotti, M.A. (2018). Present and Future of the Exchange of Electronic Evidence in Europe in Biasiotti MA, Bonnici JPM, Cannataci J and Turchi F (eds), *Handling and Exchanging Electronic Evidence Across Europe*. Cham: Springer.

Buono, L. (2019). The genesis of the European Union's new proposed legal instrument(s) on e-evidence: Towards the EU Production and Preservation Orders. *ERA Forum* 19(3), 307-312.

Commissie tot bestudering van de positie van verdachten en andere belanghebbenden in de internationale strafrechtelijke samenwerking (1993). *Individu en internationale rechtshulp in strafzaken*.'s Gravenhage.

Daskal, J. C. (2018). Borders and Bits. *Vanderbilt Law Review*, 71(1), 179-240.

de Hert, P., & Kopcheva, M. (2011). International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case. *Computer Law & Security Review*, 27(3), 291-297.

Depauw, S. (2018). Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0?. *European Criminal Law Review*, 8(1), 62-82.

De Schrijver, S. and Daenens, T. (2013 September 27). The Yahoo! Case: The End of International Legal Assistance In Criminal Matters. *Who's Who Legal*, <https://whoswholegal.com/features/the-yahoo-case-the-end-of-international-legal-assistance-in-criminal-matters >.

L'Ecluse, P. & D'hulst, T. (2016 January 11). Supreme Court Condemns Yahoo For Failure To Cooperate With Belgian Law Enforcement Officials. *Mondaq*, <http://www.mondaq.com/x/456514/Corporate+Commercial+Law/Supreme+Court+Condemns+Yahoo+For+Failure+To+Cooperate+With+Belgian+Law+Enforcement+Officials>.

McMeley, C. & Seiver, J. (2018, February 28). The CLOUD Act, A needed fix for U.S. and foreign law enforcement or threat to civil liberties. *Iapp* <https://iapp.org/news/a/the-cloud-act-a-needed-fix-for-u-s-and-foreign-law-enforcement-or-threat-to-civil-liberties/>.

Miglio, A. (2017). Back to Yahoo!? Regulatory clashes in cyberspace in the light of EU data protection law in Vermeulen G and Lievens E (eds), *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data*. (pp. 101-122) Antwerpen: Maklu.

Nagel, K.F. (1988). *Beweisaufnahme im Ausland*. Freiburg: Max-Planck-Inst. für Ausländ. u. Internat. Strafrecht.

O'Neil, A. (2017). Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance. *Australian Journal of International Affairs*, 71(5), 529-543.

Weiss P (2017, October 10) 'In Microsoft, U.S. Supreme Court Will Review Extraterritorial Reach of Search Warrants. *Paul Weiss*, <https://www.paulweiss.com/media/3977440/19oct17-microsoft.pdf>.

Pfluke C. (2019) 'A history of the Five Eyes Alliance: Possibility for reform and additions. 38 *Comparative Strategy*, 38, 302-315.

Gewijzigde veldcode

Robinson, G. (2018). The European Commision's e-Evidence Proposal. *European Data Law Review*, 3, 347-352.

Sallavaci, O. (2020). 'Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters' in Jahankhani, H., Akhgar, B., Cochrane, P. and Dastbaz, M. (eds), *Policing in the Era of AI and Smart Societies*. Springer.

Seger, A. (2018). e- Evidence and Access to Data in the Cloud Results of the Cloud Evidence Group of the Cybercrime Convention Committee' in Biasiotti MA, Bonnici JPM, Cannataci J and Turchi F (eds), *Handling and Exchanging Electronic Evidence Across Europe*, Springer.

Siry, L. (2019). Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens. *New Journal of European Criminal Law*, 10(3), 227-250.

Sjöcrona, J.M. (1990). *De kleine rechtshulp. Nederlands procesrecht ten behoeve van buitenlandse justitie en politie. Een onderzoek naar de betekenis van de artikelen 552h-552q van het Wetboek van Strafvordering*. Gouda: Quint BV.

Smuha, N. A. (2018). Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency. *European Criminal Law Review*, 8(1), 83-115.

Stefan, M., & González Fuster, G. (2018 November). Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters, State of the art and latest developments in the EU and the US. *CEPS*, <www.ceps.eu> .

Tosza, S. (2019). 'The European Commission's Proposal on Cross-Border Access to E-Evidence. *Eucrim*, 2018(4), 212-219.

Valgaeren, E. (2017, February 24). Skype Luxembourg condemned in Belgium for refusing to set up wiretap. *Stibbe*, <https://www.stibbe.com/en/news/2017/february/skype-luxembourg-condemned-in-belgium-for-refusing-to-set-up-wiretap>

Vazquez Maymir, S. (2020). Anchoring the need to revise cross-border access to e-evidence' (2020) 9 Alexander von Humboldt Institute for Internet and Society 1.

Vermeulen, G., Vander Beken, T., De Busser, E., Van den Wyngaert, C., Stessens, G., Masset, A., Meunier C. (2002). *Een nieuwe Belgische wetgeving inzake internationale rechtshulp in strafzaken* Maklu.

Vermeulen, G. (2019a). International transfer of data in a criminal investigation Article 14 of Convention 108+ in practice. T-PD opinion on the provisional text & explanatory report of the draft 2nd Additional Protocol to the Budapest Convention on the direct disclosure of subscriber information and giving effect to orders for the expedited production of data (Octopus Conference, Council of Europe, Strasbourg).

Vermeulen, G. (2019b). Inclusion of data protection safeguards relating to law enforcement trans-border access to data in the Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) (Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, T-PD(2019)3, Strasbourg, <https://rm.coe.int/inclusion-of-data-protection-safeguards-relating-to-law-enforcement-tr/168094b73a>.

Warken, C., van Zwieten, L., & Svantesson, D. (2020). Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence. *International Review of Law, Computers & Technology*, 34(1), 44-64.