Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines

Revised study and guidelines

This project is funded by the European Union and the Council of Europe and implemented by the Council of Europe

Contact
Giorgi JOKHADZE
Project Manager
Giorgi.Jokhadze@coe.int
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania

Disclaimer

This document has been produced as part of a project co-funded by the European Union and the Council of Europe, with inputs from experts Markko Kunnapu (Estonia) and Nigel Jones (United Kingdom). The views expressed herein can in no way be taken to reflect the official opinion of either party.

Table of contents

1. Developments since the adoption of the initial guidelines in 2008

a. Introduction

Cooperation between public and private sector and in particular between law enforcement authorities (LEA) and Internet Service Providers (ISP) has always been important in order to ensure effective criminal justice response and fight against cybercrime.

Although the Budapest Convention provides for sufficient basis in terms of procedural measures at domestic level, further guidance is also needed. Cooperation and information exchange, including preservation and production of computer data must always be based on national legislation. National legislation provides both legal basis for procedural measures as well as conditions and safeguards.

However, while the national legislation provides for the basis for cooperation, all the technical details, channels of cooperation, joint activities on awareness raising and education as well as training, could be regulated in the guidelines, cooperation agreements or MoU-s.

In order to provide guidance to both LEA's and ISP's, the Council of Europe took action. In 2007 the Council of Europe - under the Project on Cybercrime - set up a working group[1] with representatives from law enforcement, industry and service provider associations. The tasks of the working group were to conduct a study[2] and draft LEA-ISP Guidelines[3]. The Guidelines were discussed and adopted at the Octopus Conference on cooperation against cybercrime[4] on April 1-2 2008 in Strasbourg, France.

The guidelines adopted:

- include common guidelines for both law enforcement and service providers and specific guidelines for each of them;
- are not to substitute legislation or other formal regulations, but rather to supplement and help regulations work in practice
- are based on good practices already available
- are to be adapted to the specific circumstances in each country.

The guidelines were able to serve as a blue-print or source of inspiration to national authorities in order to enhance and facilitate cooperation with private sector.

The Guidelines are available in the official languages of the Council of Europe – English and French as well as in Albanian, Arabic, Armenian, Azeri, Croatian, Georgian, Macedonian, Portuguese, Romanian, Russian, Serbian, Spanish, Turkish and Ukrainian.

The Guidelines have been used already in many countries, they have been used to promote public-private cooperation in capacity building projects and they have been also endorsed by the European Court of Human Rights.

As both documents were finalized in 2008, then a lot of information can be considered as out of date.

[1] https://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation

[2] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3bb

[3] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f69ac

[4] https://www.coe.int/en/web/cybercrime/ocotpus-interface-2008

The purpose of the present study is to provide an overview of relevant developments since 2008 at both Council of Europe and European Union level, and to provide updated template that could be used for cooperation and updated guidelines.

While several aspects described in the 2008 study are still useful today, these two studies could be read in conjunction.

b. 2020 Update information

The original study, when conducted in 2008, was up to date and relevant for the time. Much has changed in the intervening 12 years, particularly in respect of technological advances. Cloud storage for the masses was embryonic in 2008 with only Windows Sky Drive (2007) and Dropbox (2008) offering services that allowed the public to store data online as a commercial service. Since then, cloud storage has become ubiquitous and one of the biggest challenges to law enforcement investigating cybercrime and electronic evidence.

There have been many other changes, including the wide use of cryptocurrency, such as bitcoin, which was not introduced until 2009 and yet today is one of the favoured currencies used by cybercriminals. Although the technology and the concept of the dark market existed for many years, the beginning of the development of the TOR browser in 2008 and it subsequent release, had the then unintended consequence of providing a platform for criminals to conduct their business with more anonymity that had previously been possible. Through the vehicle of Darknet markets such as Silk Road and notable others, the task of law enforcement to access data about criminals and their crimes became more and more problematic.

The Internet and the services offered on it, are now the number one place for the commission of crime in the world. Some countries are seeing more online crime than offline crime. This has placed a great reliance by law enforcement on identifying criminals and collecting evidence from service providers. The initial report focused very much on the service providers that offered Internet connectivity and discussed effective mechanisms for the requestors, typically law enforcement agencies and the requestees - typically ISP's - could work more effectively to ensure that lawful access to data held by service providers could be managed. Addressing the cooperation between law enforcement authorities and Internet Service Providers cannot be considered as sufficient anymore. There is a need to encompass also other online service providers, including over-the-top service providers and information society service providers. As these services provided can also be used or abused by criminals, they need to be covered by necessary cooperation frameworks. The volume of requests for data by law enforcement have increased exponentially, with some countries such as the USA being inundated with requests for emergency action, preservation, production of data and take down of illegal material. Multinational Service Providers (MSP's) in the US, such as Google, Facebook, Microsoft, Apple and Yahoo have introduced law enforcement portals through which lawful requests may be made. These companies produce transparency reports, so that the public and each country can see the number of requests made under different categories and the level of response they have received. This approach is discussed later in the report. The approach of the 2020 study is to enhance the information provided in the 2008 report and guidelines, and bring it up to date, with legislative as well as procedural information. In addition, the template document for the submission of requests has been created and is included at Appendix "C"

Most of the findings in the original report are still valid today and as only a handful of countries have created formal relationships based on the recommendations of the report, it is worth reiterating the importance of service providers, whether Internet or Online service providers and those working in the criminal justice system, creating effective working relationships the manage lawful access to data. Those countries that have developed working relationships and, in some cases, working groups, have jointly overcome issues, created point of contact regimes and in some

instances, improved national legislation in this field[5].

As of June 2020, the Budapest Convention has 65 State Parties and that number is increasing every year.[6] Having State Parties in all the continents of the world and being supported by capacity building programs, as well as being used as source of information for policy makers and legislators worldwide, the Budapest Convention can be considered as a global instrument.

Probably the most important challenges for the law enforcement authorities in the future would be the development and use of Artificial Intelligence, further advances in the use of encryption technologies across a wider set of technologies than at present and the challenges created by use of cryptocurrencies, in particular identifying the criminals at one or other end of cryptocurrency transactions.

These new technologies on one hand would open lots of new opportunities to provide additional services, to automate different processes, bring new products and increase the security and privacy. However they could also bring additional challenges and obstacles for law enforcement.

As the use of the Artificial Intelligence could bring additional opportunities to fight crime, to prevent and tackle cyberattacks, it could also create new tools and modus operandi for cybercriminals.

Encryption is widely used in ensuring information security and cybersecurity. It can be used to protect personal data and secrecy of communications. Encryption tools are largely available and both commercial and open-source software can be used. Industry and service providers often use encryption by default which on one hand ensures protection of their customers. On the other, if these tools are used for malicious purposes, to prepare or commit crime, law enforcement authorities would have several problems and challenges related to access to data. If strong encryption, including end-to-end encryption is used, law enforcement authorities might not get access to computer data or electronic evidence that is needed to prevent or investigate crime.

Cryptocurrencies and virtual currencies have become a means of payment as well as used for investment and trading purposes. While individuals can use these currencies to make transactions, to buy and sell goods, they have also brought additional risks. They can be considered as a target for criminals who can try to steal or otherwise unlawfully obtain them form their owners. However, it can also be used to commit or facilitate crime as well as hide and launder the crime proceeds.

Law enforcement authorities will need to investigate criminal cases and have timely access to electronic evidence in the future. Therefore, both legislative framework and cooperation mechanisms need to keep the pace with new developments. As in addition to new opportunities these technologies will also bring new threats and could be used for malicious purposes. Law enforcement authorities need to be prepared in facing new threats and be ready to cooperate with relevant service providers.

Due to the extensive use of cloud computing technologies, service providers often have establishment in one country, infrastructure and servers in another and provide services in the third country.

Multinational service providers target customers in different countries. However, questions related to jurisdiction, respect of domestic legislation and rules as well as governments' roles and responsibilities, remains unclear.

While service providers need to respect the laws on privacy and personal data protection, there are also obligations related to cooperation with law enforcement and their lawful requests.

As most of the criminal investigations including all cybercrime investigations involve computer data or electronic evidence, lawful cooperation between law enforcement authorities and service providers must be ensured.

[5] http://www.internetcrimeforum.org.uk/
[6] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=7rYWn4r9

Law enforcement authorities while conducting criminal investigations depend more on electronic evidence and access to computer data. While most of the cybercrime offences are of cross-border nature, more international cooperation is needed to ensure access to data in the cloud.

However, there are problems and difficulties related to the international cooperation and mutual legal assistance (MLA). The MLA system and framework that has been in place for decades was not designed for and is not an effective tool to address computer data or electronic evidence.

Computer data can be manipulated with, changed, moved or deleted in a moment. MLA framework that requires communication between central authorities or even diplomatic authorities and involves lot of bureaucracy cannot be used effectively to investigate cybercrime or other cyber-related offence.

By the time requesting country prepares the request and transmits it to receiving country, the computer data needed could be lost. Although law enforcement authorities can take measures to have the computer data preserved very quickly, the actual production or disclosure of data could take a long time. When the computer data is finally obtained, it could have become useless or obsolete due to the lapsed time period. Therefore, additional opportunities for international cooperation should be explored.

Countries and law enforcement authorities are using more and more direct cooperation where law enforcement authorities address preservation and production orders directly to service providers that are physically established abroad.

The Budapest Convention remains as legal basis for such cooperation as well. Article 18 of the Convention allows State Parties to use production orders in order to obtain data from persons including service providers.

It is important to highlight that although being a domestic procedural measure, it can be used to obtain computer data from a service provider abroad. Law enforcement authority can, pursuant to domestic legislation, send a production order for subscriber data also to a service provider who is not based in the territory of an investigating State Party but is offering a service there.

Against these concerns, the Cybercrime Cooperation Committee (T-CY) of the Council of Europe is looking into questions concerning the enforcement of a domestic procedural measure in other jurisdictions since 2017, in the framework of work on the text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime.

Last but not least, the recent onset of COVID-19 pandemic and continuing disruption of social interactions across the globe have further exacerbated these problems. As individuals, businesses and governments are increasingly dependent on the use of information technology in the pandemic-related restrictions, computer-facilitated crime is on the rise and thus even stronger and more efficient cooperation is needed.

2. New legislative and other developments since 2008

a. Developments at the Council of Europe level

i. The Cybercrime Convention Committee (T-CY)

Legislative framework needs to keep the pace with new developments and where needed must be updated accordingly.

As regards fight against cybercrime and access to electronic evidence, the Budapest Convention remains as the only legally binding international instrument that has a global impact and coverage.

Although the Convention remains valid in terms of domestic and international cooperation measures, additional work has been started.

The Cybercrime Cooperation Committee (T-CY) has for years analysed and worked on topics related to cooperation with service providers and international cooperation.

The T-CY has established several working groups such as Transborder Group and Cloud Evidence Group to analyse international cooperation and access to electronic evidence in cyberspace and adopted several reports.[7]

In the report of the Transborder Group for 2013, the first time the elements for the 2nd Additional Protocol to the Budapest Convention were introduced.[8]

In December 2014 options for further action and Terms of Reference for a Cloud Evidence Group were proposed.[9]

During the next years the T-CY held several debates on access to cloud evidence and related challenges with a view to find both legislative and practical solutions.[10][11][12]

In September 2016 the T-CY prepared a report including recommendations for further action.[13]

In 2017 discussions on the scope and use of Article 18 started with a particular focus on Article 18 (1)b and production orders to foreign service providers. In March 2017 the T-CY adopted a Guidance Note #10 on Production orders for subscriber information (Article 18 Budapest Convention).[14]

---

[7] Transborder Access to Data and Jurisdiction: what are the options?(Adopted in December 2012)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8

[8] Report of the Transborder Group for 2013 (Adopted in November 2013)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e712e

[9] Transborder access to data and jurisdiction: Options for further action by the T-CY (Adopted in December 2014)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e

[10] Criminal Justice access to data in the cloud : challenges (May 2015)
https://rm.coe.int/1680304b59

[11] Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group (February 2016)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8

[12] Criminal justice access to data in the cloud: cooperation with "foreign" service providers (May 2016)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d

[13] Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY (September 2016)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e

[14] T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention)
https://rm.coe.int/16806f943e

Although the T-CY agreed on the content of the provision and provided explanations, there were still remaining questions concerning the enforcement of a domestic procedural measure in other jurisdiction. Therefore, it was also decided that this topic would be further analysed and included in the text of 2nd Additional Protocol.

The same year, in June 2017 the T-CY agreed and adopted the Terms of Reference for the Preparation of a Draft 2nd Additional Protocol.[15]

The work on the 2nd Additional Protocol started in September 2017, when the first Protocol Drafting Group meeting took place. It was followed by the first Protocol Drafting Plenary in November 2017. As of June 2020, the protocol negotiations are still taking place and are expected to be completed by December 2020.[16]

b. Other developments at the Council of Europe level

Since the adoption of the Guidelines at the Octopus Conference in 2008 there have been discussions on cooperation with service providers and Internet intermediaries also at other Council of Europe bodies.

The T-CY has endorsed guidelines during its meetings, and it has also been a useful resource for different capacity building activities. Although the cooperation between public and private sector is at first place based on domestic law and applicable legislation it has been recommended also to engage in a closer cooperation, conclude cooperation agreements and MoU-s and build together a culture of cooperation.

Closer cooperation and information exchange can also be considered as important tool to raise trust among different stakeholders.

c. Case law of the European Court of Human Rights

Although governments need to provide necessary legal framework in order to ensure cooperation and access to information, it hasn't been always the case.

In December 2008, almost 8 months after the guidelines were adopted, they were addressed by the European Court of Human Rights. In its decision K.U. v. FINLAND[17] the Court considered cooperation between the law enforcement authorities and service providers and explicitly referred to the guidelines and its aims:

"27. A global conference, "Cooperation against Cybercrime", held in Strasbourg on 1-2 April 2008 adopted the "Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime". The purpose of the Guidelines is to help law enforcement authorities and Internet service providers structure their interaction in relation to cybercrime issues. In order to enhance cybersecurity and minimise the use of services for illegal purposes, it was considered essential that the two parties cooperate with each other in an efficient manner. The Guidelines outline practical measures to be taken by law enforcement agencies and service providers, encouraging them to exchange information in order to strengthen their capacity to identify and combat emerging types of cybercrime. In particular, service providers are encouraged to cooperate with law enforcement agencies to help minimise the extent to which services are used for criminal activity as defined by law.".

Moreover, the Court also found a violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, because due to the lack of proper legislative framework

[15] Terms of Reference for the preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime
https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b
[16] Protocol negotiations
https://www.coe.int/en/web/cybercrime/t-cy-drafting-group
[17] https://hudoc.echr.coe.int/eng#{"tabview":["document"],"itemid":["001-89964"]}

the government had failed to fulfill its positive obligation to protect the individual and provide effective criminal justice response. The Court also found that the right to privacy and freedom of expression were not absolute and had to be balanced with other legitimate interests:

"49. The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not, however, in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged. This deficiency was later addressed. However, the mechanisms introduced by the Exercise of Freedom of Expression in Mass Media Act (see paragraph 21 above) came too late for the applicant.".

In January 2020 the Court, in its decision Breyer v. GERMANY[18], referred back to the decision K.U. v. FINLAND.

In this case the Court found that there was no violation of the Convention and reiterated the need to find a balance between the right to privacy and other imperatives:

"62. The Court is therefore not called in the present case to decide if and to what extent Article 10 of the Convention maybe be considered as guaranteeing a right for users of telecommunication services to anonymity (see, regarding the interest of Internet users in not disclosing their identity, Delfi AS v. Estonia [GC], no. 64569/09, § 147, 16 June 2015) and how this right would have to be balanced against others imperatives (see, mutatis mutandis, K.U. v. Finland, no. 2872/02, § 49, 2 December 2008).".

"76. The Court notes that while it has already examined a wide range of interferences with the right to private life under Article 8 of the Convention as a result of the storage, processing and use of personal data – see, for example, the use of surveillance via GPS in criminal investigations (Uzun v. Germany, no. 35623/05, 2 September 2010, or Ben Faiza v. France, no. 31446/12, 8 February 2018), the disclosure of identifying information to law enforcement authorities by telecommunication providers (K.U. v. Finland, no. 2872/02, 2 December 2008 or Benedik v. Slovenia, no. 62357/14, 24 April 2018), the indefinite retention of fingerprints, cell samples and DNA profiles after criminal proceedings (S. and Marper, cited above), the so-called metering or collection of usage or traffic data (Malone v. the United Kingdom, no. 8691/79, 2 August 1984; Copland v. the United Kingdom, no. 62617/00, 3 April 2007) or the inclusion of sex offenders in an automated national judicial database subsequent to a conviction for rape (B.B. v. France, no. 5335/06, Gardel v. France, no. 16428/05 and M.B. v. France, no. 22115/06, all 17 December 2009) – none of the previous cases have concerned the storage of such a data set as in the present case.".

[18] https://hudoc.echr.coe.int/eng#{"tabview":["document"],"itemid":["001-200442"]}

d. Work under Steering Committee on Media and Information Society (CDMSI)

In parallel to the work and activities of the T-CY the Council of Europe Steering Committee on Media and Information Society (CDMSI) has also discussed the cooperation between law enforcement and service providers (Internet intermediaries).[19][20]

From January 2016 to December 2017 the Committee of experts on Internet Intermediaries (MSI-NET) was active.[21]

The task of the MSI-NET was under supervision of the CDMSI to analyse and prepare standard setting proposals and draft recommendation by the Committee of Ministers.

Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries was adopted by the Committee of Ministers on 7 March 2018.[22] The appendix to the recommendation includes "Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities".

The recommendation recommends Member States to implement the guidelines included. However the recommendation in its point 12 also refers to the 2008 Guidelines for the cooperation between law enforcement and internet service providers against cybercrime.

*"12. Against this background and in order to provide guidance to all relevant actors who are faced with the complex task of protecting and respecting human rights in the digital environment**, the Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe (ETS No. 1), recommends that member States**:*

- implement the guidelines included in this recommendation when devising and implementing legislative frameworks relating to internet intermediaries in line with their relevant obligations under the European Convention on Human Rights, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, "Convention 108"), the Convention on Cybercrime (ETS No. 185, "the Budapest Convention"), the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, "the Lanzarote Convention") and the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS No. 210, "the Istanbul Convention"), and promote them in international and regional forums that deal with the roles and responsibilities of internet intermediaries and with the protection and promotion of human rights in the online environment;

- take all necessary measures to ensure that internet intermediaries fulfil their responsibilities to respect human rights in line with the United Nations Guiding Principles on Business and Human Rights and the Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business;

***- in implementing the guidelines, take due account** of Committee of Ministers Recommendation CM/Rec(2016)5 on Internet freedom, Recommendation CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, Recommendation CM/Rec(2015)6 on the free, transboundary flow of information on the Internet, Recommendation CM/Rec(2014)6 on a Guide to human rights for Internet users, Recommendation CM/Rec(2013)1 on gender equality and media, Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines, Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services, Recommendation CM/Rec(2011)7 on a new notion of media, Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context*

[19] https://www.coe.int/en/web/freedom-expression/internet-intermediaries#{"36890493":[1]}
[20] https://rm.coe.int/leaflet-internet-intermediaries-en/168089e572
[21] https://www.coe.int/en/web/freedom-expression/committee-of-experts-on-internet-intermediaries-msi-net-
[22] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14

of profiling, Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet, as well as the 2017 Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, and ***the 2008 Guidelines for the cooperation between law enforcement and internet service providers against cybercrime****;*

- implement the guidelines included in this Recommendation in the understanding that, as far as they concern the responsibilities of internet service providers that have significantly evolved in the past decade, they are intended to build on and reinforce the Human rights guidelines for internet service providers, drawn up in 2008 by the Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA);

- engage in a regular, inclusive and transparent dialogue with all relevant stakeholders, including from the private sector, public service media, civil society, education establishments and academia, with a view to sharing and discussing information and promoting the responsible use of emerging technological developments related to internet intermediaries that impact the exercise and enjoyment of human rights and related legal and policy issues;

- encourage and promote the implementation of effective age- and gender-sensitive media and information literacy programmes to enable all adults, young people and children to enjoy the benefits and minimise the exposure to risks of the online communications environment, in co-operation with all relevant stakeholders, including from the private sector, public service media, civil society, education establishments, academia and technical institutes;

- review regularly the measures taken to implement this Recommendation with a view to enhancing their effectiveness.".

e. Internet Governance and Cooperation with Companies

On 30 March 2016, the Internet Governance Strategy 2016-2019 was adopted by the Council of Europe's member states which inter alia called for dialogue and cooperation with Internet companies and their representative associations.

On 8 November 2017 the Secretary General of the Council of Europe signed the agreement – in the form of an exchange of letters – with representatives of eight leading technology firms and six associations.[23] Later in 2018 and 2020 additional companies and business associations have joined the cooperation framework.[24]

Since the establishment of the cooperation framework several meetings have taken place.[25]

New established platform has enabled both Member States and Internet companies and associations to exchange views, discuss the challenges and propose solutions.

So far, the Internet companies and Member States have proposed the following:

"Summary of points raised by Internet companies

- more dialogue with governments is welcomed, including exchanges of views, collecting best practice, promoting transparency, and building capacity
- tackling crime effectively is difficult because of uncertainty and lack of harmonization in applying law across borders, and inconsistency between national regulations and international obligations
- companies which work too closely with governments can be negatively perceived

[23] https://www.coe.int/en/web/freedom-expression/exchange-of-letters#{"39018364":[]}
[24] Initially the companies were Apple, Deutsche Telekom, Facebook, Google, Microsoft, Kaspersky Lab, Orange and Telefónica. The associations were Computer & Communications Industry Association (CCIA), DIGITALEUROPE, the European Digital SME Alliance, the European Telecommunications Network Operators' Association (ETNO), GSMA and the multi-stakeholder Global Network Initiative (GNI).
On 23 on May 2018 two new entities, Cloudflare and EuroISPA joined.
On 6 February 2020, five new companies and business associations, Element AI, ICCO, IEEE, Intel and RIPE NCC joined the cooperation framework.

[25] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168074fe18

- *there is increasing pressure on companies to respect human rights, in particular the right to privacy*
- *there is need for greater certainty, predictability and efficiency in the application and implementation of legal frameworks; and need for a clear legal basis on which to provide Internet services so that law and jurisdiction is understood and interpreted in a manner which does not lead to the re-engineering of Internet services that might render data less secure*
- *greater efforts should be made to raise judges' awareness of the unique features and challenges of the Internet".*

"Summary of points raised by member States

- *more regular dialogue with Internet companies is welcomed*
- *guidance is needed to interpret partnerships undertaken, in particular their added value, scope, rules of procedure, and tangible outcomes envisaged*
- *roadmaps are necessary to help measure progress in the implementation of partnerships undertaken, this should include a "rendez-vous clause" for their periodic review".*

f. Work under the Parliamentary Assembly

On 26 June 2015 Parliamentary Assembly of the Council of Europe adopted Recommendation 2077 (2015) and Resolution 2070 (2015) on "Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet".[2627]

In the recommendation Parties to the Budapest Convention are inter alia invited to draft another additional protocol on mutual assistance regarding investigative power and invite the Cloud Evidence Group established by the Cybercrime Convention Committee to study the feasibility of drafting an additional protocol to the Convention on Cybercrime regarding criminal justice access to data on cloud servers.

It also calls for increased assistance and monitoring activities regarding the implementation of the Convention on Cybercrime in domestic law and practice, as well as practical measures and co-operation against large-scale cyberattacks, in particular for the benefit of member States where the practical implementation of the Convention on Cybercrime faces difficulties.

The resolution that was adopted together with the recommendation goes even more into details. It points out that through the growth of the Internet and other computer networks new vulnerabilities have emerged. The Assembly believes that further work is necessary to react, address adequately new challenges and secure electronic evidence.

The Assembly also recommends that Member States establish an adequate legal framework for public–private co-operation and ensure that service providers report on large-scale cyberattacks.

[26] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21976&lang=en
[27] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21975&lang=en

3. Developments at European Union level

a. Work on the e-evidence

The European Union as an observer at the T-CY has been closely following the discussions at the Council of Europe level related to new legislative and practical solutions.

In June 2016, the European Union Justice and Home Affairs Council adopted council conclusions where the European Commission was given a task to commence work, analyse the feasibility and prepare legislative proposals on access to electronic evidence.[28]

According to the conclusions one of the tasks was to analyse and propose solutions on how to improve cooperation with service providers.[29]

The European Commission started consultations with private sector, industry and law enforcement authorities and as a result proposed an e-evidence proposal or package that consisted of draft regulation and draft directive.[30]

As the regulation would provide for the EU-wide framework and common standards on European Preservation Order and European Production Order, the Directive is addressing the challenges related to enforcement of those abovementioned orders.

International cooperation and direct cooperation with service providers in other jurisdictions often fails due to the lengthy processes and complicated bureaucracy. Voluntary cooperation that has been used between law enforcement authorities and service providers abroad can often be discretionary and not effective. Although countries can send orders to service providers abroad there are no legislative mechanisms to enforce the orders and ensure their timely execution.

Directive takes an important step here and obliges all service providers abroad who offer services in the European Union, to designate a legal representative in one or more Member States. Having a legal representative in the European Union solves then problems related to enforcement, because the representatives would be bound by European Union law and in case of non-compliance sanctions can be imposed.

The draft regulation covers wide range of different service providers. In addition to the providers of Internet and telecommunication services it covers also information society services and Internet registries and registrars.

Although the proposal was tabled already in April 2018 and discussions on the text started immediately, there is still no final position or agreement.

As the European Union is also looking at additional options to expand and facilitate international cooperation with non-European countries, it is also participating at other international negotiations.

In February 2019 the European Commission proposed draft mandates on negotiations for 2nd Additional Protocol and agreement between European Union and United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters.[31]

The discussions on the draft mandates started in March and in June 2019 the Justice and Home Affairs Council adopted both mandates and gave the European Commission an authorisation to engage in negotiations.[32]

---

[28] https://www.consilium.europa.eu/en/press/press-releases/2016/06/09/criminal-activities-cyberspace/
[29] Council conclusions on improving criminal justice in cyberspace https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf
[30] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en
[31] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en#internationalnegotiations
[32] https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

b. Other developments at the European Union level

i.Substantive law

Since 2008 there have been extensive changes in the legislative and policy framework related to fight against cybercrime. Several previous legislative instruments have been updated and new instruments have been adopted.

The central piece of legislation at the European Union level to fight cybercrime used to be Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.[33] While being mostly substantive law instrument it did cover also certain procedural law aspects such as information exchange and the use of network of operational points of contact available 24 hours a day and seven days per week.

As the Framework Decision was considered outdated, the European Commission proposed a new draft directive which was adopted in 2013.[34]

New Directive on attacks against information systems was based on the previous instrument, but introduced higher standards concerning substantive law, including aggravating circumstances. It also went further in terms of information exchange, monitoring and statistics.

Neither the framework decision nor directive covered the aspects of computer related fraud. Instead a separate instrument from 2001 was in place to address combating fraud and counterfeiting of non-cash means of payment.[35]

As the legislation was very limited and covered only few aspects of fraud, a new draft directive was proposed by the European Commission in 2017 and it was adopted in 2019.[36]

The new text was more detailed and introduced higher standards compared to previous framework decision. It makes a distinction between corporeal and non-corporeal payment instruments and accordingly introduces different offences related to the commission and preparation of non-cash means of payment fraud.

New directive also covers certain aspects of procedural law, including jurisdiction, exchange of information, reporting of crime, prevention and assistance to victims.

ii. Procedural law

Until 2014 the Member States of the European Union had to rely on European Union Mutual Legal Assistance Convention of 2000 while cooperating in criminal matters and exchanging evidence.[37]

In 2014 it was replaced by the new directive that introduced European Investigation Order.[38]

New directive introduced direct cooperation between competent authorities, shorter deadlines to respond and was based on the mutual recognition principle that made possible to execute a request

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1585917740838&uri=CELEX:32005F0222
[34] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040
[35] Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1585918163006&uri=CELEX:32001F0413
[36] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG
[37] Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:42000A0712(01)
[38] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041

or order from one Member State in another. However, it excludes two Member States – Denmark and Ireland – and this means that in order to cooperate with these two Member States it is still necessary to use the provisions of the MLA Convention 2000.

Although the introduction of a new European Investigation Order was much welcomed, it became still clear that it was not suitable to address electronic evidence. That in turn has led to a situation where negotiations on European Union e-evidence proposal were started and Member States' law enforcement authorities are looking forward to the outcome.

iii. Personal data protection framework

In 2016 new European Union framework for personal data protection was adopted. New data protection reform package contained General Data Protection Regulation[39] and Police Directive.[40]

This data protection reform not only repealed previous instruments on personal data protection, but also brought personal data protection in European Union to a next level. By having new regulation which is directly applicable in all Member States, common European Union wide standards were introduced. While previously Member States had certain flexibility in terms of implementation then new regulation established common standards for all.

Still, as regards the processing of personal data for law enforcement purposes then these rules were provided by the directive and that meant that each Member State had to implement it in its domestic law.

New data protection framework introduced additional rights to data subjects and obligations to data processors from both public and private sector. However new rules had also an impact on the activities of law enforcement authorities.

Computer data or electronic evidence that is needed for criminal investigation purposes often contains personal data. Personal data could be both in outgoing orders or requests and incoming responses. Requests for personal data need to be lawful and respect personal data protection principles and rights of the data subject. In general terms private sector entities including service providers are not allowed to disclose personal data unless there is a proper legal basis.

Law enforcement authorities and international cooperation in criminal matters must also respect the rules on transborder data flows. If the other country doesn't have a sufficient or adequate data protection standards in place then transfer of personal data is only allowed in exigent circumstances.

This affects also direct cooperation between law enforcement authority and service provider based in another country. As also the request to a service provider may contain personal data all personal data protection related conditions and safeguards must be applied.

According to Article 39 of the Police Directive transfer of personal data may occur if it is based on international agreement. In principle such an agreement could also be the 2nd Additional Protocol to the Budapest Convention. Still, countries need to pay attention to personal data protection standards.

[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/eli/reg/2016/679/oj

[40] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680

Part of the personal data protection reform was also update to ePrivacy directive[41] and to provide new set of rules for electronic communications sector.

In 2017 the European Commission proposed a new draft ePrivacy Regulation.[42] Although the negotiations at the European Union level have lasted for years, there is still no agreement or final position on the text.

iv. Retention of telecommunications data

One way to ensure the availability of data in the telecommunications sector, is to provide a legal framework on mandatory retention of data.

In 2006 the European Union adopted Data Retention Directive[43] according to which Member States had to oblige telecommunication service providers to retain subscriber and traffic data.

In April 2014 the European Court of Justice in its joined Cases C-293/12 and C-594/12 decision[44] declared the directive invalid. Although the directive was declared invalid Member States could still preserve the data retention framework based on their domestic law and ePrivacy Directive.

In December 2016 the European Court of Justice delivered another decision on the topic. In the decision in joined cases C-203/15 and C-698/15[45] the Court declared that obligation relating to the general and indiscriminate retention of traffic and location data was not in line with the European Union law.

As of April 2020, there are still several similar cases pending at the Court. While several Member States have dropped data retention frameworks, there are others who are analysing and working in order to improve the relevant legislation.

As many countries don't have data retention frameworks, their telecommunication service providers are not bound by obligation to retain data. This has led to a situation where law enforcement authorities have often difficulties in obtaining electronic evidence needed in criminal investigations. In addition to domestic cases it has also an impact on international cooperation.

[41] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058
[42] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation
[43] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0024
[44] Digital Rights Ireland
http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TXT&ancre=
[45] Tele 2 Sverige / Watson
http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN

4. Voluntary cooperation vs binding legislative framework

As regards cooperation with service providers then often it can take place on a voluntary basis. In this case law enforcement authorities may ask for preservation or production of data even when the service providers are not obliged to do so.

However, it is possible only when legislative framework allows this and there are no restrictions or limitations to the service providers' actions.

Cooperation on a voluntary basis has worked with service providers based in the United States of America who are subject to US laws. The reason for this has been the flexibility of Electronic Communications and Privacy Act 1986 (ECPA) which enables service providers to disclose non-content data. ECPA prohibits service providers to give access to content data on a voluntary basis, except in cases of emergency.

However, the voluntary nature means that the disclosure would be entirely within the discretion of a service provider and for law enforcement authority there would be no foreseeability. Service provider might provide necessary data, it could provide it only partially and also decide when to disclose the data. Service provider could also notify the data subject and therefore cause harm or jeopardise the ongoing investigation.

Voluntary cooperation also means that although it is possible to send the request or order to a service provider, there are no means to enforce it.

Several countries have also been skeptical whether to send request directly to service providers or not, because question on the jurisdiction and limits of domestic procedural laws have arisen.

Still, as such a direct cooperation has been provided by the Budapest Convention and recommended by the T-CY, it is still a measure underused.

As it has been mentioned above, the voluntary cooperation works with US-based service providers. Although European law enforcement authorities can benefit from such a cooperation and get data from US, it doesn't work the other way around.

While European law enforcement authorities can get data from US-based service providers they cannot use this opportunity for providers based in Europe, in particular in European Union Member States.

Service providers have also obligations related to their customers, subscribers and their personal data. Obligations to keep the personal data confidential and not to disclose it without clear legal basis derive from both European Union and Member States' domestic legislation.

This in turn means that there would be no room for a cooperation on a voluntary basis. If provider decides to disclose personal data on a voluntary basis, it could be considered as a breach of data protection rules and provider could face sanctions.

a. Memoranda of Cooperation

The concept of creating Memoranda of Understanding (MOU) between Service Providers and law enforcement has been established for over two decades in some countries[46] and was very well articulated in the 2008 report, which provided clear advice on how this could be achieved. The document has been used to assist countries receiving support under the various Council of Europe capacity building programmes, in the intervening period. Moreover, the European Court of Human

[46] http://www.internetcrimeforum.org.uk

Rights referred in the case of K.U. v Finland[47] to the Guidelines as relevant international materials applying in this case related to the protection of the right to respect for private and family life (article 8 of the European Convention for Human Rights). In practical terms, representatives of law enforcement and service providers in a given country may establish a working group with the aim of reaching an understanding or even a formal agreement on how to cooperate with each other. The guidelines could serve as a blue-print or simply as a basis for discussion. The guidelines have been updated in the 2020 study.

Georgia, in 2010 introduced an MOU that was signed by the ten largest ISP's, the prosecution service and Ministry of the Interior. "[48]The Memorandum defines the principles of cooperation between ISPs and law enforcement agencies in the process of investigation of cybercrime and specifies the rights as well as responsibilities of the parties to the memorandum. Among the most important achievements under the document is the creation of specialized contact points within the structure of ISPs and the law enforcement, and significant reduction of time for processing of law enforcement requests". At the time of this study, the Georgian authorities are seeking to renegotiate the terms of the current MOU, as it is now considered in need of improvements. The original agreement has however, engendered a culture of cooperation between the parties that continues.

Another example of an MOU is that of Armenia, where,"[49]On 23 November 2015 the Investigative Committee signed a Memorandum of Understanding with Armenian Internet service providers, such as ArmenTel, K-Telecom, UCom, Orange Armenia, with the intention of reducing workload and saving human resources. The main goals of the Memorandum are to undertake effective joint measures in the direction of operative transmission of court decisions and transcripts, and to develop mutual cooperation on introduction of technical capabilities. Within this framework, parties agreed to communicate in a standardized manner (including cover letters, electronic signatures) and agreed to cooperate in solving issues as soon as possible in case of such procedures. Furthermore, the providers agreed to process electronic transmissions from the Investigative Committee within a short period of time and also to execute expeditiously court decisions which are designated as "urgent". A second objective of the Memorandum is to ensure that Internet Access Providers retain traffic data of their users for a set period of time".

In Bosnia and Herzegovina, "[50]The Ministry of Interior of Republika Srpska (MoI RS) – entered an agreement between MOI RS and service providers „Telekom Srpske" A.D. Banja Luka". This is applicable only to Republika Srpska.

In Denmark, "[51]The Danish Police and the service providers cooperate on the basis of informal agreements as to templates and exchange of information etc. according to the Act on Electronic

---

47 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa42a

48 https://www.coe.int/en/web/octopus/-/georg-3?redirect=https://www.coe.int/en/web/octopus/information-on-parties?p_p_id=101_INSTANCE_mSQWwCwFWET1&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_count=3

49 https://www.coe.int/en/web/octopus/-/armen-2?redirect=https://www.coe.int/en/web/octopus/information-on-parties?p_p_id=101_INSTANCE_mSQWwCwFWET1&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_count=3

50 https://www.coe.int/en/web/octopus/-/bosnia-and-herzegovi-3?redirect=https://www.coe.int/en/web/octopus/information-on-parties?p_p_id=101_INSTANCE_mSQWwCwFWET1&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_count=3

51 https://www.coe.int/en/web/octopus/-/denma-3?redirect=https://www.coe.int/en/web/octopus/information-on-

Communications Networks and Services. Cooperation with other private sector holders of data is agreed upon on a case-by-case basis of mutual cooperation".

In France, the "[52]The Ministry of Interior has set up partnership agreement with major providers to request them information from on a voluntary basis. There are 3 categories to request data:

- N1: General affairs
- N2: Serious harm to persons and property
- N3: The fight against terrorism and attacks on the fundamental interests of the nation"

"[53]In Hungary it is an obligation for the ISPs to answer law enforcement requests based on the Act XIX of 1998 on Criminal Proceedings. Beside this, the Hungarian Police has some special agreements with major ISPs." The extent of these special agreements is not known.

In Japan, "[54]Authorities exchange information with some service providers to facilitate seizure process; for instance, they exchange information on the location to execute a seizure warrant and how to describe the "object to be seized" in a seizure warrant".

The above seven, of the fifty-nine[55] listed parties to the Budapest Convention, have provided positive information on the Council of Europe Octopus Community website[56], where information on parties to the Budapest Convention is listed. This includes legislative mechanisms to ensure compliance with Articles 16/17 and 18 of the Budapest Conventions and the existence or otherwise of agreements between Parties and national service providers is listed. Unfortunately, many countries do not provide any information on the portal and analysis of the available information, indicates that many countries are relying solely on the rule of law in their interactions with service providers, and do not have any mechanism whereby they interact with providers on, for example creating single points of contact or create priority scales for cases under investigation.

Other useful documents that may assist countries in developing more effective working relationships between law enforcement and providers are contained in the documentation of the various capacity building programmes operated by the Council of Europe in the period since the 2008 report.

5. Council of Europe Cybercrime Capacity Building Initiatives

The Council of Europe Guidelines for cooperation between law enforcement and Internet service providers (2008) were developed under the Global Project on Cybercrime, as a part of the capacity building project. Overall, certain progress has been noted with regard to law enforcement/Internet service provider cooperation in line with the Guidelines, some of which are noted below.

There is a pressing need to reconcile the obligation of governments to protect society and individuals against crime while respecting the principles of rule of law and protecting the privacy, freedom of expression and all human rights of individuals. This is also true for countries participating in the Eastern Partnership. Often, local and multinational service providers are reluctant to cooperate, criminal justice measures and national security measures are not clearly

parties?p_p_id=101_INSTANCE_mSQWwCwFWET1&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_count=3

[52] https://www.coe.int/en/web/octopus/-/denma-3?redirect=https://www.coe.int/en/web/octopus/information-on-parties?p_p_id=101_INSTANCE_mSQWwCwFWET1&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_count=3
[53] https://www.coe.int/en/web/octopus/-/denma-3?redirect=https://www.coe.int/en/web/octopus/information-on-parties?p_p_id=101_INSTANCE_mSQWwCwFWET1&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_count=3
[54] https://www.coe.int/en/web/octopus/-/denma-3?redirect=https://www.coe.int/en/web/octopus/information-on-parties?p_p_id=101_INSTANCE_mSQWwCwFWET1&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_count=3
[55] There are 65 parties to the Budapest Convention at the time of this study. Only 59 are listed on the COE page referred to in this report.
[56] https://www.coe.int/en/web/octopus/information-on-parties

separated, there is lack of transparency and redress mechanisms, and public trust is limited. Moreover, law enforcement powers such as those foreseen in the Budapest Convention on Cybercrime are not always clearly defined in criminal procedure law, and this adversely affects law enforcement/service provider cooperation as well as human rights and the rule of law. Cooperation agreements thus need to contain safeguards to ensure that rule of law and human rights (including data protection) requirements are met.

In many cases, targeted capacity building activities can help in resolving these concerns. It is thus important that capacity building programmes maintain the level of importance on the creation and maintenance of working relationships between law enforcement and service providers at the national level. Those countries that are developing their national cybercrime strategies should ensure that component on the subject is included in the programme, especially the creation of memoranda of understating to ensure the efficient management of lawful request for data made by the authorities to industry. The advantages are set out in the updated guidance.

a. IPA Region Projects

In the Cyber@IPA project, which ran from 2010 to 2013, result 7, envisioned the objective of strengthening cooperation between law enforcement and Internet service providers (ISPs) in investigations related to cybercrime. This priority was identified in the assessment report[57] of June 2013 of the Cyber@IPA project and brought forward and adopted by countries as part of the declaration by Ministers and Senior Officials of the IPA region at the regional conference held in Dubrovnik from 13th to 15th February 2013.

There were a number of activities in the project designed to achieve the desired result, including a regional workshop on LEA/ISP cooperation held in Albania in June 2011. The meeting discussed the guidelines for cooperation between law enforcement and internet service providers against cybercrime, adopted by the Octopus Conference, Strasbourg, 1-2 April 2008. Law enforcement experts from Germany, France and Slovenia as well as representatives from Microsoft and the Association of the German Internet Industry (ECO) shared their experience.

This continuation of this priority was identified in the assessment report[58] of June 2013 of the Cybercrime@IPA project and brought forward and adopted by countries as part of the declaration by Ministers and Senior Officials of the IPA region at the regional conference held in Dubrovnik from 13th to 15th February 2013. This priority was not included in the workplan of the iProceeds project, which succeeded the cybercrime capacity building in the IPA region, nor in the project areas listed for the iProceeds-2 project, recently commence by the Council of Europe. However, it fair to note that law enforcement/ISP cooperation has featured as a component of some iProceeds activities, in particular the training courses and cybercrime scenario training activities, even though not included directly as a main priority of the projects.

b. Eastern Partnership Region

One of examples in the Eastern Partnership region is the Memorandum of Understanding between law enforcement and ISPs concluded in Georgia in 2010, prepared with the assistance of the EU/COE joint Project on Cybercrime in Georgia. The Memorandum of Understanding developed in Georgia is still in demand by others in the region and will help improve levels of cooperation in countries where the relationships are currently coercive and where cooperation can bring benefits in terms of information exchange and a better understanding of the issues faced by various parties.

---

57 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a0d

58 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a0d

The CyberCrime@EAP1 project, commenced in 2011, also contained a component on Law Enforcement – Internet service provider cooperation. A Regional seminar on LEA/ISP cooperation in cybercrime investigations was held from 26-27 April 2012, in Yerevan, Armenia, Law enforcement officers from five Eastern Partnership countries and representatives from the private sector discussed challenges and good practices to increase their cooperation in cybercrime investigations. Among the main obstacles identified were insufficient implementation of the Budapest Convention and related standards that provide a legal basis to provide such cooperation. The project identified follow-up on the recommendations made during these events;[59] one of the indirect outcomes of these was the conclusion of the Memorandum between the Investigative Committee and ISPs in Armenia in 2015

The declaration on strategic priorities held in Kyiv, Ukraine on 31st October 2013, included within the declaration, a commitment to strengthen cooperation with the private sector, in particular between law enforcement authorities and Internet Service Providers. The CyberCrime@EAPIII project responded to this objective by efforts to improve public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region. One relevant output of the project was the [60]General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership.

As a follow up to these initiatives, Output 3.4 of the current CyberEast project[61] foresees implementation of existing agreements on public/private cooperation and conclusion of such agreements in the remaining countries.

Overall, the countries of the Eastern Partnership have seen a great deal of support in past projects dealing with the subject of law enforcement/ISP cooperation and this is continued into the current CyberEast project. Georgia and Armenia are among the few countries that have developed memoranda of understanding and should continue to be encouraged to provide support to the remaining countries in the region. There have been clear issues relating to trust and need and it appears these still need to be resolved in order that the remaining countries are able to benefit from closer cooperation mechanisms.

c. Global Cybercrime Projects including GLACY and GLACY+

The Strategic priorities for cooperation on cybercrime and electronic evidence in GLACY countries[62] were adopted at the closing conference of the GLACY project on Global Action on Cybercrime Bucharest, 26 to 28 October 2016.

Although the strategic priorities carried forward into the GLACY+ project, there are no specific objectives on the subject area in the project summary document,[63] the commitment in the project summary to strengthen the cybercrime policies and strategies in 20 countries, may of course see the subject covered in these documents, especially as the issue of cooperation between law enforcement and online providers, should be a key strand of a national cybercrime policy. An example of this in action is the cybercrime strategy[64] of 2017 of Mauritius, one of the beneficiary countries of the GLACY+ project. Cooperation between private sector, in particular the service provider sector, and law enforcement, is seen as a crucial part of the strategy.

---

[59] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046c477

[60] https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b

[61] https://rm.coe.int/2088-cybereast-summary-and-workplan/168095cf19

[62] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b57b4

[63] https://rm.coe.int/3148-glacy-summary-v5/16809c8ad6

[64] http://cert-mu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf

6. Cooperation with Multinational Service Providers (MSP)

Since the 2008 report, more focus has been forthcoming on the issue of obtaining evidence from foreign service providers. The exponential growth of cloud storage together with the increase in international criminality has meant an ever-increasing number of requests to multinational service providers. The work, final report and recommendations of the COE Cloud Evidence Group[65] and the continuing work in relation to the 2nd Additional Protocol to the Budapest Convention are increasingly important.

Under the CyberCrime@EAP III project, a study on the strategy of cooperation with multinational service providers was conducted and a report[66] produced. The report offered insight into opportunities for effective cooperation between the law enforcement of the EAP and the multinational service providers. The overall purpose of the report is to evaluate the current direct cooperation mechanisms between law enforcement authorities in EAP region and multinational service providers with the aim to provide solutions on how to strengthen direct cooperation and increase the number of responses to requests. It noted that some law enforcement agencies experience difficulties to receive information in criminal cases from multinational service providers when using the direct communication channels, which prevents them to solve a criminal case in a timely manner. The study attempts to analyse the existing methods for cross border cooperation among law enforcement and multinational service providers, identify bottlenecks and propose solutions for timely exchange of information and protection of individuals' privacy.

The report sought to explore the issues form the perspectives of both law enforcement and the private sector.

For the purposes of this study, it is worth noting that the study examined the concerns of both parties to the ability to create cooperation mechanisms. Many of the concerns expressed are also relevant to the creation of models at the national level. Concerns include:

Dealing with law enforcement is challenging for the global companies for several reasons and their concerns fall broadly into the following categories:

a. MSP Concerns

- Low level of understanding about the business model by law enforcement.
- Multinational service providers provide variety of services and very often law enforcement are not familiar with them and how data in respect of these services may or may not be available. The lack of knowledge about a platform might have direct implications for a successful investigation. From multinational service provider point of view, better understanding about the services offered and mechanisms of data gathering process will help law enforcement in drafting better requests
- Maturity of the cooperation model between service providers and law enforcement has direct implications on the quality of the requests. It is advised for law enforcement to seek direct contact with service providers and build trusted relationships. This will increase their knowledge about the platform and as well will help them draft better data requests.
- Protection of human rights and abuse of power - if a request comes from a country with a poor human rights record, a request for data might be subject to a higher scrutiny. This might not be publicly announced in the multinational service providers' policies but is usually a consideration to take into account. In such situations it will be advisable to use the MLATs for requesting information.

[65] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e

[66] https://rm.coe.int/608-18-msp-cooperation-study-final/168074a4e3

- Multinational service providers have different level of commitment when dealing with law enforcement requests. Some providers do not have this infused in their management and thus have not build capabilities to deal with law enforcement request directly.
- Bad quality of requests: the reasons for a data request refusal could vary but the most often one is incomplete requests. To avoid this, it is advisable for law enforcement to undergo training how to build a data request with multinational providers.

b. Law Enforcement Concerns

Dealing with MSP's is challenging for law enforcement for several reasons and their concerns fall broadly into the following categories:

- Varying policies of MSP's in dealing with requests and, as a consequence, different response levels to different countries from different MSP's. For example, the response rate to the Netherlands is over 80% from Google and Microsoft, whereas Yahoo does not respond at all to requests from the Netherlands.
- The uncertainty of whether any response will be received from some MSP's. It has been described by some as a "lucky dip" in that a request is submitted and relies entirely on the decision of a private sector organisation as to whether data will be released.
- Many MSP's provide no response at all to some countries, leading them to the view that MSP's are making decisions based on their view of a country rather than a legal basis.
- No feedback is provided by MSP's as to the reason for refusal. In some instances, it may be administrative rather than substantive and capable of being rectified.
- One major concern to law enforcement is the disclosure policies of the MSP's. Examples were given in the recent COE "training programme on International Cooperation, including multinational ISP's, for the Eastern partnership region", where countries made direct request to MSP's when confronted with the potential that the individual personal information, including name, rank, position, email address and phone number, may be released to terrorist suspects as a result of the disclosure policy. They were not able to receive any assurance from the MSP's that their personal data was secure. This is an issue that cannot be solved with this report, other than being raised in the conclusions and recommendations.
- While the issue of lawful access to data held by MSP's in largely confined to those based in the USA, the issue of data exchange with service providers in other countries is often mentioned by law enforcement

Some of the conclusions of the study are relevant to both international and national level cooperation. As this report is fundamentally concerned with the mechanisms for cooperation at the national level, the relevant conclusions are included:

There are clearly issues with the quality of some submissions to MSP, even though most use a template format for completion by the law enforcement agency. This is in part because there is no requirement by the MSP for the request to be submitted by a Designated Point of Contact (POC), such as the designated 24/7 POC for parties to the BCC, or POC's of the G8 countries network. Similarly, there is no evidence that countries require all requests to be sent via such POC's, through which an element of quality control and suitability of the requests could be made.

Other than emergency requests, there is no prioritisation list for requests, in place to assist requesting and requested parties to better evaluate each request and provide a trusted method of establish the importance of requests. An agreed timetable of responses would also be beneficial.

Perhaps one of the main issues that lead to misunderstanding between parties is that there is no direct discussion or explanation of each parties concerns with the process. At the national level, there are examples of how discussion can ameliorate many of the problems. One example is the United Kingdom, where similar challenges were identified as long ago as 1986. Government, Law enforcement and the Internet Industry met to discuss how the lawful access to data could be achieved most effectively. Interestingly the model in place at that time was that of voluntary

disclosure under provisions of the UK Data Protection Legislation. As with the current international situation, the decision to release data was made by the ISP. A discussion group was created which later became known as the Internet Crime Forum. This led to an improvement in the quality of requests, better decision making by ISP's, development of dedicated POC's on each side and ultimately joint representation to government to introduce legislation to control lawful access to data with appropriate safeguards.

The only real prospect for improvement is for the parties (or representative groups) to discuss the issues and try to understand how the current difficulties impact on the businesses of the MSP's on one hand and the effective administration of justice on the other. It is clear, from national solutions that have been provided, that there is room for improvement and some of these may provide a baseline for discussion. Agreement from all MSP's and all LE may be challenging, however as with all solutions, the benefits are often not seen until positive action has been taken. Inertia is not an option, in this case. Ultimately, the MSP community could simply insist that all requests are made through the MLAT procedures and this is not a desired outcome, for the administration of justice.

The following, non-exhaustive list identifies some of the issues that may be included for discussion:

- Broad and Strategic Cooperation
- Legislation
- Procedures for Legally Binding Requests
- Designated Contact Points
- Training for LE and MSP's
- Technical Resources
- Authority for Requests
- Verification of Source of Request
- Standard Request Format
- Specificity and Accuracy of Requests
- Prioritisation of requests basedon agreed criteria
- Responses to requests
- Appropriateness of requests
- Confidentiality of data
- Disclosure of existence of requests
- Coordination among Law Enforcement Agencies
- Cross border service of national production orders
- Criminal compliance programmes (Audit)
- Costs
- Public awareness and crime prevention

The most recent initiative dealing with cooperation with MSP, was an international meeting held by the European Commission and the Cybercrime Programme Office of the Council of Europe (C-PROC) based in Bucharest, Romania hosted in Tbilisi, Georgia from Wednesday, 26 February 2020 to Friday, 28 February 2020 and was organised as a joint effort of several projects implemented by C-PROC, namely CyberEast, GLACY+, CyberSouth, iPROCEEDS-2. The sessions addressed the context for cooperation with foreign service providers, practical examples, Eurojust's SIRIUS project which is a useful repository for law enforcement and judiciary in Europe, provider policies and cooperation channels and opportunities: European perspective, human rights aspects/data protection concerns related to cooperation with foreign service providers, strategies of cooperation with foreign service providers, new opportunities for cooperation, as well as open discussion on experience of cooperation from across all regions represented during the event.

Conclusions

Many new challenges have arisen in the period since the 2008 study. Many of the considerations at that time still exist today. One main concern is the lack of memoranda dealing with LEA/SP Cooperation created since 2008. New impetus is needed to try and improve the situation, possibly best achieved through the Council of Europe capacity building programmes and other similar initiatives. Those countries that have developed working relationships between the parties have seen an improvement in the efficiency of the system and understand the benefits of establishing POC's.

Private sector and industry engagement activities with law enforcement, such as education, training, processes and impact assessment are very useful activities and should continue.

The benefit of representative organisations in areas of large numbers of Internet Industry players and law enforcement agencies/departments is significant to ensure consistent and transparent approaches to best practices.

The benefit of a single point of contact and a 24/7 contact and resourcing these points-of-contact is essential for it to be a success.

Working together creates a more accurate picture of the scale and impact of criminal use of the Internet, trends related to cybercrime and other online crime and its impact on the workload of Law Enforcement and Internet Industry. In addition, this would encourage greater appreciation (internally and externally) of the work of the ISP/OSP teams who handle requests from law enforcement. It is expected that if requests are managed by service providers through constant dialogue with LEA on the quality of the processes, they will be in a better position to anticipate the increasing and changing demands of LEA and will be at the same time protect themselves from inappropriate/excessive requests.

Sharing of good practice is essential for everyone to learn from each other and should continue.

The initial guidelines as adopted in Strasbourg on 1-2 April 2008 are most helpful in this respect.

The guidelines have been updated and due to new trends and emerging forms of crime their scope has been expanded. The importance of structured and effective cooperation mechanisms, whether through MOU's or incorporation within national cybercrime strategies cannot be overstated.

Appendix "A"
Template Request Form

Details of the organisation making the request		
Legal Name	(Full published name of the organisation)	
Address	(Published address of the organisation)	
Legal Status	(public prosecutor, national/local police etc)	
Web site	(official website of the organisation)	
Details of person making the request and to whom all responses should be addressed		
Name including badge/id number		
Rank	(Applicable to rank-based organisations such as the police)	
Position	(Such as cybercrime investigator, senior prosecutor, national SPOC etc)	
Email	(Must be an official email address (not yahoo, gmail etc))	
Telephone	(Must be a telephone number, not a personal one)	
Nature of the Request		
Emergency	YES/NO*	(Only to be used in cases of life at risk or death or serious injury/terrorism cases)
Data Preservation	YES/NO*	(Detail exactly what is being requested. Be specific and only use scope of what is necessary for the investigation. Provide all available information, including time zones of the criminal activity) This is to be used when requesting preservation pending lawful order to disclose data.
Data Production	YES/NO*	This is to be used when data is being requested to be produced or disclosed and requires the same level of detail as for data preservation.
Takedown	YES/NO*	(To request takedown of website, social network or other online posting)
Legal/Court Order	YES/NO*	(Any court or other judicial authority order must be attached to the request form)
Other	YES/NO*	(Provide full details and the legal basis for the request)
What Crime/s is Being investigated	(Provide the crime type/s according to your legislation and the Article/Section of the relevant law) The criminal case file or proceedings number should be included	
Overview of the criminal activity	(Provide an outline of how the crime was committed and any unique aspects. It is not necessary to identify individuals in this section. It is a summary of the crime). It is important to set out the legal basis for the request. This of course may be the court or other	
Subject of the request	(Provide as much detail of the individual or entity that is the subject of the request, include any physical information, such as name, address, date of birth and any online information such as user name/s, other online identities, IP addresses known, attach copies of any online information available, such as postings, photographs etc)	
What is being requested	(Provide details of exactly what you are asking for – account ownership, activity, postings etc. Be specific – no fishing expeditions)	

Type pf data requested	Subscriber Information YES/NO*	Traffic Data YES/NO*	Content Data YES/NO*
Time Limits	(Include if this request is limited by time, e.g. custody time limits, limitation on proceedings etc)		
Confidentiality	Some jurisdictions are required to inform data subject of requests made in respect of their data. Timescales for this vary between jurisdictions. If the application requires confidentiality, this must be set out here along with the legal basis for the confidentiality request.		

Note - * = Delete as Appropriate

Appendix "B"

Summary of Parties to the Budapest Convention, as listed on the COE Octopus Community

Country	Production Order Art 18	Preservation Order Arts 16 and 17	Emergency Provisions	Confidentiality	Partnership Agreement
Albania	Yes	Yes	Damage to Investigation	Yes	No
Andorra	No information	No Information	No Information	No Information	No
Argentina	No information	No Information	No Information	No Information	No
Armenia	No	No	Threat to Life	Yes	On 23 November 2015 the Investigative Committee signed a Memorandum of Understanding with Armenian Internet service providers, such as ArmenTel, K-Telecom, UCom, Orange Armenia, with the intention of reducing workload and saving human resources. The main goals of the Memorandum are to undertake effective joint measures in the direction of operative transmission of court decisions and transcripts, and to develop mutual cooperation on introduction of technical capabilities. Within this framework, parties agreed to communicate in a standardized manner (including cover letters, electronic signatures) and agreed to cooperate in solving issues as soon as possible in case of such procedures. Furthermore, the providers agreed to process electronic transmissions from the Investigative Committee within a short period of time and also to execute expeditiously court decisions which are designated as "urgent". A second objective of the Memorandum is to ensure that Internet Access Providers retain traffic data of their users for a set period of time.

Australia	No information	No Information	No Information	No Information	No
Austria	No information	No Information	No Information	No Information	No
Azerbaijan	No	No			There is currently no agreement between Government of the Republic of Azerbaijan and service providers offering a service at the territory of Azerbaijan. At the same time, general legal obligation to cooperate under Article 39 of Law of the Republic of Azerbaijan on Telecommunications tasks all communication providers to set up suitable conditions for carrying out operative-search activities by authorized state agencies, in particular, to "promote in proper legal manner implementation of search actions, supply telecommunication networks with extra technical devices a cording to terms set by corresponding executive power body for this goal, solve organizational issues and keep methods used in implementation of these actions as secret." NB: There is a general requirement for service providers to cooperate with law enforcement under Article 39 of the Law of Azerbaijan on Telecommunications
Belgium	No information	No Information	No Information	No Information	No
Bosnia and Herzegovina	Yes	Yes	Yes	Yes	Ministry of Interior of Republika Srpska (MoI RS) – agreement between MOI RS and service providers „Telekom Srpske" A.D. Banja Luka
Bulgaria	Yes	Yes	General Provisions	Yes	No

Cabo Verde	No information	No Information	No Information	No Information	No
Canada	No information	No Information	No Information	No Information	No
Chile	No information	No Information	No Information	No Information	No
Costa Rica	No information	No Information	No Information	No Information	No
Croatia	Yes	Yes	Risk of delay	Yes	No
Cyprus	No information	No Information	No Information	No Information	No
Czech Republic	Yes	Yes	No	Yes	No
Denmark	Yes	Yes	Only risk of delay	Yes	The Danish Police and the service providers cooperate on the basis of informal agreements as to templates and exchange of information etc. according to the Act on Electronic Communications Networks and Services. Cooperation with other private sector holders of data is agreed upon on a case-by-case basis of mutual cooperation.
Dominican Republic	No information	No Information	No Information	No Information	No
Estonia	Yes	Yes	State of Emergency	Yes	No

Finland	Yes	Yes	Risk to life or health	Yes	No
France	Yes	Yes	Risk to life, person in danger	Yes	Partnership agreement with providers The Ministry of Interior has set up partnership agreement with major foreign provider to request them information from on a voluntary basis. There are 3 categories to request data: • N1: General affairs • N2: Serious harm to persons and property • N3: The fight against terrorism and attacks on the fundamental interests of the nation
Georgia	Yes	Yes	State of Emergency	Yes	Since 2010, a Memorandum of cooperation between Internet Service Providers and Law Enforcement Agencies is in force. Ten largest ISPs representing the majority of the Internet industry and the representatives of government agencies, such as Prosecution Service and the Ministry of the Interior, signed the memorandum in January 2010. The Memorandum defines the principles of cooperation between ISPs and law enforcement agencies in the process of investigation of cybercrime and specifies the rights as well as responsibilities of the parties to the memorandum. Among the most important achievements under the document is the creation of specialized contact points within the structure of ISPs and the law enforcement, and significant reduction of time for processing of law enforcement requests.
Germany	Yes	Yes	Risk of Delay	Yes	No
Greece	No information	No Information	No Information	No Information	No

Hungary	Yes	Yes	Specific Crimes	Yes	In Hungary it is an obligation for the ISPs to answer law enforcement requests based on the Act XIX of 1998 on Criminal Proceedings. Beside this, the Hungarian Police has some special agreements with major ISPs.
Iceland	No information	No Information	No Information	No Information	No
Israel	Yes	Yes	Yes	Yes	No
Italy	Yes	Yes	No	No	No
Japan	Yes	Yes	No	Yes	Authorities exchange information with some service providers to facilitate seizure process; for instance they exchange information on the location to execute a seizure warrant and how to describe the "object to be seized" in a seizure warrant.
Latvia	No information	No Information	No Information	No Information	No
Liechenstein	Yes	Yes	Exceptional situations	Yes	No
Lithuania	No information	No Information	No Information	No Information	No
Luxembourg	No information	No Information	No Information	No Information	No
Malta	No information	No Information	No Information	No Information	No

Mauritiius	No information	No Information	No Information	No Information	No
Moldova	Yes	Yes	State of emergency	Yes	There are no agreements of cooperation between the Government of Moldova and the Internet service providers operating in the country. At the same time, the Law on Preventing and Combating Cybercrime of 2009 creates general obligations for the service provider to cooperate with the law enforcement. Under Article 5 of the Law, "in the activities of prevention and combating of cybercrime, competent authorities, service providers, non-governmental organizations and other representatives of the civil society cooperate through exchange of information and experts, through joint activities of criminal cases research, of offenders' identification and of personnel training, through the development of initiatives aimed to promote some programs, practices, measures, procedures and minimum security standards of computer systems, through information campaigns regarding the cybercrime and the risks to which the computer system users are exposed and through other activities related to this field."
Monaco	No information	No Information	No Information	No Information	No
Montenegro	Yes	Yes	Defined by case law	Yes	No
Netherlands	No information	No Information	No Information	No Information	No
North Macedonia	Yes	Yes	Risk to life, person in danger	Yes	No

Norway	No information	No Information	No Information	No Information	No
Panama	No information	No Information	No Information	No Information	No
Philippines	No information	No Information	No Information	No Information	No
Poland	No information	No Information	No Information	No Information	No
Portugal	No information	No Information	No Information	No Information	No
Romania	Yes	Yes	No	Yes	No
Senegal	No information	No Information	No Information	No Information	No
Serbia	No	Yes	Emergency situation	Yes	No
Slovakia	No information	No Information	No Information	No Information	No
Slovenia	No information	No Information	No Information	No Information	No
Spain	No information	No Information	No Information	No Information	No

Sri Lanka	No information	No Information	No Information	No Information	No
Switzerland	No information	No Information	No Information	No Information	No
Tonga	No information	No Information	No Information	No Information	No
Turkey	Yes	Yes	Risk of Delay	Yes	No
Ukraine	Yes	Yes	Emergency situation	Yes	No
United Kingdom	No information	No Information	No Information	No Information	No
United States o America	No information	No Information	No Information	No Information	No

Appendix "C"

Updated Guidelines

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Introduction

These guidelines have been updated to reflect the situation in 2020. The original guidelines already are often referenced as good practice in this field. This update should be considered as an addendum to the original guidelines and bring some new information to be considered and provide practical support to countries that are adopting cooperation mechanisms for the first time.

The number of cyber dependent crimes and other cyber enabled crimes is constantly increasing. The ability to combat cybercrime and to deal with crimes involving electronic evidence, more often, requires effective cooperation between the criminal justice authorities (CJA), law enforcement authorities (LEA), on the one hand and Internet Service Providers (ISP) and other Online Service Providers (OSP) on the other hand. Cooperation is needed, both with national and international providers.

Lawful access to electronic evidence in all its forms, wherever it is held, has become a key factor in criminal investigations. Most traditional as well as cyber dependent criminal investigations nowadays involve electronic evidence. Without timely access to electronic evidence criminal investigations and prosecutions often fail, allowing perpetrators to continue their illegal activities and create more victims. At the same time governments have positive obligation to protect its citizens from crime and ensure rule of law in cyberspace.

Most of the data needed in criminal investigations are being stored by private sector entities. In addition to ISP's attention has to be paid also to other service providers who offer services through information and communications technologies.

While governments have introduced legal frameworks and obligations for Internet and telecommunication service providers, there are no clear regulations for information society service providers online.

Online service providers are often established in one country and are offering services and targeting customers in other countries. This has raised questions and practical problems related to jurisdiction, access to data and enforcement.

Privacy and protection of personal data has become more important. Additional standards have been adopted by both Council of Europe and European Union. Updated Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) as well as European Union General Data Protection Regulation both provide for additional standards related to privacy and personal data protection.

Computer data used as evidence in criminal investigations often includes personal data. This brings additional obligations to governments as well as for CJA/LEA and ISP/OSP.

Criminal investigations, in particular cybercrime investigations often rely on international cooperation. As both Convention 108+ and GDPR have obligations related to transborder data flows, particular attention has to be paid when disclosing personal data to foreign entities.

ISP/OSP's have introduced different technological measures to protect their customers and their data. Often these measures include encryption which on one hand enable protection of customers' data and communications, but on the other make preservation and production of computer data for criminal justice purposes virtually impossible.

Both LEA and ISP/OSP's rely on domestic data retention policies for Internet service and telecommunications. While many countries have retained the policies and legislation for the retention of telecommunications data, it is not always the case. In case there is no data retention policy at domestic or at SP level or if domestic legislation prohibits retention of data, it also impacts on criminal investigations. If data is deleted or destroyed, there would be no opportunities to use either preservation or production order. This has a negative impact not only on domestic, but also on international investigations.

Many of the issues that impact on the lawful access to data required by CJA/LEA's and which is held by ISP/OSP's, occur because of misunderstanding of procedures and requirements, rather than any ill intent by the parties. Many of these issues could and should be managed by a closer level of cooperation between the parties. The aims of bringing criminal to justice and protecting the rights of individuals should be complimentary and not contradictory. Parties should strive towards a culture of cooperation and be as open and transparent as possible while paying respect to rules on confidentiality of criminal investigations and personal data protection and the laws that cover access to data in given circumstances. There are many examples of countries that have worked for many years in developing the interparty relationships, and which have led to the introduction of practice, procedure and in some cases legislation, which are clearly understood, lead to lawful access to data and in which any disputes can be easily managed. It is this level of cooperation that should be the aim of countries at the domestic level. At the international level countries should avail themselves of the provisions that are already available to enable lawful access to data. Countries should ensure that their prosecutors and investigators are fully aware of the provisions available to them for lawfully accessing data held internationally and that facilities are available for them to utilise these provisions.

It is important that agreements between parties are made at a strategic level, which will enable practitioners to work within clear guidelines and allow for lawful access to data to become a more effective mechanism, while allowing for oversight of the activities undertaken as a result of the agreements. It should not be left to individual practitioners to develop ad hoc relationships that cannot be maintained and that do not provide necessary safeguards for the parties.

Countries should use the Guidelines to the largest extent possible. Also, the European Court of Human Rights has endorsed the use of 2008 Guidelines in judgement K.U. v. Finland. The latter judgment has also been referred to in the judgment Breyer v. Germany.

While governments have positive obligation to protect its citizens from crime and establish necessary legal and organizational framework, balance need to be found between the rights of an individual and ISP/OSP and obligations of the governments.

It is important that cooperation mechanisms are created at the national level and in a timely manner.

Common guidelines

The Budapest Convention and provision implemented at domestic level remain as legal basis for both preservation and production orders to ISP/OSP's.

Article 18 of the Budapest Convention allows LEA to send production orders also to ISP/OSP's abroad if they are offering a service in the territory of the State Party.

As international organizations and governments are seeking new opportunities for closer cooperation between LEA and SP and to facilitate access to computer data, both LEA and SP side should be prepared to implement new rules and standards.

Both authorities and service providers should protect the fundamental rights of citizens according to United Nations and other applicable European and international standards such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the

1966 United Nations International Covenant on Civil and Political Rights, the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as domestic law. This places reasonable limits to the level of cooperation possible;

The guidelines are not intending to substitute existing legal instrument but assume adequate legal instruments exist that provide a well-balanced system of investigation instruments as well as related safeguards and a protection of fundamental human rights such as freedom of expression, the respect for private life, home and correspondence and the right to data protection. It is therefore recommended that states adopt regulations in their national law in order to fully implement the procedural provisions of the Convention on Cybercrime, and to define investigative authorities and obligations of law enforcement while putting in place conditions and safeguards as foreseen in Article 15 of the Convention. This will

a. ensure efficient work of law enforcement authorities;
b. protect the ability of ISP/OSP's to provide services;
c. ensure that national regulations are in line with global standards;
d. promote global standards instead of isolated national solutions;
e. help ensure due process and the rule of law, including principles of legality, proportionality and necessity.

For the purposes of these guidelines we use the definition of service provider included in the Convention on Cybercrime in Article 1 which defines "service provider" in a broad manner as meaning:

- any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service;

The purpose of the present guidelines is to help law enforcement authorities and Internet service providers structure their interactions in relation to cybercrime issues. They are based on existing good practices and should be applicable in any country around the world in accordance with national legislation and respect for the freedom of expression, privacy, the protection of personal data and other fundamental rights of citizens;

It is therefore recommended that States, law enforcement authorities and Internet service providers undertake the following measures at a national level:

- Parties should be encouraged to engage in a cooperation and information exchange. LEA should be encouraged to raise awareness with ISP/OSP's, concerning the threats and trends related to cybercrime and other online crime they are encountering. ISP/OSP's may also be aware of these crime types from a different perspective and can input their experience to the wider discussion.
- Law enforcement authorities and Internet service providers should be encouraged to engage in information exchange to strengthen their capacity to identify and combat emerging types of cybercrime. Law enforcement authorities should be encouraged to inform service providers about cybercrime trends;
- Parties should promote a culture of lawful cooperation, including sharing best practices and organizing regular joint meetings and trainings. Regular meetings in order to exchange experience and resolve any issues are encouraged.
- Law enforcement and service providers should be encouraged to develop written procedures for cooperation with each other, including designating points of contact and channels to exchange information. Where possible, both parties should be encouraged to provide structured feedback on the operation of these procedures to each other;

- Formal partnerships between law enforcement and service providers should be considered in order to establish longer-term relationships with proper guarantees for both sides that the partnership will not infringe any legal rights on the side of the industry or interfere with any legal powers on the side of law enforcement;
- LEA and SP, within the margins provided by domestic legislation, should explore ways to facilitate cooperation and shorten the time needed to execute LEA requests. Consideration should be given to grading requests according to the severity of the matter under investigation, and parallel response times introduced.
- If the domestic legislation of the country provides for a possibility for cost reimbursement, parties should consult with each other what costs and how could be reimbursed. Cost reimbursement schemes and related agreements between parties could be considered. Where possible, both parties should be encouraged to provide structured feedback on the operation of these procedures to each other;
- The Budapest Convention and provision implemented at domestic level remain as legal basis for both preservation and production orders to ISP/OSP's.
- Article 18 of the Budapest Convention allows LEA to send production orders also to ISP/OSP's abroad if they are offering a service in the territory of the State Party.
- As international organizations and governments are seeking new opportunities for closer cooperation between LEA and SP and to facilitate access to computer data, both LEA and SP side should be prepared to implement new rules and standards.
- Both law enforcement authorities and Internet service providers should protect the fundamental rights of citizens according to United Nations and other applicable European and international standards such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as domestic law. This places reasonable limits to the level of cooperation possible;
- Law enforcement authorities and Internet service providers are encouraged to cooperate with each other in view of enforcing privacy and data protection standards at the domestic level but also with regard to cross-border data flows. The work of the Council of Europe, the European Union and the OECD provides guidance in this respect;
- Both sides should be mindful of the costs involved in creating and responding to requests. Procedures should be developed with consideration of the financial impact of these activities and issues of cost reimbursement or fair compensation to relevant parties should be considered.

Measures to be taken by law enforcement

- Broad and Strategic Cooperation
    - Parties should be encouraged to engage in a cooperation and information exchange. LEA should be encouraged to raise awareness with ISP/OSP's, concerning the threats and trends related to cybercrime and other online crime they are encountering. ISP/OSP's may also be aware of these crime types from a different perspective and can input their experience to the wider discussion. It is imperative that any agreements made are at the strategic level, in order that they carry their full weight of each party.
- Legislation

- Parties should carefully consider the legislation that is in place to allow lawful access to data and consider proposals for any new legislation that may be needed to ensure that effective investigations may be undertaken with due respect for privacy and human rights considerations. Cooperation should be undertaken to ensure that gaps in legislation do not place undue burdens on parties to agreements. For example, in jurisdictions where there is no legal definition of electronic evidence and physical equipment is seized by LEA, the burden on businesses, whose equipment is seized is inequitable to the purpose of the seizure. Parties may consider it appropriate to propose new legislation to obviate this situation.

- Procedures for Legally Binding Requests
    - An MOU should contain clear and unambiguous procedures to be followed by parties in the event of applications being made. They should take into account the position of all parties and not be over onerous on one or the other party. Clarity is needed in all aspects of the development of joint working provisions of an MOU.

- Designated Points of Contact (POC)
    - Parties should develop written procedures for lawful cooperation, including designating points of contact and channels to exchange information. There are now several networks that operate through 24/7 POC schemes, for example the COE network dealing with requests made under Article 35 of the Budapest Convention, so the concept is well understood. It is less common for industry to have similar networks although in some countries there are parallel, industry and LEA POC's that work seamlessly in dealing with lawful access to data requests. These should be encouraged at the national level, not only because they are more effective, but they also engender a level or trust between the parties, that is often seen as an obstacle to cooperation.
    - Law enforcement should be encouraged to restrict the use of emergency contact points service to extremely urgent cases only to ensure this service is not abused;

- Training and information sharing
    - Parties should promote a culture of lawful cooperation, including sharing best practices and organizing regular joint meetings and trainings. Regular meetings in order to exchange experience and resolve any issues are encouraged. Law enforcement should be encouraged to provide training to a designated set of their personnel on how to implement these procedures, including the manner in which records may be obtained from service providers and how to process information received, but also on internet technologies and their impact in general as well on how to respect due process and the fundamental rights of individuals;

- Technical Resources
    - Some countries have introduced legislation that sets out who is responsible for the provision of equipment necessary to fulfil some lawful requests for data, such as where a court order has been issued for lawful interception of data. In many cases, smaller service providers will not be able to comply with such requests, because they simply do not have the necessary equipment and have not had the need to foresee circumstances when such activity will be necessary. In these instances, it is often the case that LEA's have the necessary equipment to carry out these lawful orders. Where there

is not clear legislation in place, consideration should be given to incorporate agreed procedures within an MOU.

- Law Enforcement should be in a position to be able to accept results of requests electronically.

- Authority for Requests
    - Any lawful request for access to data, must be accompanied by the relevant level of authority, whether the legislation allows for authority to be issued by a court, a prosecutor or in some cases by a senior police officer. Whereas the police should be aware of which authority may be needed for an application to be made, service providers may need to have further training in order to ensure they act in accordance with lawful authorities. This is an area where some joint training may be considered appropriate.
    - Law enforcement authorities should be encouraged to define clearly in their written procedures which law enforcement personnel can authorise what type of measures and requests to Internet service providers and how these requests can be validated/authenticated by Internet service providers;
- Verification of Source of Request
    - It should be possible for a recipient organisation to be able to verify the source of any request by reference to the issuing organisation or through a POC scheme set up as part of an MOU. It should not be necessary for a recipient to go through detailed investigation to validate the source of a request.
- Standard Request Format
    - Recipients of requests should be able to rely on a consistent approach by requesting bodies. One of the recommendations of the original study was for the creation of a standard template report. This has been addressed in this updated report and a proposed standard request template is included for consideration at Appendix "A"
- Specificity and Accuracy of Requests
    - Service providers receiving requests are entitled to receive documents that are clearly set out, specific and accurate. It is expected that the proposed standard request form will alleviate many of the difficulties associated with this aspect.
    - Law enforcement should be encouraged to provide as many facts about the investigation as possible without prejudicing the investigation or any fundamental rights in order to enable service providers to identify relevant data;
- Responses to requests and prioritisation of requests based on agreed criteria
    - Parties, within the margins provided by domestic legislation, should explore ways to facilitate cooperation and shorten the time needed to execute LEA requests. Consideration should be given to grading requests according to the severity of the matter under investigation, and parallel response times introduced.
    - Law enforcement should be encouraged to prioritise requests, especially those related to large volumes of data, to enable service providers to address the most important ones first. Prioritization is best done in a consistent manner across national law enforcement authorities and if possible

internationally;

- Appropriateness of requests
    - It should not be necessary to actually stipulate that all requests should be appropriate, however, there may be cases where a request may over reach or be so wide as to make it very difficult for recipients to carry out the request. Requests for information that is not strictly necessary should be avoided and it is the responsibility of the requesting body to ensure that requests are only made for data that is relevant and covering types of data and timescales that are appropriate. It may be necessary for further investigations to be made in order that these considerations are met before an application is made.
    - Law enforcement should be encouraged to be mindful of the cost that requests entail for service providers and give service providers sufficient response time. They should be mindful that service providers may also need to respond to requests from other law enforcement authorities, and should be encouraged to carefully monitor volumes submitted;
- Confidentiality of data
    - A concern of industry is to understand what happens to the data that is passed to LEA's as a result of lawful access requests they receive. LEA's are under the same legal obligations to handle data correctly and should be able to satisfy industry concerns through their published data protection policies. Developing an MOU may of course include requirements in this respect.
- Disclosure of existence of requests
    - LEA's have long expressed concerns that industry are often under an obligation to inform data subjects about any request for data that may be made against them. In some circumstances it has been known that these provisions have led to the disclosure the personal details of LEA staff to potential terrorist and organised crime groups. Most commercial organisations have public interest exemptions in their contracts with customers, that should afford the possibility to avoid these situations occurring, It is important that cases where disclosure would impact adversely on an investigation or put individuals at risk of injury or even death are discussed between parties. The creation of MOU's can help alleviate some of these issues.
- Coordination among Law Enforcement Agencies
    - One of the biggest concerns among providers is the sheer number of requests that are received from different law enforcement agencies at the national level. This may cause challenges for companies trying to work out if the request comes from a legitimate LEA. The establishment of POC's and clear lines of communications where lawful requests are being made, will assist. It is important therefore, that LEA's communicate and coordinate with each other when dealing with requests to service providers. It may be that having POC's in different agencies will be appropriate, however they should all come under the same framework programme to be developed.

      Law enforcement authorities should be encouraged to coordinate their cooperation with Internet service providers and share good practices among each other nationally and internationally. Internationally they should make use of relevant international representative bodies for that purpose;

- Cross border service of national production orders
    - There may be instances where a provider has legal presence in jurisdictions other than where the MOU is undertaken. Careful consideration should be given to the ability for providers to assist is serving production orders to associated companies in other jurisdictions. It will give additional comfort to the recipient in the other jurisdiction that the order is legal and effective.
- Audit
    - Law enforcement authorities should be encouraged to track and audit the system of processing requests for statistical purposes, for identifying strengths and weaknesses and publish such results if appropriate;
- Costs
    - If the domestic legislation of the country provides for a possibility for cost reimbursement, parties should consult with each other what costs and how could be reimbursed. Cost reimbursement schemes and related agreements between parties could be considered. Where possible, both parties should be encouraged to provide structured feedback on the operation of these procedures to each other;
- Public awareness and crime prevention
    - It is important that public awareness and crime prevention initiatives dealing with online crime, present a united front as far as possible, and to avoid mixed messaging that may occur if strategies are developed at the individual level. There will always be a place for individual public awareness campaigns, for example dealing with child safety online, however a programme based on the joint knowledge of the parties will be beneficial. This is particularly important when it comes to which body, incidents should be reported to and the establishment of clear lines of contact between parties to ensure the reports go to the correct organisation.

Measures to be taken by service providers

- Cooperation to minimize use of services for illegal purposes
    - Subject to applicable rights and freedoms, such as freedom of expression, privacy and other national or international laws, as well as user agreements, service providers should be encouraged to cooperate with law enforcement to help minimize the extent to which services are used for criminal activity as defined by law;
    - Service providers should be encouraged to report criminal incidents affecting the Internet service provider of which he is aware of to law enforcement. This does not oblige service providers to actively search for facts or circumstances indicating illegal activities;
    - Service providers should be encouraged to assist law enforcement with education, training and other support on their services and operations.
- Follow up to requests from law enforcement authorities
    - Service providers should be encouraged to undertake all reasonable efforts to assist law enforcement in executing the request;
- Procedures for responding to requests
    - Service providers should be encouraged to prepare written procedures,

which include appropriate due diligence measures, for the processing of requests, and ensure that requests are followed up to pursuant to the agreed procedures;

- Training
    - Service providers should be encouraged to make sure that sufficient training is provided to their personnel responsible for implementing these procedures;
- Designated personnel and contact points
    - Service providers should be encouraged to designate trained personnel as contact points for cooperation with law enforcement. These should mirror those created by law enforcement and become the default communication path for parties when dealing with lawful requests for data.
    - Service providers should be encouraged to establish a means by which law enforcement may reach their criminal compliance personnel outside of normal business hours to address emergency situations. Service providers should be encouraged to provide law enforcement with relevant information for emergency assistance;
    - Service providers should be encouraged to provide contact points or personnel responsible for cooperation with law enforcement with the resources necessary to enable them to comply with requests from law enforcement;
- Criminal compliance programmes
    - Service providers should be encouraged to organise their cooperation with law enforcement in the form of comprehensive criminal compliance programmes, and provide a description of such programmes to law enforcement, including:
    - The information necessary to contact the providers' designated criminal compliance personnel, as well as the hours during which such personnel are available
    - The information necessary for law enforcement to be able to provide documents to the criminal compliance personnel
    - Other particulars specific to the providers' criminal compliance personnel (such as the extent that a service provider operates in multiple countries, documents to be translated into a particular language etc.);
    - In order to allow law enforcement to make specific and appropriate requests, service providers should be encouraged to provide information on the type of services offered to users, including web links to the services and additional information as well as contact details for further information;
    - Where possible, the Internet service provider should be encouraged to provide a list, on request, of which types of data could be made available for each service to law enforcement on receipt of a valid disclosure request from law enforcement accepting that not all this data will be available for every criminal investigation;
- Verification of source of requests
    - Service providers should be encouraged to take steps to verify the authenticity of requests received from law enforcement to the extent possible and necessary to ensure that customer records are not disclosed to

unauthorized persons;

- Response
    - Service providers should be encouraged to respond to requests from law enforcement in writing (or other legally acceptable electronic method) and ensure that a documentary trail is available in relation to requests and responses accepting that this trail might not include any personal data;
- Standard response format
    - Taking into account the format for requests used by law enforcement, service providers should be encouraged to standardise the format for sending information to law enforcement;
    - Service providers should be encouraged to process requests in a timely manner, in line with the written procedures they have defined and provide guidelines to law enforcement on the average delays incurred to respond to requests;
    - Service providers should be encouraged to ensure that information transmitted to law enforcement is complete, accurate and protected;
    - Service providers should ensure the confidentiality of requests received;
- Explanation for information not provided
    - Service providers should be encouraged to provide explanations to the law enforcement authority sending a request if requests are rejected or information cannot be provided;
- Audit
    - Service providers should be encouraged to track and audit the system of processing requests for statistical purposes, for identifying strengths and weaknesses and publish such results if appropriate;
- Coordination among service providers
    - Being mindful of anti-trust/competition regulations service providers should be encouraged to coordinate their cooperation with law enforcement and share good practices among each other and make use of service provider associations for that purpose.