CyberEast

Public/Private Cooperation under the Partnership for Good Governance with Eastern Partnership countries

23rd May 2022

Study on Law Enforcement access to data from Multinational Service Providers for use in criminal proceedings

Prepared by Council of Europe experts
CyberEast Project

www.coe.int/cybercrime

Partnership for Good Governance

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Email cybercrime@coe.int

Disclaimer
This review has been prepared by independent Council of Europe experts Markko Kunnapu and Rajka Vlahovic.

Contents

1 Introduction

Cooperation between the criminal justice and private sectors has long been accepted as a necessity in order to protect society from crime. Today, pervasive abuse of the internet for criminal purposes means that a growing proportion of criminal evidence, both of cyber and other crimes, is electronic. This fact more than ever underlines the importance of effective cooperation between those responsible for enforcing the law and conducting criminal investigations, (police and prosecutors) and service providers in the business of offering Internet based services to the public. Such services are related to (inter alia) webmail, hosting, social networking, online marketplaces, online gaming platforms, virtual private networks and virtual currencies. The most significant of these service providers, and also the focus of this study, are the multi-national service providers (MSPs), the companies known as Apple, META (Facebook, Messenger, Instagram, WhatsApp), Google, Microsoft, Yahoo!, Twitter. All of these companies have a global reach and operate from businesses headquartered in the USA, often with regional offices in Europe. This means that cooperation between these companies and law enforcement authorities for the purposes of obtaining data for use as evidence frequently takes place across borders and it is this cross-border process which is addressed in this study.

The present study is a follow-up to the earlier: *Study on Strategy of Cooperation with Multinational Service Providers*[1] prepared by the Council of Europe in 2017. Although the practices of individual countries have remained constant, numbers of requests for data, being sent directly to MSPs by law enforcement, are increasing annually. As the direct cooperation model has also been recommended as a possible option and facilitated by various international conferences and in discussions with service providers, law enforcement in some countries have become aware of the possibilities and more adept at avoiding problems. In addition, the international landscape has changed significantly and international organisations such as Council of Europe and also the European Union, as well as individual countries, have taken legislative steps and adopted other measures to promote and facilitate such direct cooperation.

Specifically with regard to the Eastern Partnership (EAP) region, during the five years that have elapsed since the last study, the EAP region has become more integrated into the global economy, and as in other regions in the world, its inhabitants have benefited from the continuing development of technology, access to the internet and related services offered by the above mentioned MSPs. Although the services in question may be available to users in the EAP region, the data generated by the users through use of the services are invariably stored in the US where the MSP is based, or potentially in a third location. This means that although law enforcement in one of the EAP countries may be investigating a domestic offence within their jurisdiction, relevant data may well be held (or be accessible) in the USA or elsewhere in a third location. In these circumstances international cooperation processes must be deployed in order to access data for use as evidence.

As indicated above, the focus of this study is the international cooperation process supporting access to data from MSPs by law enforcement outside the USA for use in criminal proceedings in their country. The study will outline relevant options available to law enforcement including access to data using the traditional method of treaty based mutual legal assistance (MLA); it will explain the reasons for the growth of direct cooperation between law enforcement and MSPs when it is appropriate to rely on this as a cooperation model, detailing difficulties and conflicting priorities arising in the course of such cooperation.

[1] https://rm.coe.int/study-on-strategy-of-cooperation-with-multinational-service-providers/16808f1e16

The study will discuss the growing acceptance of direct cooperation, the new legal frameworks such as the Second Additional Protocol to the Convention on Cybercrime[2] and the US Clarifying Law on Overseas Use of Data (CLOUD Act)[3] which support it, and which are intended to provide a greater degree of legal certainty lacking to date in direct cooperation. Additionally, the study aims to provide practical information and recommendations for law enforcement seeking access to data from MSPs.

Whilst it is recognised that direct cooperation has been a feature of international cooperation in criminal matters for some time, as stated above, it has only recently been placed on a more comprehensive legal footing. This may be the reason that some countries, including those of the EAP region, have been slow to embrace this as an effective model of cooperation enabling access to data, however it is hoped that this study will encourage further appropriate use of direct cooperation, alongside the mutual legal assistance process.

Moreover, the new opportunities provided by the Second Additional Protocol are now available and countries are expected to make use of these; the Protocol was opened for signature on 12th May 2022 and signed by 22 countries, including the US.[4] More countries are expected to sign the Protocol in the near future and work on the ensuring implementation and ratification has started. In order for the Protocol to enter into a force, five ratifications are required.

2 Purpose of the study

This study has been prepared within the parameters of the Council of Europe CyberEast project which supports action on cybercrime for cyber resilience in the EAP region. The study outlines the range of cooperation models which support cross border access to data and aims to further motivate appropriate direct cooperation between law enforcement of the EAP region and MSPs whilst outlining obstacles and providing recommendations for successful access to data. In addition, it aims to encourage the establishment of conditions for direct cooperation within the EAP region, and between the EAP region and MSPs, based on the principles in the Second Additional Protocol to the Council of Europe Convention on Cybercrime.

The study also emphasises the growing acceptance of direct cooperation by referring to other national, bi-lateral and regional frameworks and initiatives aiming at facilitating access to data and cooperation with MSPs such as the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) and its executive agreements[5], the European Union e-evidence proposal[6] and negotiations of an EU-US e-evidence agreement[7][8] as well as work done within the European Union SIRIUS project[9][10].

---

[2] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence
https://rm.coe.int/1680a49dab

[3] https://www.justice.gov/dag/page/file/1152896/download

[4] https://www.coe.int/en/web/portal/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention

[5] https://www.justice.gov/dag/cloudact

[6] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[7] 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

[8] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[9] https://www.europol.europa.eu/operations-services-innovation/sirius-project

[10] https://www.eurojust.europa.eu/sirius

This is an update of an earlier study completed in 2017[11] which sought to promote understanding and cooperative relationships between law enforcement in the EAP region and MSPs. It also offered insight into opportunities for effective, timely direct cooperation and discussed the data disclosure policies of MSPs.

This study therefore builds on the earlier information, whilst providing an update on new legislative frameworks, and in addition seeks to stimulate acceptance of the direct cooperation model as a mainstream model for cross- border access to data from MSPs based on the principles of the Second Additional Protocol.

For the purposes of further background information on the consideration of international cooperation and direct access to data, the following sources are also recommended:

- *Criminal justice access to data in the cloud: challenges. Discussion paper prepared by the T-CY Cloud Evidence Group*[12]
- *Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group*[13]
- *Criminal justice access to data in the cloud: Cooperation with "foreign" service providers. Background paper prepared by the T-CY Cloud Evidence Group*[14]
- *The 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";*[15]
- *T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention).*[16]

Criminal justice access to data and cooperation with service providers have also been addressed during the Octopus Conferences[17]. Similarly, readers interested in developing their understanding of cooperation with internet service providers more generally are referred to Council of Europe study and guidelines on: *Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines*[18], initially based on an earlier study from 2008, it was updated in 2020. Readers who are familiar with the Council of Europe Convention on Cybercrime and international cooperation practice will benefit most from this study.

3 Background

Traditionally, cross-border access to physical evidence for the purposes of criminal proceedings has been conducted in accordance with international law principles which form the basis of mutual legal assistance treaties (MLATs). These treaties set out a state-to-state process for cooperation as between central authorities for the purpose of requesting, collecting, and

[11] https://rm.coe.int/study-on-strategy-of-cooperation-with-multinational-service-providers/16808f1e16

[12] https://rm.coe.int/1680304b59

[13] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8

[14] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806477d

[15] https://rm.coe.int/16806a495e

[16] https://rm.coe.int/16806f943e

[17] https://www.coe.int/en/web/cybercrime/octopus-conference

[18] https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7

returning evidence. The treaties may be multilateral, or bilateral, and for member states of the Council of Europe, would include the Council of Europe Convention on mutual assistance of 1959 and protocols[19] (1959 MLA Convention).

The Council of Europe Convention on Cybercrime contains well known domestic procedural provisions, as well as provisions related to international cooperation, to be exercised subject to safeguards provided by Article 15 of the Convention, regulating access to computer data[20]. The provisions are required to be implemented in the national laws of Parties to the Convention so that access to data in all Parties is based on common procedural measures and minimum standards and safeguards. The Convention and guidance also differentiate between categories of data such as subscriber information[21], traffic data[22] and content data[23]. These differences are also relevant when seeking data from MSPs relying on both the provisions of the Convention as well as on domestic law provisions for that purpose. Access to the particular categories of data and definitions are discussed further below in Section 5 and in the Annex to this study.

For the purposes of international cooperation and cross-border access to data, the Convention on Cybercrime sets out international equivalent provisions[24] enabling parties to request access to data based on the same national procedural measures. In order to support such cooperation, the Convention requires parties to rely on existing MLAT arrangements[25] relating to the obtaining of evidence of criminal offences established in accordance with Articles 2 through 11 of the Convention or electronic evidence related to any other offence. In case other treaties are not applicable, the Convention itself can be used as a legal basis and this is of particular relevance to those countries not party to the 1959 MLA Convention. Essentially, the Convention on Cybercrime and Council of Europe 1959 Convention on mutual assistance in criminal matters can serve as a joint legal basis for seeking cross border access to data for use as electronic evidence.

Unfortunately though, the MLAT process has developed a reputation over the years for being slow, bureaucratic and cumbersome, it has also been found to be particularly unsuited to the obtaining of data urgently needed at the start of an investigation and/or data which is retained for limited periods[26]. As computer data can be volatile and altered, removed, transferred from

[19] https://www.coe.int/en/web/transnational-criminal-justice-pcoc/MLA-council-of-europe-standards

[20] Article 16 – Expedited preservation of stored computer data
Article 17 – Expedited preservation and partial disclosure of traffic data
Article 18 – Production order
Article 19 – Search and seizure of stored computer data
Article 20 – Real-time collection of traffic data
Article 21 – Interception of content data

[21] Article 18(3)

[22] Article 1 d

[23] See the Explanatory Report. Section 209 - "Content data" is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data). https://rm.coe.int/16800cce5b

[24] Article 29 – Expedited preservation of stored computer data
Article 30 – Expedited disclosure of preserved traffic data
Article 31 – Mutual assistance regarding accessing of stored computer data

[25] Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

[26] T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime. Adopted by the T-CY in December 2014

one jurisdiction to another or deleted very quickly, a fast and effective cooperation process is required. Due to the inefficiency of the MLAT process and sheer volume of requests for data required from US-based MSPs, the use of so-called direct cooperation became the cooperation model of choice. As countries are sending hundreds of thousands of direct requests a year to US-based MSPs, this cooperation model has also been supported by US authorities so as to ease the burden of the authorities responsible for MLA.

It is not difficult to see why direct cooperation is seen as an attractive option by law enforcement; in comparison with the MLAT process, which requires a number of steps to be taken before a request for evidence can even be transmitted, the direct cooperation model simply relies upon initiating contact with the MSP in question and requesting the data. Despite the comparative simplicity of this model, law enforcement in the EAP region and elsewhere have found it a difficult model to deploy successfully. The model can be referred to as asymmetric cooperation because it rests on lawfully made requests, made by those having the power to do so and the disclosure of data which is at the discretion of the MSP and is entirely voluntary[27], based on an interpretation of relevant US legislation[28] regulating access to content data. Practice has shown (and as pointed out in the 2017 study) other issues may also be taken into account such as human rights considerations, procedural safeguards and privacy issues. The criteria for acceptance or refusal of requests vary as between MSPs are not explicitly articulated leading to frustration on the part of law enforcement when a request is unsuccessful.

The 2017 study identified particular issues impeding cooperation; in the view of MSPs, law enforcement requests were not regarded as a business priority and resources to deal with these were allocated accordingly. Further, poor understanding by law enforcement of MSP business models, with regional and national offices established to deal with business priorities such as product management rather than law enforcement issues was found to be a factor. Also mentioned was the fact that user data retained by MSPs was in order to assist decision making within the business and as such may not meet law enforcement expectations or requirements.

The study confirmed that law enforcement and MSPs had a lot to learn from one another through communication and building of effective relationships. Much of this has been taken forward since 2017, by training and capacity building work in the EAP region and as shown by the updated 2020 guidelines for cooperation between law enforcement and service providers[29]. Discussions on how to facilitate cooperation and overcome the various challenges have also been taking place at the Council of Europe and Cybercrime Convention Committee (T-CY) level aiming at bringing together both law enforcement and MSPs.

Summing up at this point; the current methods available to law enforcement seeking cross-border access to data held by US-based MSPs - pending the coming into force of the Second Additional Protocol - appear to be twofold; in the first case there is the MLAT process which operates in combination with Cybercrime Convention provisions, a legally binding, established

---

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

T-CY assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers. Adopted by the T-CY in November 2017

https://rm.coe.int/t-cy-2017-2-mla-follow-up-rep/168076d55f

[27] Final report of the T-CY Cloud Evidence Group, *Criminal justice access to electronic evidence in the cloud (CEG Final Report)* p. 28

[28] The US *Stored Communications Act* of 1986

[29] Council of Europe Report: *Cooperation between law enforcement and internetservice providers against cybercrime: towards common guidelines*, updated version 2020

and transparent process but too slow and unwieldy to ensure speedy access to data. In the second case, direct cooperation whilst appearing to offer a more efficient process is voluntary, not always reliable and lacks transparency, though this can depend on the particular country and MSP concerned. While some countries have reported an effective cooperation process with a particular MSP, the situation may be completely different where other countries or MSP-s are involved. It has also been the case, that cooperation has been working one way only; whilst European law enforcement was able to cooperate and obtain data from US-based MSPs, such cooperation was not possible other way around[30]. It was also not possible to deploy this form of cooperation amongst European law enforcement and European MSPs.

In the end both methods (MLAT based cooperation and direct cooperation) can result in considerable dissatisfaction for different reasons. The current possibilities for access to data directly from MSPs are discussed in further detail in Section 5 of this study.

New legal initiatives

Whilst recognising the difficulties with mutual legal assistance the Council of Europe accepted it as the primary method for accessing data held in other territories for use as evidence[31]. Through the Cybercrime Programme Office C-PROC, the Council of Europe instituted various capacity building projects in the EAP region including (inter alia) training on international cooperation for law enforcement and prosecutors, the development of guidance and template requests for preservation and obtaining of subscriber information[32].

During the same period the Cloud Evidence Group established by the Council of Europe Cybercrime Committee was also charged with considering the difficulties associated with mutual legal assistance, direct cooperation with US based MSPs and complications caused by the storage of data in the cloud in a third or unknown location. One particularly useful output was Guidance Note #10 (referred to in Section 2 above) which advises on the use of domestic procedural measures for obtaining subscriber information, from MSPs operating on the territory through local offices, subject to law enforcement in the relevant territory having jurisdiction over the investigation and providing that the criteria in Article 18 of the Cybercrime Convention are met. Although such national measures, having extraterritorial effect, have been successfully deployed in this way in Belgium[33] there has been little or no use of this guidance in the EAP region. Nevertheless, the guidance remains available for consultation.

The main consequence of the deliberations of the Cloud Evidence Group were recommendations relating to the Second Additional Protocol to improve cross-border access to data with terms of reference[34] and working methods[35] being adopted in 2017 leading to the final draft of the protocol being completed in 2021, now open for signature from 12th May 2022. Briefly, the Second Additional Protocol aims to support direct cooperation by providing a new legislative framework, legal certainty, previously lacking, for the purposes of obtaining domain name registration information, subscriber information and traffic data from service providers. It also aims to improve the efficacy of mutual legal assistance in emergencies and introduces a provision on expedited cooperation with the support of the 24/7 Network. All

[30] CEG Final Report, p. 26

[31] CEG Final Report, p. 9

[32] Templates available at coe.int/en/web/cybercrime/resources as at 17th May 2022.

[33] CEG Final Report p. 21 Belgian Spreme Court decision of 1st December 2015 in respect of a case against Yahoo to the effect that Yahoo was subject to the coercive measures in Article 46bis of the Belgian Rules on Criminal Procedure and was thus obliged to produce subscriber information

[34] https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690

[35] https://rm.coe.int/t-cy-2017-20-pdg-workplan/168076cfda

provisions are subject to data protection and privacy provisions. The Second Additional Protocol and its impact on the direct cooperation with MSPs is discussed in detail in Section 6 of this study.

In 2018 there was another legal development of relevance to cross border access to data; on 23rd March 2018 US Congress brought into force the CLOUD Act[36] which amended the Stored Communications Act of 1986, having the effect of allowing US law enforcement to compel production of data from US service providers (MSPs) when under their control regardless of location in another country. Although this legislation clarified the position of US law enforcement access to data held in other countries, it was not intended to regulate access of non-US law enforcement individuals seeking access to data from US based MSPs. That said, the Act does authorise the US Government to enter into bi-lateral agreements or so-called executive agreements with other states (providing specific criteria are met) which would allow law enforcement in both states to directly cooperate with service providers in the other state for the purpose of obtaining electronic evidence in cases of serious crime. As already mentioned, and given that the major MSPs are headquartered in the US, this legislation has the potential for a significant impact on the conduct of international cooperation in criminal matters going forward. This legislation and relevant agreements are further discussed with direct cooperation in Section 7 below.

It is also relevant to mention that there are other new initiatives concerning access to data stored by MSPs-: In the EU the European Commission tabled a proposal for the so-called e-evidence package in April 2018, however the discussions are still ongoing. In parallel, discussions and negotiations for a new convention dealing with the criminal use of information technology in the United Nations have started. These initiatives and relevance to accessing data from MSPs are discussed in Section 7 below.

4 Concerns related to cooperation

For reasons already mentioned, a proportion of cooperation activity, traditionally based on MLAT requests to secure data from MSPs, has given way to direct cooperation where this is legally permissible. This development then gave rise to a series of concerns, both on the part of MSPs and law enforcement ; essentially, in the view of MSPs there was an inadequate understanding of their (MSP) business models and processes on the part of law enforcement whilst in the view of law enforcement, the MSPs did not exhibit sufficient transparency in dealing with their requests. The concerns were set out in the 2017 study and are now revisited below together with a discussion of relevant action taken by the Council of Europe through development of guidance and training to assist an improved level of understanding and cooperation for the purposes of better access to data.

4.1 Multinational Service Providers concerns

In short, the concerns of MSPs can be summarised to include:

The perceived low level of understanding on the part of law enforcement about their (MSPs) business models, their services and extent of data kept and for which purpose ; this can result in requests being sent to wrong MSP or wrong legal entity, or for requests for non-existent data or data that has been deleted.

The importance of verification; that a request is legitimate and has in fact been sent by a law enforcement authority.

[36] The Clarifying Overseas Use of Data Act, enacted on 23rd March 2018

The need for acceptance by law enforcement of the value of mutual trusted relationships developed through direct contacts and assisted by use of dedicated online portals established by some MSPs.

The implications of making disclosures of data to law enforcement in countries where commitment to human rights and associated issues is regarded a questionable.

Difficulties in assessing the lawfulness of the request; the legal basis for the request is absent from the request or is incorrect, or the request does not provide the details of the law enforcement authority or is missing letterhead or signature.

Bad quality, incomplete, or overly broad requests received from law enforcement; insufficient information provided and lack of valid identifiers. In case of an emergency requests, lack of information to justify and explain the emergency situation.

4.2 Law Enforcement concerns:

In short, the concerns of law enforcement include:

The variation of policy as between the MSPs which has the effect of divergent responses country to country. Also, the fact that MSP policies are not publicly available, or are often amended. These issues can cause difficulties in correctly addressing requests, particularly if no contact information is given, or if there is no dedicated portal.

The fact that MSPs only accept requests in certain languages.

Delays in responses, or requested information is provided only partially, or data is not preserved at all, or is deleted by the time the request is made.

Lack of certainty of response to requests by MSPs and lack of feedback in case of refusal.

Notification by MSPs to their users of requests made and implications for confidentiality of the investigation and security of personal data relating to the law enforcement official concerned.

Divergence of response of MSPs when dealing with an EU subsidiary.

4.3 Attempts to solve these concerns

The 2017 study makes reference to various efforts by the Council of Europe to solve these concerns which remain relevant today. These include the deliberations of the Cloud Evidence Group (CEG) which worked to bring clarity to challenging aspects of international cooperation. The recommendations in the CEG final report of 2016 themselves referring to implementation of the earlier T-CY Assessment Report of 2014 and the recommendations on international cooperation, including necessity for a capacity building programmes to support such implementation.

In 2017 the T-CY adopted the CEG's suggestion for guidance on the use of national production orders to compel MSPs to submit subscriber information (instead of resorting to the MLA process) leading to the issue of Guidance Note #10 in March 2017. As stated above countries

in the EAP region do not appear to have made use of this possibility, nevertheless the advice is extant and remains valid[37].

Since 2017, the EAP region has benefited from comprehensive Council of Europe capacity building and training, provided through the Cybercrime Programme Office C-PROC, to address international cooperation in cybercrime and for the obtaining of electronic evidence. Such capacity building and training was delivered to all EAP countries through the CyberEast and predecessor projects (Cybercrime@EAPII and Cybercrime@EAPIII). Additional training on international cooperation, including direct cooperation with MSPs, was delivered to law enforcement and prosecutors in EAP countries, Ukraine and Moldova in the context of training on online child sexual exploitation and abuse OCSEA) during 2020 – 2021.

The training offered by the Council of Europe did tackle some of the concerns identified above, for instance training on direct cooperation with MSPs, use of online portals and preparation of requests were components of the international cooperation training delivered in all the countries of the EAP region in 2017 and in updated training in 2021. Further and in response to the earlier T-CY recommendations of 2014 (and also relevant to MSP concerns about the quality of requests), request templates were developed, within the parameters of CyberEast predecessor projects, for the preservation of all categories of data and the obtaining of subscriber information, suitable for use when seeking to cooperate with MSPs[38]. Additional specialised training on the practical use of the templates in a case scenario setting was delivered in all countries of the EAP region and Western Balkans during 2018 and 2019 and updated again for the EAP region in training given during 2021.

The potential notification of users by MSPs, relating to law enforcement requests received[39], remains an ongoing concern and the template requests do identify this as an issue citing a requirement for immediate notification in advance of any possible breach of confidentiality. In addition, it should be noted that US legislation will not disclose the request in certain circumstances, these exceptions are discussed in Section 5 below.

Despite the training delivered, there is little evidence that the templates are in regular use in the EAP region. In some cases this may be due to insufficiency of national procedural measures, lack of legal definitions of data categories or simple reliance on existing national request templates and preference of more traditional methods of cooperation. But recent transparency reports of MSPs (further discussed in Section 5) do show small increases in requests received from some countries of the EAP region in comparison to five or six years ago.

Potential rejection of requests by MSPs on the grounds of perceived human rights concerns relating to issues such as data privacy, fair trial or data retention remains a difficult issue to respond to particularly in the face of lacking transparency. Resort to MLAT based requests in this situation is unlikely to generate a different response, even where grounds for refusal of a request are limited, due to overriding human rights obligations.

The concerns on the part of MSPs, relating to lack of understanding of business models by law enforecement, and issues associated with the retention and processing of particular data in support of business priorities, should abate based on longevity of experience and relationships. It should also be clearly articulated at this stage that direct cooperation possibilities exist with US-based service providers only. This is not the position in the EU – even when cooperating with subsidiaries of US providers in Ireland (Meta, Microsoft and Google). In the EU a clear

[37] Available at coe.int/en/web/cybercrime/guidance-notes as at 17th May 2022.

[38] Available at coe.int/en/web/cybercrime/resources as at 17th May 2022

[39] CEG Final Report, p. 28

legal basis is required to transfer or disclose data, and this cannot be done voluntarily as in the USA. It is anticipated that the Second Additional Protocol will be able to assist here. The Second Additional Protocol is discussed in detail in Section 6 below.

It is hoped that some of the other law enforcement concerns in the EAP region around variation of disclosure policies as between MSPs and differentiation of response per country as well as the lack of certainty of response and lack of transparency will be met by the Second Additional Protocol once in force, if ratified by the countries of EAP region and the United States. The Protocol will require parties to implement legislation at national level to compel their service providers to fulfil requests directly made, for domain name registration information and subscriber information or on order of national judicial authorities. These provisions are subject to data protection safeguards and are fully discussed in Section 6 below.

Cooperation between law enforcement authorities and MSP-s has also been much discussed at the European Union level. In 2018 a SIRIUS Project[40] was established to analyse law enforcement access to electronic evidence from foreign based online service providers for criminal investigation purposes. Since then, several SIRIUS EU Digital Evidence Situation Reports have been published (2019[41], 2020[42] and 2021[43]). In addition, guidelines and templates have been prepared for law enforcement authorities to facilitate cooperation and overcome problems and challenges that have been identified. Practical problems and concerns have also been addressed in order to understand why requests are frequently delayed or refused. In addition to publicly available resources (reports, templates) more detailed guidance is available on a restricted website. As of May 2022, this restricted platform has also been made available to non-EU countries having cooperation agreement with Eurojust and/or Europol[44]. Developments at EU level are further discussed in Section 7 below. Meanwhile, the next Section following below discusses and assesses the currently available methods for cooperation

5 Current possibilities for cooperation

As already explained above, there are essentially two options open to law enforcement for the purposes of obtaining data from MSPs for use in criminal proceedings. This section considers these possibilities in more detail. it explains what is required by each of the processes and considers what is to be realistically expected by law enforcement.

5.1 Requests based on international legal standards

A written request based on international legal principles formalised in a mutual legal assistance treaty (MLAT request) is, as already explained, the traditional method for the seeking of physical and documentary evidence or witness testimony from another country. Requests are transmitted between central authorities established for that purpose. Often, requests are prepared and executed by law enforcement authorities (prosecutors and/or police) in the

[40] https://www.eurojust.europa.eu/sirius

[41] https://www.europol.europa.eu/sites/default/files/documents/sirius_eu_digital_evidence_report.pdf

[42] https://www.eurojust.europa.eu/publication/sirius-eu-digital-evidence-situation-report-2020

[43] https://www.eurojust.europa.eu/publication/eurojust-europol-digital-evidence-situation-sirius-report-2021

[44] Cooperation agreement with Eurojust: Albania, Montenegro, North Macedonia, Serbia, Georgia, Iceland, Liechtenstein, Moldova, Norway, Switzerland, Ukraine and the USA.
Cooperation agreement with Europol: Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, North Macedonia, Norway, Serbia, Switzerland, Ukraine and the USA.

requesting and requested states rather than the central authorities themselves and are subject to legal evaluation in the receiving country to confirm legal basis, legitimacy and prior to execution are subject judicial scrutiny. This can be a fragmented process dependent on a number of individuals and authorities playing their part.

Because this is a formal process, the content of the request is of great significance, it must adhere to treaty provisions and must satisfy legal requirements of the requesting state so that it can be admitted in evidence there, as well as the legal requirements of the requested state charged with execution. Treaties usually limit reasons for refusal of requests and human rights obligations are also be taken into account although within the Council of Europe all states are signatory to the European Convention on Human Rights (ECHR) and as such are obliged to uphold these rights.

As far as the countries of the EAP region are concerned, in relying on the MLAT process to obtain data for use as evidence from US-based MSPs, the relevant legal basis would be the Convention on Cybercrime plus an additional MLAT arrangement outlining the applicable process. In practice this will probably be the framework outlined in Articles 27 and 28 of the Cybercrime Convention unless there is an existing bi-lateral arrangement or other applicable multilateral convention for example, the UN conventions such as UNTOC, provided the offence under investigation meets the requirements of those conventions and assistance sought is legally permissible in the requested state.

The advantage of this method is that it is supported by a legally binding framework which outlines a clear process featuring judicial scrutiny. The disadvantage is that it requires a number of steps to be taken both in requesting and requested states and is often further hampered by poorly drafted and/or translated requests and/or mutual lack of understanding of legal requirements as between the requesting and requested states.

Although the Council of Europe Cybercrime Convention Committee T-CY, recognised in its Assessment of 2014 that MLA is the primary method of obtaining evidence from other countries, it also found that the MLAT system was overburdened due to the ubiquity of electronic evidence and thousands of requests directed to the US authorities year upon year. The T-CY found specifically that the MLAT system was singularly unsuitable for accommodating the majority of requests which were for subscriber information – important at the beginning of investigations - to identify potential suspects. As explained above, the T-CY assessment then also contributed to the work of the Cloud Evidence Group and resulted in number of recommendations, adoption of Guidance Note #10 already discussed, and the beginning of efforts to remove requests for subscriber information from the formal MLAT process. The obtaining of subscriber information has now been developed further in the Second Additional Protocol to the Cybercrime Convention addressed in Section 6 below.

Since 2014, a lot of work has been done in the Council of Europe to support the efficiency of the MLA process including work in the Committee of Experts on the Operation of European Conventions in Criminal Matters (PC-OC), in consultation with T-CY, as a result of which a model MLA request template was adopted in 2015[45] featuring a section on the obtaining of electronic data. In addition, T-CY later adopted its own template requests specifically for preservation of data and the obtaining of subscriber information. Council of Europe Cybercrime Programme Office C-PROC has also offered regular training and materials to law enforcement and prosecutors on international cooperation and mutual legal assistance within the project CyberEast, its' predecessors and other projects such as GLACY and GLACY+, i-PROCEEDS and i-PROCEEDS II and OCSEA. In terms of other resources, the Country Wiki pages on the Council

[45] Available at www.coe.int/tc as at 6th May 2022

of Europe Octopus Community website[46] have been developed to enable parties to the Convention to provide information on national legislation and arrangements for MLAT requests so as to provide a measure of transparency in the MLA process previously found to have been lacking.

Although these efforts are useful and certainly do have the potential to improve aspects of the MLA process, in the five years since the 2017 study, the amount of directly made requests to MSPs continued to increase. This has also been reflected in some of the countries of the EAP region which tended to rely on traditional methods until a few years ago but are now making small numbers of requests with varying degrees of success.

In the scenario described above, where numbers of directly made requests are increasing, there nevertheless remains a role for MLAT requests in the obtaining of content data (see Annex for a discussion of the definition of content data). It remains the case that even where MSPs may be prepared to make non-content data available or, where certain data may be made available in emergency situations, the general rule for the obtaining of content data is that it should be obtained using the MLAT process (this is in accordance with applicable US law and stated in policy and guidance issued by MSPs, discussed below). Although MSPs may disclose subscriber information voluntarily in certain circumstances, they do not commit themselves to doing so therefore, MLAT requests may also be required for access to subscriber information.

Requests for content data held by MSPs headquartered in the US should be addressed to the US Department of Justice and contain a level of detail which enables a warrant to be obtained in the US courts authorising the release of the said data. The required standard is the standard of "probable cause" – essentially the court must be satisfied that there is a reasonable basis for believing that a crime may have been committed and that evidence of a crime is present in the place to be searched if relevant. Therefore, in addition to the usual information that any MLAT request should contain, a request for content data should contain sufficient information to satisfy this standard. The request should also specify in as much detail as possible the data requested and ideally demonstrate a nexus between the data required and the offence in question. For these purposes the PC-OC's model template request and Country Wiki pages referred to above, are good starting points. Requests for data controlled by MSP subsidiary offices in Ireland should contain the same amount of detail. If the request does not contain the necessary information this will cause delay and if additional information cannot be provided by the requesting country, then it is not realistic to expect a successful outcome. Those making MLAT requests to the US for content data should expect a rigorous process of some length; anecdotal evidence suggests around 9 -12 months in most cases.

As the focus of this study is the obtaining of data from MSPs by relying on direct cooperation for the voluntary disclosure of data, it is not proposed to dwell on MLAT processes in any further detail here. More recent improvements to the MLAT process in emergency situations is set out in the Second Additional Protocol are discussed in Section 6 below.

5.2 Direct cooperation and voluntary disclosure Model

The reasons for growing use of this model have already been explained. The paragraphs below now discuss in further detail how the process actually works and what is required.

Recalling first of all that this is an asymmetric process, involving legally made requests by law enforcement officials who have the power to do so with the requests being considered by MSPs

[46] Accessible at www.coe.int/en/web/octopus/country-wiki

on a voluntary basis and in accordance with the extent of disclosure allowed pursuant to US law. As already stated above, this model is supported by the US authorities. Once received by MSPs, requests are subject to a rigorous review – much in the same way as MLAT requests – before a disclosure decision is made. Unlike the MLAT process though, this process lacks an international legal framework and is not a legally binding process. However, the Second Additional Protocol has sought to fill this gap and the relevant provisions are discussed in Section 6 below.

In general, law enforcement relying on direct cooperation to obtain voluntary disclosure of data must expect a variance in level of engagement from MSPs based on different capabilities and levels of commitment in responding to law enforcement requests. For this reason, it is difficult to suggest a singular approach which guarantees success. Some providers cooperate well with law enforcement leading to high response rates to requests, others will not respond to requests, or will scrutinise more intensively depending on the perceived political regime in a particular country. In order to achieve a better level of understanding, trust and cooperation many countries now engage with MSPs though the development of a relationship based on a specific contact point.

Most MSP's have created online resources to assist law enforcement in the making of requests for disclosure of information but do not necessarily ask for the same information. Whilst this is difficult for law enforcement, it is incumbent on those making the requests to ensure that they meet the requirements set out by the MSP. Failure to do so will result in no response from the MSP.

Whether law enforcement uses an online portal and/or online form to contact an MSP, or whether requests are made based on the T-CY approved templates, particular attention should be paid to use of terminology referring to categories of data sought and the specificity of data types within those categories, for instance subscriber information can include a number of different pieces of information (see Annex for relevant definitions).

A discussion of selected MSP resources and policies follow below, including those of Apple, Google, Meta, Microsoft, Twitter and Yahoo!. The resources are regularly updated and as of the time of writing[47] could be accessed online at the following online locations:

Apple www.apple.com/legal/transparency-guidelines-uspdf

Google www.transparencyreport.google.com

Meta www.transparency.fb.com/data/government-data-requests

Microsoft www.microsoft.com/en-uscorporate-responsiblity/law-enforcement-requests-pdf

Twitter www.help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support

Yahoo! www.transparency.yahoo.com/government-data-requests

The general guidance issued by the above MSPs emphasises that requests are considered based on applicable legal principles. The guidance differentiates between US and non-US requests to take into account the MLAT element for non-US requests. Although not specifically articulated by all, Microsoft being an exception here, it should be assumed that the legal

[47] Accessed 6th May 2022

consideration extends to both local US law and the laws (substantive and procedural) of the requesting country, including human rights due diligence.

Explanations of data categories retained, periods of retention and types of data within these categories, are given. Advice is also provided on the information to be included in a request; Apple provides very comprehensive advice available in a downloadable pdf document available at the online location identified above.

Law enforcement is directed to a variety of online portals for the purposes of making a request and where requests concern EU data, accounts or users, enquiries are directed to subsidiaries in Ireland in some cases for submission to a postal address. There might be potential for use of the Council of Europe template requests for preservation and subscriber information here. It is advisable that law enforcement refer to the guidance of a particular MSP in advance of a request being made.

Some of the MSPs (Apple, Google, Meta, Microsoft and Yahoo!) issue transparency reports outlining country by country statistics for requests and disclosures made on an annual or twice-yearly basis. An perusal of the most recent of such reports - available at the online locations indicated above - show that Meta (specifically facebook data) has been the most requested MSP by countries of the EAP region with all five making requests to Meta in the period January – June 2021, showing Armenia making 15 requests, Azerbaijan with 9, Georgia 14, Moldova at 14 and Ukraine at 65 – with varying degrees of success. To put this information in context, Meta (facebook) received over 200,000 requests in total during this period and made disclosures in around 70% of cases. Most of the EAP countries achieved a success rate close to this figure. Yahoo! appeared to be the least requested by EAP countries whilst Apple, Google and Microsoft all received smaller numbers of requests.

Guidance shows that al above mentioned MSPs accept directly submitted, legally valid requests for preservation of data upon receipt of which they may preserve data in connection with a specific criminal process and in anticipation of a formal request being made to obtain the data content. Preservation is for an initial 90-day renewable period. In these cases Twitter will, according to guidance available at the location given above, preserve "a temporary snapshot of the relevant account" and Apple will conduct a "one time data pull" of the relevant account. It is always advisable to check the guidance of the relevant MSP relating to the information required to be included in the request including information to enable MSPs to:

(a) establish the legitimacy the request – where letters are to be submitted (Microsoft, Twitter, Yahoo!) these must be on an official letterhead of the requesting party submitted to the MSP through a particular site or email address, where requests are to be submitted through an online request system, this must be done from an official law enforcement domain.

(b) establish the exact data category required (subscriber, traffic, content) and data type required to be preserved (IP address, particular tweet or email) indicating clearly the time, date and period of interest.

Anecdotal evidence from law enforcement in a range of countries, including the countries of the EAP region, suggests that – subject to legal review and sufficiency of information - data can be successfully preserved in response to a directly submitted request.

Readers of this study will also be aware that Article 30 of the Cybercrime Convention requires service providers to disclose a certain amount of traffic data on preservation in certain circumstances. The extent of such disclosures to law enforcement in EAP countries has been difficult to verify both in terms of anecdotal evidence and transparency reports.

Moving on to consider data disclosures in case of emergencies, all above mentioned MSPs indicate in their guidance that they will consider – case by case or on a discretionary basis – legitimate, legally based requests for disclosure in an emergency. Each MSP provides details of how a request should be submitted and the information it should contain from simply requiring a summary of the emergency (Microsoft) to more prescriptive information (Twitter). Apple helpfully provides a contact telephone number for initial discussions serviced in multiple languages, although the actual request must be made in writing.

All guidance further makes it clear that only information necessary to address the emergency will be disclosed. Meta provides useful examples on its' website (accessible at the online location given above) where for example WhatsApp traffic data appears to have been disclosed to locate kidnappers. Microsoft provides reports on emergency disclosures; in the period July – December 2021 when Ukraine was the only EAP country to have requested emergency disclosure of data, making 12 requests, with a high success rate. To put this information in context against other European countries. Poland made 9 requests in the same period and Austria made 2 such requests.

The difficulty that law enforcement has had with the making of emergency requests, and this was alluded to in the 2017 study, is that the definition of an emergency is slightly different form MSP to MSP. Whilst most refer to disclosures in case of imminent danger or exigent emergency to prevent death or serious physical injury, others refer to suicide, harm to a child or in the case of Apple, threats to state security are included as well as threats to critical infrastructure (details available at the online location given above). It may be that these definitions are reflective of the experience of the particular MSP, but it should be said that to date there has been an element of legal certainty lacking, as to what legally constitutes an emergency, sufficient to generate disclosure of data. This question was taken forward in the negotiations relating to the Second Additional Protocol to the Cybercrime Convention and is discussed in Section 6 below.

As far as access to content data is concerned, as made clear above, a formal MLAT request is required. Also, of relevance to mention here, is the obligation incumbent upon US based service providers – including the above mentioned MSPs - to report content data containing imagery of child sexual abuse and exploitation to the National Center for Missing and Exploited Children (NCMEC) and once so reported to preserve the data for a 90-day period. Following analysis conducted at NCMEC, this data is usually forwarded on to law enforcement in other countries for further investigation. NCMEC[48] publishes regular reports of disclosures made country by country (showing disclosures are made to all EAP countries). Training conducted with law enforcement of Moldova during 2021 in the context of Council of Europe training on online child sexual exploitation and abuse (OCSEA) showed that Moldovan authorities cooperate effectively with NCMEC.

Turning now to requests for disclosure of non-content data such as subscriber information and traffic data in response to non-US law enforcement requests; here the guidance is extremely broad giving the MSPs maximum discretion and emphasising commitment to privacy of users. To an extent, guidance to US and non-US law enforcement appears to be conflated, with references to both legally valid demands, or requests, or legal process, and a preparedness to assist with MLAT requests. The reference to legally valid requests would appear to include a reference to the US Electronic Communications Privacy Act which states that disclosure of subscriber information is authorised upon subpoena. Requests are to be directed to either the US or Ireland depending on the data controller for the relevant account.

[48] www.missingkids .org

If considering an approach to MSPs for subscriber information, reference should be made to the relevant MSP's guidance to determine where the request should be submitted, how it should be transmitted, and the information required. Based on the guidance available, preparation of a detailed request is recommended and the use of the Council of Europe's template request for subscriber information should help to ensure that all relevant information is included. Anecdotal evidence does suggest that there have been instances of voluntary disclosure of subscriber information following directly made requests. However, to date, as responses during Council of Europe training of law enforcement in EAP and other regions, on international cooperation training have shown, there has been a level of uncertainty as to the best approach to take when seeking subscriber information. As already explained efforts such as Guidance Note #10 and the template request have attempted to assist. Again, this question was taken forward in provisions in the Second Additional Protocol, discussed in Section 6 below, which should bring more clarity to current practice.

Based on the above discussion, direct cooperation with MSPs for the purposes of voluntary disclosure of data is a worthwhile approach for law enforcement to take and this has proved to be the case as far as preservation of data is concerned and the disclosure of data in emergencies. The disclosure of content data subject to an MLAT process is clear, however the position on disclosure on non-content data, such as subscriber information, is more of a grey area and it is here that the clarifying impact of the Second Additional Protocol will perhaps be most welcomed.

5.3 Customer notification

All the above MSPs WILL notify their users of any request for their data UNLESS:

- prohibited by the law (pursuant to 18 U.S.C. § 2705(b) Electronic Communications Privacy Act (ECPA)).
- In emergency cases;
- Where notice could result in danger;
- Where notice could be counterproductive.

Other than this legal prohibition, the decision to notify is made by the companies.

This is an important consideration for criminal justice authorities and one of which they must be aware in advance of making any request to MSP's. There are situations where potentially, the personal details of the requesting party could be released to the person who is the subject of the request. In cases involving terrorism or organised crime groups, this could place the individual at risk.

5.4 Quality of relationship with MSPs

A perpetual complaint by law enforcement has concerned the low level of response received from MSPs to requests sent. From MSPs perspective requests not receiving a response were either of poor quality or did not meet the required legal standard and were not worthy of a response. In this situation a focus on the part of law enforcement on development of relationships with MSPs may encourage providers to participate in training to improve cooperation. Although a great deal of information is available in the relevant guidance, training may have more impact on quality of requests.

As the Study on cooperation between law enforcement and internet service providers has shown[49] law enforcement in some EAP countries have successfully developed working

[49] Council of Europe Report, *Cooperation between law enforcement and internet service providers against cybercrime: towards common guidelines*, updated version 2020

relationships with domestic service providers. This shows that similar relationships are required and should be developed with MSPs as part of the solution to improved international cooperation.

5.5 Reasons for disqualification of requests

The guidance discussed above identifies some major reasons which will result in disqualification of a law enforcement request. These are listed below and should be taken into account when a request to an MSP is being considered:

- Where information requested by law enforcement is or is perceived to be in violation of human rights principles; requests from countries with poor protection of privacy and human rights are not likely to generate a response.

- Poorly drafted requests; the reason for this is that law enforcement from some countries have limited experience in applying the voluntary disclosure model and send very few requests for data on an annual basis. This lack of experience may be reflected in the quality of the request and miss some of the information required by the MSP. These requests are unlikely to generate a response. In order for a request to be successful, MSPs need to understand the context in which a crime is taking place. Thus, it is necessary for law enforcement to provide as much information as possible about a case to help the MSP understand why the information is requested. It is not sufficient to provide only the relevant article of the criminal code, criminal procedure code or other act, it is necessary to describe the case stating the full facts.

- Vague and overly broad requests which do not ask for specific data will be rejected.

- Requests sent in national language; all requests should be sent translated in English language.

6 The impact of the Second Additional Protocol on international cooperation

As indicated above the Council of Europe and the Cybercrime Convention Committee (T-CY) have been discussing the problems and challenges related to law enforcement access to data in criminal investigations for several years. This section now outlines those discussions, the progression towards the Second Additional Protocol (to the Council of Europe Cybercrime Convention) and explains the impact it will have on the current international cooperation process.

Although the negotiations for the Second Additional Protocol started in September 2017, the preparatory work began years earlier. The outcomes of previous T-CY working groups such as the Transborder Group and in particular the CEG provided inputs to the future protocol. Although it was found that State Parties were able to analyse their own domestic situation, streamline capacity and provide training alongside T-CY to develop templates and facilitate discussions with the MSPs, it was also noted that an additional legislative framework needed.

The results of the T-CY assessment on mutual legal assistance and international cooperation, as well as discussions during the preparation and adoption of Guidance Note on the implementation of Article 18 of the Convention, also highlighted the need for additional international cooperation tools. Therefore, as a result of this work, recommendations for the future protocol were proposed together with its possible elements.

The Council of Europe, through the work of the CEG, already referenced above, has sought to bring some clarity to the challenges of recognising and collecting evidence in the cloud, often located outside the jurisdiction where lawful access to data has been granted. The final report of the CEG sets out some recommendations, including one for the Council of Europe to develop a guidance note on the issue of production orders; Guidance Note#10 was issued in June 2017[50] and is referenced elsewhere in this study.

In in 2016, the CEG submitted the following recommendations to the T-CY, adopted by the Committee in its 16th Plenary, the recommendations were:

1. To invite Parties and Observer States to ensure follow up to the T-CY Recommendations on MLA adopted in December 2014 and falling primarily under the responsibility of domestic authorities, that is, Recommendations 1 to 15; the T-CY to assess progress made, and capacity building programmes, if necessary, to support implementation.

2. To consider the draft Guidance Note on Production Orders for Subscriber Information as appended to this report in view of adoption and in view of offering guidance to Parties in the implementation of Article 18.

3. To invite Parties and Observer States to review domestic procedures for access to subscriber information and thus to ensure full implementation of Article 18, Council of Europe Cybercrime Convention.

4. To take practical measures – pending longer-term solutions – to facilitate more coherent cooperation between service providers and criminal justice authorities, in particular with respect to the disclosure of subscriber information upon a lawful request in a specific criminal investigation but also with respect to emergency situations.

5. CEG recommendations: to consider the preparation of a draft Protocol to the Council of Europe Cybercrime Convention with the following elements:

- Provisions for more effective mutual legal assistance
  - a simplified regime for mutual legal assistance requests for subscriber information;
  - international production orders;
  - direct cooperation between judicial authorities in mutual legal assistance requests;
  - joint investigations and joint investigation teams;
  - requests in English language;
  - audio/video hearing of witnesses, victims and experts;
  - emergency MLA procedures.
- Provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests.
- Clearer framework and stronger safeguards for existing practices of transborder access to data.
- Safeguards, including data protection requirements.

During the 17th Plenary of the T-CY in June 2017, the Committee adopted the Terms of Reference for the preparation of a draft Second Additional Protocol to the Cybercrime Convention and tasked the CEG to work in this direction.

In September 2017 the negotiations formally started[51]. The work took place in the format of a protocol drafting group (PDG) and a protocol drafting plenary (PDP). The PDG formed sub-

[50] http://rm.coe.int/doc/09000016806f943e

[51] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

groups on different topics and conducted its work between the T-CY plenary sessions submitting inputs to the PDP for approval. Several public consultation rounds with the industry and civil society were organised to present the work and findings of the T-CY for feedback.

On 28th May 2021 T-CY adopted the text of the Protocol and transmitted it to the Committee of Ministers for its approval. The Committee of Minister adopted the Protocol on 17th November 2021.

On 12th May 2022 the Protocol was opened for signature and was signed by 22 State Parties at the same day. Additional signatures by State Parties are expected in the near future. Several State Parties have also started discussions on related implementation at national level and future ratification of the Protocol. In order to enter into force ratification by five State Parties are required.

The Protocol was built on the existing provisions of the Convention, it complements the Convention and provides additional tools related to international cooperation.

In addition to measures related to direct cooperation with MSPs concerning subscriber information, there are also provisions on access to domain registration information through direct cooperation as well as international cooperation measures related to emergency situations. Provisions on video conferencing and joint investigation teams and joint investigations would also contribute to the effectiveness of international cooperation. Article on language also specifies the language to be used for requests either to other State Parties or to Service Providers.

As regards cooperation with MSPs then, the following provisions would be the most relevant here.

Article 7 – Disclosure of subscriber information

Article 7 of the Protocol provides for the disclosure of subscriber information. Pursuant to this, Parties need to take legislative and other measures which would allow their competent authorities to issue an order for subscriber information to the service provider located in the territory of another Party. The same Article also requires that Parties enable service providers in their territory to receive and respond to requests from competent authorities of other Parties and disclose subscriber information.

A Party may also declare that such requests or orders must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision. A Party may also require that in case of such orders simultaneous notification to the competent authorities take place. Upon notification the competent authorities may also instruct the service provider not to disclose information if grounds for refusal exist. If necessary, competent authorities may request additional information to assess the order.

In order to speed up the process, a Party may use electronic channels and send orders in electronic form while respecting appropriate levels of security and authentication. Still, the latter would depend on the service providers and way the operate and communicate.

If a service provider refuses disclosure of information or does not respond within 30 days or within requested timeframe, the competent authority of issuing Party may seek enforcement pursuant to Article 8 of the Protocol or use other forms mutual assistance.

A Party may also declare that before seeking information pursuant to Article 8 of the Protocol, an issuing Party must first seek disclosure of subscriber information directly from a service provider, unless issuing Party provides reasonable explanation for not having done so.

Last but not least a Party may also make a reservation that it would not apply this Article in full or only in relation to disclosure of certain types of access numbers.

Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data

Whilst the previous Article 7 already referred to Article 8 and related endorsement or giving effect procedure, it is also important to explain it in a more detailed manner.

Pursuant to Article 8 Parties must take legislative and other measures to empower its competent authorities to issue an order to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored subscriber information and traffic data. Therefore, in case a Party receives such an order from another Party, it gives effect to the order effectively compelling the service provider to execute the order and disclose the requested data.

As in the case of Article 7, a Party may also send requests in electronic form while respecting appropriate levels of security.

Whilst assessing the request, the receiving Party may refuse execution and rely on grounds for refusals in case they exist.

Parties may also require that requests be sent through central authorities and may also reserve the right not to apply this measure with regard to traffic data.

To sum up, these two new Articles (Article 7 and 8) create a completely new legislative framework, complementing the current voluntary cooperation scheme and mutual legal assistance. In place of existing voluntary cooperation, with its uncertainties and unforeseeabilities and complete lack of enforcement measures, these Articles represent a new legally binding framework which provides for detailed procedures with clear roles and obligations of both requesting and requested Parties, and deadlines and safeguards.

If properly and fully implemented, then such new tools would give a definitive boost to international cooperation and facilitate access to electronic evidence. In particular, the new regulation would be beneficial for those Parties who did not have a satisfactory level of cooperation with MSPs and whose requests for computer data were often denied. The use of the tools provided by the Protocol will improve quality of cooperation making investigations more effective.

As it can also be seen from the text of the Protocol, the new framework allows different shades or angles, allowing Parties to make declarations and reservations. Still, despite that, the new Protocol would nevertheless provide considerable added value and complement the already existing international cooperation frameworks. The Protocol also gives a clear message to, and raises awareness amongst the Parties, that this kind of direct cooperation is recommended and that it can make a positive difference in criminal investigations.

Article 9 – Expedited disclosure of stored computer data in an emergency

Although Article 9 and the measure provided therein does not constitute direct cooperation between law enforcement and MSP, it is still a new and useful measure to obtain stored computer data from MSPs through the use of 24/7 network by expedited means in case of an emergency.

There have been numerous discussions on how to facilitate and speed up cooperation and obtain stored computer data, including content data, in cases of urgent need or in an emergency. So far, some MSPs together with national competent authorities have taken measures and can provide computer data in a more expedited manner. However, the overall situation is still unclear and practices of individual MSPs vary because there is no common understanding as to what constitutes an emergency, or emergency situation.

In order to solve this issue, it was also proposed to address this in the Second Additional Protocol. Pursuant to the Article 3 (2) c an "emergency" means a situation in which there is a significant and imminent risk to the life or safety of any natural person. Therefore, in the future, Parties to the Convention and Protocol can rely on this definition as well as use the measure provided by the Protocol as this would also be applied by MSPs on the territory of Parties.

According to Article 9, Parties need to take legislative and other measures in order to authorize their 24/7 point of contact to transmit in case of an emergency a request to 24/7 point of contact of another Party to seek immediate assistance from a Service Provider located in the territory of that Party and request disclosure of specified stored computer data without a MLA request.

Computer data that can be addressed by this measure include subscriber information, traffic data as well as content data. However, Parties may declare that they will not execute such requests for subscriber data.

Requests can be sent in electronic form. A Party may also accept a request transmitted orally and confirmation in electronic form. Parties may also require appropriate levels of security and authentication. Parties may also declare that after the execution of request, they would require submission of request in a format and through a channel specified by the requested Party.

Therefore Article 9 would complement Articles 7 and 8 and provide for additional opportunities to request computer data, including content data from MSPs, using expedited means. However, this would apply only to emergency situations as provided by the Protocol, and instead of direct cooperation with MSPs 24/7 points of contact need to be used. The advantage of Article 9 is that it does not require the preparation of an MLA request, though where there is an emergency and an MLA request is required to access the data, Parties may rely on Article 10 which provides for rapidly expedited MLA. The measure in Article 10 is distinct from an expedited MLA request already provided for in the Cybercrime Convention[52] which allows urgent requests to be made using expedited means.

[52] Council of Europe Convention on Cybercrime, Article 25 (3)

7 The impact of other legislative initiatives on international cooperation

This section discusses other national, regional and international frameworks currently in progress and the extent of their support to direct cooperation for access to data.

The US CLOUD Act

The United States Clarifying Lawful Overseas Use of Data (CLOUD) Act[53][54] was passed by US Congress, in March 2018, to facilitate access to electronic information/computer data stored by US-based providers.

As numbers of requests for computer data to US authorities have been increasing for years, and in order to ease the burden on US authorities, and to encourage and facilitate direct cooperation with US-based MSPs, the CLOUD Act provides for a possibility for the US to conclude executive agreements with countries that meet necessary criteria. These agreements can then be used to enable US-based MSPs to comply with lawful orders for disclosure of data from other countries on a reciprocal basis bypassing MLAT processes.

As at May 2022, there are potentially four executive agreements in progress pursuant to the CLOUD Act; firstly, negotiations with the UK were completed in 2019 but the agreement is not yet in force as the UK authorities still need to complete some additional formalities. Negotiations between the EU and US started some time ago but have not yet been completed (these negotiations are discussed in the paragraphs below). A third set of negotiations with Australia have recently been completed and it is anticipated that the agreement will enter into force later in 2022. A fourth set of negotiations are likely to be pursued with Canada. Although expected to have a significant impact on MLA traffic and requests for data between these countries and the US, as none of the agreements are yet in force, it is not possible to comment further on practice and efficacy of these arrangements for securing access to data. Nonetheless, they represent an important step in the mainstreaming of direct cooperation.

European Union

Discussions on international cooperation, cooperation with MSPs and more effective access to computer data stored abroad, have also been taking place at European Union level.

On 9th June 2016, the Council of the European Union adopted two sets of conclusions to set out practical and legislative options[55] to improve cross-border access to e-evidence.

Among the problems of lawfully accessing data in other jurisdictions are:

- In cross-border cases, law enforcement and judicial authorities tend to cooperate using mutual legal assistance procedures or the European Investigation Order. However, these means of judicial cooperation are often deemed too slow and cumbersome for accessing e-evidence which can be transferred or deleted at the click of a mouse.
- In parallel, voluntary cooperation between law enforcement and US based MSPs has developed as an alternative path to access e-evidence. This form of cooperation is generally faster than judicial cooperation, but as discussed above, service providers have

[53] https://www.justice.gov/dag/page/file/1152896/download

[54] https://www.justice.gov/dag/page/file/1153436/download

[55] https://www.consilium.europa.eu/en/press/press-releases/2016/06/09/criminal-activities-cyberspace/

different approaches regarding the handling of requests for disclosing electronic evidence, and the process lacks transparency and accountability.

- Finally, a number of Member States and third countries are working on national solutions that could lead to conflicting obligations for service providers. The current system is patchy and generates legal uncertainty for all parties concerned; for service providers, law enforcement and judicial authorities and also for EU citizens who are concerned about access their data and whether their fundamental rights are sufficiently protected.

The following practical measures to improve cooperation with service providers were identified:

Voluntary cooperation between national authorities and service has become the main channel to obtain non-content data, such as information on the subscriber's account. While US-based MSPs can provide non-content data to foreign law enforcement, this is currently done in the EU only for service providers based in Ireland.

Measures to improve the situation:

- Establishing single points of contact within Member States to ensure the quality of outgoing requests and build relationships of confidence with providers;
- Streamlining service providers' policies to release the requested data;
- Developing training programmes and exchange of best practice for EU law enforcement and judicial authorities for cooperation with US-based providers;
- Establishing an online information and support portal at EU level to provide support to online investigations.

In addition to the practical measures detailed above the report also examines the potential to introduce legislative measures to improve cross-border access to electronic evidence. Among the measures identified are:

- The issuing of production requests/orders to service providers in another Member State; one of the possible solutions is an EU legal framework enabling authorities to request ("production request") and authorising service providers to respond, or enabling authorities to compel ("production order") a service provider to disclose information about a user, regardless of the location of its headquarters.

- Direct access to e-evidence; sometimes finding a service provider to address with a request or order is difficult or impossible and there may be a risk of losing valuable leads. In such cases, some Member States already make it possible to access the data directly from a device of a suspect or through a computer system. Those investigation techniques have to be considered with caution in view of their potential invasiveness and the risk for fundamental rights and privacy. The conditions and minimum safeguards for direct access in potential cross-border situations could also be set up at EU level.

- Legislative measures beyond the European Union. As the internet is borderless these options for legislative measures could be complemented by agreements with key partner countries or through expanding multilateral treaties, in particular the Council of Europe Convention on Cybercrime.

As a next step Council of the European Union on 20th November 2017 adopted a set of council conclusions[56] where it called on the European Commission to present a legislative proposal t improve cross-border access to electronic evidence.

On 17th April 2018 the European Commission proposed the e-evidence package[57] which consisted of a draft Regulation[58] and Directive[59].

While the Regulation provides for new additional tools such as European Production Order and European Preservation Order, including relevant conditions and safeguards, the Directive obliges MSPs who are not established in the European Union but are offering services in the European Union, to designate one or more legal representatives in one or more Member States.

The proposal is based on the principles that offering services in the European Union by MSPs would make them also fall under the European Union law and jurisdiction. Therefore, they would need to comply also with lawful orders by Member States' competent authorities. The physical location of the MSP establishment or location of stored data is also considered as irrelevant and MSPs are required to preserve and produce data if requested so.

As European Union Member States send thousands of requests to US-based providers every year and not all of them have an office or representative in the European Union, a new legislative framework could facilitate access to data and provide added value compared to existing European Union and international instruments. In the same way, the proposal would address cooperation between Member States and enable direct cooperation between law enforcement and MSPs within the European Union.

Although the negotiations started in April 2018, and Council of the European Union has adopted a general approach, and agreed on both the Regulation and Directive, there are still negotiations or trilogues taking place with the European Parliament.

On 5th February 2019 the European Commission proposed the start of international negotiations on cross-border access to electronic evidence between the European Union and the US. A recommendation for a Council decision[60] and its Annex[61] were proposed to the Council of the European Union to agree on the mandate for the negotiations. As the US CLOUD Act and its executive agreements would cover areas that are within the competence of the European Union, such as personal data protection, Member States of the European Union cannot conclude bilateral agreements with the US. Therefore, an agreement could be concluded between the US and European Union.

Although the negotiations started in 2019, there has not been very much progress and as of May 2022 no discussions are taking place. One of the reasons has been inability to reach a

[56] https://www.consilium.europa.eu/media/31666/st14435en17.pdf

[57] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[58] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD)
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN

[59] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD)
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN

[60] https://ec.europa.eu/info/sites/default/files/recommendation_council_decision_eu_us_e-evidence.pdf

[61] https://ec.europa.eu/info/sites/default/files/annex_eu-us_evidence.pdf

compromise over the e-evidence proposal discussed above and the necessity to adopt internal rules for the European Union beforehand.

United Nations

In December 2019 the United Nations General assembly adopted a resolution 74/247[62] to establish an open-ended ad hoc intergovernmental committee of experts[63] to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

A new United Nations convention would also be likely to address international cooperation and related issues. It is expected that new convention would also take into account existing instruments and practices including related to the Council of Europe Convention on Cybercrime and relevant United Nations criminal justice conventions.

However, the exact scope and objectives are still not clear and are being debated by the ad hoc committee. Although the Convention on Cybercrime as well as the Second Additional Protocol have been proposed as guidance or as a benchmark by several countries and organisations, it is quite doubtful that a new convention would go beyond MLAT processes for access to data and that agreement could be reached with regard to other types of cooperation, including the direct cooperation with MSPs.

The substantive sessions started in 2022 and, pursuant to the resolution the ad hoc committee, is expected to conclude its work in 2024.

The above discussion shows that additional legal frameworks to support direct cooperation are likely to be regional (as in the case of the EU) or bi-lateral (US and partner country based on the CLOUD Act). As at the time of writing, a globally supported initiative on direct cooperation looks some way off.

8 Conclusions and recommendations

As stated at the beginning of this study, cooperation between the criminal justice and private sector is a necessity and the ability of law enforcement to lawfully access data held by MSPs, is essential to the functioning of criminal justice processes. Access to such data – subject to safeguards - will help to ensure that criminal perpetrators are brought to justice and that victims of crime are protected in the course of trials that are fair and just. This study has discussed the processes concerned in the accessing of that data when it is held or accessible in another jurisdiction.

In considering the efficacy of direct cooperation with MSPs for the purposes of accessing data, the 2017 study concluded that there are both advantages and disadvantages to reliance on this process. This remains the case today; as discussed above, direct cooperation is less fragmented as a process than MLA, and therefore potentially quicker but it can also be less than certain and less than transparent. It is hoped that the information provided in Section 5 above is of assistance and that it has provided some clarity on when to engage directly with MSPs and what to expect. As stated, practice has shown that there has been success when requesting preservation of data or in the requesting of data in emergency situations, subject to the requirements of the relevant MSP policy being met. As also explained, the uncertainties

[62] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement

[63] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

concerning access to subscriber data and the definition of an emergency (for the purposes of expedited cooperation and MLA) will be met once the Second Additional Protocol is in force. Meanwhile, the MLA process will not be abandoned and will continue to complement access to data through direct cooperation.

The earlier study also conceded that the poor quality of law enforcement requests is an issue which can fetter direct cooperation however, guidance issued by the Council of Europe, as well as the international cooperation training delivered in 2017 and since, should have an impact on quality of requests. Law enforcement must be encouraged to participate in relevant training made available by the Council of Europe and to use resources such as the request templates developed precisely in order to ease the cooperation process. Where law enforcement does decide to engage in direct cooperation, they must expect requests to be thoroughly reviewed by MSPs for legitimacy and legality, and that access to data may be more difficult for those from countries with questionable human rights records or where implementation of the provisions of the Convention on Cybercrime is poor. MSPs themselves must be aware that requests for access to data will not subside and that sufficient resources to deal with such requests are needed. Also, greater transparency and ease of access to relevant policies would not go amiss.

The 2017 study emphasised the development of relationships between law enforcement and MSPs and use of discussion as a means of raising and solving issues of mutual concern. Also recommended was the development of internal structures and use of national contact points who could act as transmission points for requests and "relationship managers" with service providers also superintending requests thus injecting an element of quality control into the process. Much of this was reiterated in the in the Council of Europe updated report entitled: *Cooperation between law enforcement and internet service providers against cybercrime: towards common guidelines* (updated in 2020)[64]. The same report pointed to examples in the EAP region of the development of arrangements with service providers at national level[65] and other examples of good practice and training opportunities[66].

The discussion of the Second Additional Protocol and other initiatives in the EU and as a result of the CLOUD Act in Section 7 above show that direct cooperation with MSPs will take its place alongside MLA for the purposes of obtaining data, going forward. This means that the building of relationships between law enforcement and MSPs will remain in sharp focus as will international cooperation training, in anticipation of the Second Additional Protocol coming into force in the near future.

There is no doubt that direct cooperation between law enforcement and MSPs has become a viable option and provides law enforcement in countries all over the world additional tools to obtain evidence and fight crime. Still, it must be highlighted that one of the preconditions of such cooperation and key to success, is a clear and solid legislative framework, in particular procedural law provisions, conditions and safeguards.

The Second Additional Protocol and its tools are built on the existing provisions of the Council of Europe Convention on Cybercrime. Therefore, countries need to make sure that existing standards and requirements of the Convention are fully implemented. Otherwise, it will be difficult if not impossible to ensure effective implementation of the Protocol.

[64] At p 22 – 25 of the report.

[65] At p 20 – 21 of the report (Armenia and Georgia).

[66] At p 22 of the report: Conference hosted by European Commission and Council of Europe including several projects implemented by C-PROC including CyberEast, GLACY+, iproceeds2, cybersouth on international cooperation with service providers.

Countries are therefore encouraged to use all available options as well as channels for international cooperation, including direct cooperation with MSPs, cooperation between 24/7 points of contact and MLA. A particular measure, or type of cooperation, cannot fully replace or substitute another. Therefore, depending on the situation and type of data needed, countries need to make use of all the international cooperation possibilities available.

Direct cooperation is available now, and many countries have positive experiences, however, as this is still based on voluntary cooperation and lacks enforcement measures, it is not always entirely reliable. The new Second Additional Protocol introduces a legally binding framework for direct cooperation and a completely new mechanisms relating to emergency situations. Therefore, it is expected that once the Protocol enters into force, State Parties would use these measures more often, though there would still be certain limitations and countries would need to continue using MLAT requests where appropriate.

9 Annex

Definitions of categories of data

Whilst the Cybercrime Convention does not define electronic evidence, it does differentiate between categories of computer data which can be used as electronic evidence, these are: 'subscriber information', 'traffic data' and 'content data'. These categories of data are subject to different procedural powers and corresponding conditions and safeguards. For example, subscriber information is regarded as being less privacy intensive than content data, thus conditions to access it by way of grant of a production order are less onerous than the requirements for a search warrant or interception order to access content data which is the data category enjoying the highest level of protection.

Definitions of the data categories follow below:

Subscriber information is defined in Article 18(3) of the Cybercrime Convention, as:

> *any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*
> *a) the type of communication service used, the technical provisions taken thereto and the period of service;*
> *b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*
> *c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

The notion of **"traffic data"** is used in the Convention and also in the current EU e-privacy directive[67][68], e-evidence proposal and many national sources of law. It should be noted that definitions in these sources differ and that they are differently applied in different areas of law. According to Article 1(d) of the Convention, **traffic data** means:

> *any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*.

[67] Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

[68] However, new draft e-privacy regulation uses instead of traffic data electronic communications metadata: „*electronic communications metadata*" *means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication.*
Proposal for a Regulation of the European Parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

Such data is in possession of **service providers**, which are defined in Article 1(c) of the Convention as:

> *i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and*
> *ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.*

The notion of **content data** is relevant since it is subject to Convention's most intrusive procedural power – interception of content data, defined in Article 21. While the term 'content data' is not defined in the Convention itself, according to Explanatory report it refers to "content of the communication" or "information being conveyed by the communication (other than traffic data)".[69]

Most jurisdictions have legislation in place that allows for lawful access to data, including data held by national service providers. This is usually by way of a production order issued on application to a judge by a prosecutor or law enforcement official, conducting a criminal investigation. Some countries allow for emergency situations where interim orders data may be obtained in expectation of a final order with retrospective effect.

The question of obtaining data from MSPs became contentious and as a result the Cybercrime Convention Committee (T-CY) issued Guidance Note #10 on the use of national production orders to obtain subscriber information from MSPs offering services in a given territory [70]. This guidance was based on recommendations in final report of the T-CY Cloud Evidence Group on criminal justice access to electronic evidence in the cloud. The recommendations, for consideration by the T-CY, influenced the issuance of the guidance note.[71] It is recommended that readers of this study consider the contents of the above documents, in conjunction with this document to gain a full picture.

Extracts from the Convention on Cybercrime

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
   a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
   b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
   a the type of communication service used, the technical provisions taken thereto and the period of service;
   b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

[69] Explanatory report, para 209.

[70] https://rm.coe.int/16806a495e

[71] https://rm.coe.int/16806a495e

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Extracts from the Second Additional Protocol

Article 7 – Disclosure of subscriber information

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

2 a Each Party shall adopt such legislative and other measures as may be necessary for a service provider in its territory to disclose subscriber information in response to an order under paragraph 1.

b At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, a Party may – with respect to orders issued to service providers in its territory – make the following declaration: "The order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision".

3 The order under paragraph 1 shall specify:

a the issuing authority and date issued;
b a statement that the order is issued pursuant to this Protocol;
c the name and address of the service provider(s) to be served;
d the offence(s) that is/are the subject of the criminal investigation or proceeding;
e the authority seeking the specific subscriber information, if not the issuing authority; and
f a detailed description of the specific subscriber information sought.

4 The order under paragraph 1 shall be accompanied by the following supplemental information:

a the domestic legal grounds that empower the authority to issue the order;
b a reference to legal provisions and applicable penalties for the offence being I nvestigated or prosecuted;
c the contact information of the authority to which the service provider shall return the subscriber information, from which it can request further information, or to which it shall otherwise respond;
d the time frame within which and the manner in which to return the subscriber information;
e whether preservation of the data has already been sought, including the date of preservation and any applicable reference number;
f any special procedural instructions;
g if applicable, a statement that simultaneous notification has been made pursuant to paragraph 5; and
h any other information that may assist in obtaining disclosure of the subscriber information.

5 a A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, notify the Secretary General of the Council of Europe that, when an order is issued under paragraph 1 to a service provider in its territory, the Party requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding.

b Whether or not a Party requires notification under paragraph 5.a, it may require the service provider to consult the Party's authorities in identified circumstances prior to disclosure.

c The authorities notified under paragraph 5.a or consulted under paragraph 5.b may, without undue delay, instruct the service provider not to disclose the subscriber information if:

i disclosure may prejudice criminal investigations or proceedings in that Party; or

ii conditions or grounds for refusal would apply under Article 25, paragraph 4, and Article 27, paragraph 4, of the Convention had the subscriber information been sought through mutual assistance.

d The authorities notified under paragraph 5.a or consulted under paragraph 5.b:

i may request additional information from the authority referred to in paragraph 4.c for the purposes of applying paragraph 5.c and shall not disclose it to the service provider without that authority's consent; and

ii shall promptly inform the authority referred to in paragraph 4.c if the service provider has been instructed not to disclose the subscriber information and give the reasons for doing so.

e A Party shall designate a single authority to receive notification under paragraph 5.a and perform the actions described in paragraphs 5.b, 5.c and 5.d. The Party shall, at the time when notification to the Secretary General of the Council of Europe under paragraph 5.a is first given, communicate to the Secretary General the contact information of that authority.

f The Secretary General of the Council of Europe shall set up and keep updated a register of the authorities designated by the Parties pursuant to paragraph 5.e and whether and under what circumstances they require notification pursuant to paragraph 5.a. Each Party shall ensure that the details that it provides for the register are correct at all times.

6 If acceptable to the service provider, a Party may submit an order under paragraph 1 and supplemental information under paragraph 4 in electronic form. A Party may provide notification and additional information under paragraph 5 in electronic form. Appropriate levels of security and authentication may be required.

7 If a service provider informs the authority in paragraph 4.c that it will not disclose the subscriber information sought, or if it does not disclose subscriber information in response to the order under paragraph 1 within thirty days of receipt of the order or the timeframe stipulated in paragraph 4.d, whichever time period is longer, the competent authorities of the issuing Party may then seek to enforce the order only via Article 8 or other forms of mutual assistance. Parties may request that a service provider give a reason for refusing to disclose the subscriber information sought by the order.

8 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that an issuing Party shall seek disclosure of subscriber information from the service provider before seeking it under Article 8, unless the issuing Party provides a reasonable explanation for not having done so.

9 At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may:

a reserve the right not to apply this article; or

b if disclosure of certain types of access numbers under this article would be inconsistent with the fundamental principles of its domestic legal system, reserve the right not to apply this article to such numbers.

Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored

a subscriber information, and

b traffic data

in that service provider's possession or control which is needed for the Party's specific criminal investigations or proceedings.

2 Each Party shall adopt such legislative and other measures as may be necessary to give effect to an order under paragraph 1 submitted by a requesting Party.

3 In its request, the requesting Party shall submit the order under paragraph 1, the supporting information and any special procedural instructions to the requested Party.

a The order shall specify:

i the issuing authority and the date the order was issued;

ii a statement that the order is submitted pursuant to this Protocol;

iii the name and address of the service provider(s) to be served;

iv the offence(s) that is/are the subject of the criminal investigation or proceeding;

v the authority seeking the information or data, if not the issuing authority; and

vi a detailed description of the specific information or data sought.

b The supporting information, provided for the purpose of assisting the requested Party to give effect to the order and which shall not be disclosed to the service provider without the consent of the requesting Party, shall specify:

i the domestic legal grounds that empower the authority to issue the order;

ii the legal provisions and applicable penalties for the offence(s) being investigated or prosecuted;

iii the reason why the requesting Party believes that the service provider is in possession or control of the data;

iv a summary of the facts related to the investigation or proceeding;

v the relevance of the information or data to the investigation or proceeding;

vi contact information of an authority or authorities that may provide further information;

vii whether preservation of the information or data has already been sought, including the date of preservation and any applicable reference number; and

viii whether the information has or data have already been sought by other means, and, if so, in what manner.

c The requesting Party may request that the requested Party carry out special procedural instructions.

4 A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, that additional supporting information is required to give effect to orders under paragraph 1.

5 The requested Party shall accept requests in electronic form. It may require appropriate levels of security and authentication before accepting the request.

6 a The requested Party, from the date of receipt of all the information specified in paragraphs 3 and 4, shall make reasonable efforts to serve the service provider

within forty-five days, if not sooner, and shall order a return of requested information or data no later than:

i twenty days for subscriber information; and

ii forty-five days for traffic data.

b The requested Party shall provide for the transmission of the produced information or data to the requesting Party without undue delay.

7 If the requested Party cannot comply with the instructions under paragraph 3.c in the manner requested, it shall promptly inform the requesting Party, and, if applicable, specify any conditions under which it could comply, following which the requesting Party shall determine whether the request should nevertheless be executed.

8 The requested Party may refuse to execute a request on the grounds established in Article 25, paragraph 4, or Article 27, paragraph 4, of the Convention or may impose conditions it considers necessary to permit execution of the request. The requested Party may postpone execution of requests for reasons established under Article 27, paragraph 5, of the Convention. The requested Party shall notify the requesting Party as soon as practicable of the refusal, conditions, or postponement. The requested Party shall also notify the requesting Party of other circumstances that are likely to delay execution of the request significantly. Article 28, paragraph 2.b, of the Convention shall apply to this article.

9 a If the requesting Party cannot comply with a condition imposed by the requested Party under paragraph 8, it shall promptly inform the requested Party. The requested Party shall then determine if the information or material should nevertheless be provided.

b If the requesting Party accepts the condition, it shall be bound by it. The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in relation to that condition the use made of such information or material.

10 Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe and keep up to date the contact information of the authorities designated:

a to submit an order under this article; and

b to receive an order under this article.

11 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it requires that requests by other Parties under this article be submitted to it by the central authority of the requesting Party, or by such other authority as mutually determined between the Parties concerned.

12 The Secretary General of the Council of Europe shall set up and keep updated a register of authoritiesdesignatedbythePartiesunderparagraph10. EachPartyshallensurethatthedetails that it has provided for the register are correct at all times.

13 At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may reserve the right not to apply this article to traffic data.

Article 9 – Expedited disclosure of stored computer data in an emergency

1 a Each Party shall adopt such legislative and other measures as may be necessary, in an emergency, for its point of contact for the 24/7 Network referenced in Article 35 of the Convention ("point of contact") to transmit a request to and receive a request from a point of contact in another Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure

of specified, stored computer data in that service provider's possession or control, without a request for mutual assistance.

b A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it will not execute requests under paragraph 1.a seeking only the disclosure of subscriber information.

2 Each Party shall adopt such legislative and other measures as may be necessary to enable, pursuant to paragraph 1:

a its authorities to seek data from a service provider in its territory following a request under paragraph 1;

b a service provider in its territory to disclose the requested data to its authorities in response to a request under paragraph 2.a; and

c its authorities to provide the requested data to the requesting Party.

3 The request under paragraph 1 shall specify:

a the competent authority seeking the data and date on which the request was issued;

b a statement that the request is issued pursuant to this Protocol;

c the name and address of the service provider(s) in possession or control of the data sought;

d the offence(s) that is/are the subject of the criminal investigation or proceeding and a reference to its legal provisions and applicable penalties;

e sufficient facts to demonstrate that there is an emergency and how the data sought relate to it;

f a detailed description of the data sought;

g any special procedural instructions; and

h any other information that may assist in obtaining disclosure of the requested data.

4 The requested Party shall accept a request in electronic form. A Party may also accept a request transmitted orally and may require confirmation in electronic form. It may require appropriate levels of security and authentication before accepting the request.

5 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it requires requesting Parties, following the execution of the request, to submit the request and any supplemental information transmitted in support thereof, in a format and through such channel, which may include mutual assistance, as specified by the requested Party.

6 The requested Party shall inform the requesting Party of its determination on the request under paragraph 1 on a rapidly expedited basis and, if applicable, shall specify any conditions under which it would provide the data and any other forms of co-operation that may be available.

7 a If a requesting Party cannot comply with a condition imposed by the requested Party under paragraph 6, it shall promptly inform the requested Party. The requested Party shall then determine whether the information or material should nevertheless be provided. If the requesting Party accepts the condition, it shall be bound by it.

b The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in relation to that condition the use made of such information or material.