26 May 2015
Strasbourg, France

T-CY (2015)10
Provisional

Cybercrime Convention Committee (T-CY)

Criminal justice access to data in the cloud: challenges

Discussion paper

prepared by the T-CY Cloud Evidence Group

www.coe.int/TCY

Contents

Contact
Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY) Tel +33-3-9021-4506
Directorate General of Human Rights and Rule of Law Fax +33-3-9021-5650
Council of Europe, Strasbourg, France Email: alexander.seger@coe.int

1 Purpose of this report

The Cybercrime Convention Committee (T-CY), at its 12th plenary (2-3 December 2014), established a working group to explore solutions for access for criminal justice purposes to evidence in the cloud, including through mutual legal assistance ("Cloud Evidence Group").[1]

This decision was motivated by the recognition that in the light of the proliferation of cybercrime and other offences involving electronic evidence, and in the context of technological change and uncertainty regarding jurisdiction, additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence in specific criminal investigations.[2]

The Cloud Evidence Group is to submit a report to the T-CY with options and recommendations for further action by December 2016 (an interim report is to be submitted by December 2015). It is to base its work on:

- The recommendations of the T-CY assessment report on the mutual legal assistance provisions of the Budapest Convention on Cybercrime (document T-CY (2013)17rev).
- The work of the Ad-hoc Sub-group on transborder access to data and jurisdiction.
- A detailed description of the current situation and problems as well as emerging challenges regarding criminal justice access to data in the cloud and foreign jurisdiction.

The purpose of the present discussion paper is to facilitate an exchange of views on current and emerging challenges faced by criminal justice authorities and to seek the cooperation of industry and other stakeholders in identifying solutions. Such solutions may range from practical measures and documentation of good practices, to guidelines or a binding additional protocol to the Budapest Convention on Cybercrime.

The present report is not covering prevention and protective measures. It is understood that effective criminal justice and preventive measures at all levels are complementary.

Solutions will remain within the scope of Article 14 Budapest Convention[3], that is, cover specified data within specific criminal investigations. They will not pertain to bulk interception of data or other measures for national security purposes.

---

[1] Document T-CY(2014)16: Transborder Access to data and jurisdiction: Options for further action by the T-CY (report of the Transborder Group adopted by the 12th Plenary of the T-CY, December 2014).

[2] The need for solutions to allow for timely access to electronic evidence in view of protecting the rights of victims is also underlined by the European Union in http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf (February 2015). The EU Agenda on Security (April 2015) notes:
"*Cyber criminality requires competent judicial authorities to rethink the way they cooperate within their jurisdiction and applicable law to ensure swifter cross-border access to evidence and information, taking into account current and future technological developments such as cloud computing and Internet of Things. Gathering electronic evidence in real time from other jurisdictions on issues like owners of IP addresses or other e-evidence, and ensuring its admissibility in court, are key issues.*"
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
The T-CY in document T-CY(2014)16
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf stated:
"The Transborder Group believes that in the absence of an agreed upon international framework with safeguards, more and more countries will take unilateral action and extend law enforcement powers to remote transborder searches either formally or informally with unclear safeguards. Such unilateral or rogue assertions of jurisdiction will not be a satisfactory solution."

[3] Article 14 – Scope of procedural provisions

2 The threat of cybercrime and the question of electronic evidence

2.1 Cybercrime and e-evidence

Cybercrime[4] and the challenges related to electronic evidence[5] have reached a level and complexity that undermines the confidence, security and trust in information and communication technologies (ICT).

A review of the current scale, scope and challenges related to cybercrime and electronic evidence (that is, evidence in the form of data generated by or stored on a computer system) suggests that cybercrime has become a serious threat to the fundamental rights of individuals, to the rule of law in cyberspace and to democratic societies:

- The theft and misuse of personal data (email account data, credit card details, address books, patient records etc.) affects the right to private life (including the protection of personal data) of hundreds of millions of individuals.[6]
- Cybercrime is an attack against the dignity and integrity of individuals, in particular children.[7]
- Cyberattacks (such as distributed denial of service attacks, website defacement and others) against media, civil society organisations, individuals or public institutions are attacks against the freedom of expression.[8]
- Cybercrime is an attack against democracy. Governments, parliaments and other public institutions as well as critical infrastructure are faced with attacks every day.[9]
- Cybercrime is a threat to democratic stability. Information and communication technologies are misused for xenophobia and racism, contribute to radicalisation and serve terrorist purposes.[10]

---

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b other criminal offences committed by means of a computer system; and
c the collection of evidence in electronic form of a criminal offence.
…..

[4] Defined here as offences against and by means of computer data and systems in the sense of Articles 2 to 11 of the Budapest Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[5] The procedural law powers of the Budapest Convention related evidence in electronic form of any criminal offence (Article 14 Budapest Convention).

[6] http://www.handelsblatt.com/technik/vernetzt/russische-bande-erbeutet-nutzerdaten-was-tun-nach-dem-datendiebstahl/10297922.html
http://www.zdnet.com/pictures/2014-in-security-the-biggest-hacks-leaks-and-data-breaches/
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[7] See also the K.U. v Finland judgment of the European Court of Human Rights
http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"]}

[8] For example, in the days following the "Charlie Hebdo" tragedy on 7 January 2015, more than 20,000 websites in France were under attack http://www.lefigaro.fr/secteur/high-tech/2015/01/15/01007-20150115ARTFIG00333-la-france-face-a-une-vague-sans-precedent-de-cyberattaques.php
The Sony attacks of November/December 2014 is another recent example.
http://www.nbcnews.com/storyline/sony-hack/sony-hack-most-serious-cyberattack-yet-u-s-interests-clapper-n281456
http://www.bbc.com/news/entertainment-arts-30512032

[9] For example: http://www.welt.de/politik/deutschland/article136114277/Cyber-Angriff-auf-Kanzleramt-und-Bundestag.html

[10] http://www.liberation.fr/monde/2014/09/14/la-radicalisation-des-futurs-jihadistes-est-rapide-la-plupart-sont-des-convertis_1100395
http://130.154.3.8/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

- Cybercrime causes economic cost and risks to societies and undermines human development opportunities through ICT.[11]
- Cybercrime is a threat to international peace and stability. Military conflicts and political disagreements are increasingly accompanied by cyberattacks.[12]

Reportedly, trillions of security incidents are noted on networks each year[13] and millions of attacks against computer systems and data are recorded every day.[14] Cybercrime is a primary concern to governments, societies and individuals.[15]

In addition, criminal justice authorities are faced with the problem that evidence in relation to any crime is now often stored in electronic form on computer systems.[16] Most international requests for data are related to fraud and financial crime followed by violent and serious crimes. These may include murder, assault, smuggling of persons, trafficking in human beings, drug trafficking, money laundering, terrorism and the financing of terrorism, extortion and, in particular, child pornography and other forms of sexual exploitation and abuse of children.[17]

Predictions are that cybercrime will grow significantly in 2015 and beyond. Reasons include technical vulnerabilities which may affect hundreds of millions of users and the security of organisations. Examples exposed in 2014 are mobile malware threats,[18] defects such as Heartbleed[19], the hacking of the UMTS standard for mobile phone communications[20], the cloning of biometric data such as fingerprints[21] or irises[22] or concerns over the security of cloud services for the storage of data.[23] New forms of electronic payments, including mobile money, provide new opportunities for fraud and financial crime.

Big data and the Internet of Everything[24] create further risks to security and privacy under a business model of the Internet that relies increasingly on the exploitation of personal data. Data available are

[11] For links between cybercrime and human development see http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/cyber%20CB_v1y.pdf
While there is general agreement on the huge cost of cybercrime, actual cost and damages are difficult to determine. http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf
[12] For example: http://www.bbc.com/news/world-europe-30453069
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf
http://www.cbsnews.com/news/cyber-warfare-the-next-front-in-the-israel-gaza-conflict/
[13] http://www.symantec.com/deepsight-products/
[14] See for example http://www.sicherheitstacho.eu/?lang=en
[15] http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf
[16] For example: subscriber information or IP address related to a ransom mail in a kidnapping case, location data of a suspected murderer or drug trafficker, connection between different terrorist acts etc.
[17] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf
[18] See joint study of Kaspersky Lab and Interpol (October 2014) on mobile phone threats at: http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/10/report_mobile_cyberthreats_web.pdf
See also http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-vulnerabilities-under-attack.pdf
[19] http://blogs.mcafee.com/consumer/what-is-heartbleed
[20] http://www.sueddeutsche.de/digital/mobilfunkstandard-umts-ultimativer-abhoeralbtraum-1.2281898
http://www.sueddeutsche.de/digital/abhoeren-von-handys-so-laesst-sich-das-umts-netz-knacken-1.2273436-2
[21] http://www.bbc.com/news/technology-30623611
http://www.macrumors.com/2014/12/29/ccc-reproduce-fingerprints-public-photos/
[22] http://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html
[23] http://www.denverpost.com/breakingnews/ci_26452892/apple-says-some-celebrity-accounts-compromised
https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf
http://arxiv.org/pdf/1404.2697v1.pdf
[24] http://www.ft.com/cms/s/0/685fe610-9ba6-11e4-950f-00144feabdc0.html#axzz3QULEgVl1
http://drivingsalesnews.com/bmw-companies-want-our-driver-data/

not only used for business purposes, but may also be used for criminal purposes, such as harvesting data through "crime-as-a-service".[25]

If only a minuscule fraction of offences involving computer data and systems can be prosecuted, victims have a very limited expectation of justice. This raises questions regarding the rule of law in cyberspace.

2.2 Confusion between criminal justice versus national security

Public and political debates on mass surveillance are marked by a confusion between criminal justice and national security. Criminal justice authorities carry out specific criminal investigations and secure specified data for use in court cases and proceedings. Such investigations may interfere with the rights of individuals and they are therefore subject to rule of law safeguards,[26] such as judicial control. The evidence can be challenged and remedies are available. This is very different from bulk interception of data for national security purposes.

However, the confusion prevails. It leads to additional conditions for criminal justice authorities and prevents solutions in view of more effective investigations and prosecutions of cybercrime and other offences involving electronic evidence.[27]

As stated by the Deputy Secretary General of the Council of Europe in March 2015:

> "We need more effective criminal justice and we need stronger safeguards regarding national security measures. What we don't need is confusion between the two types of activities which will then prevent criminal justice solutions."[28]

2.3 Uncertainty regarding the availability of data

Reports on mass surveillance and the ruling of the European Court of Justice on the EU Data Retention Directive[29] has led to uncertainty regarding rules on procedural powers not only within the European Union but also elsewhere. In some countries, not only data retention provisions but also other powers to secure electronic evidence have been abolished or are in question. Delays in the adoption of European data protection frameworks at the level of the European Union and the Council of Europe create further uncertainty.

---

[25] http://gadgets.ndtv.com/internet/news/europes-police-need-data-law-changes-to-fight-cybercrime-europol-599960
http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf

[26] See Article 15 Budapest Convention. According to the European Court of Human Rights, in order to be allowed under the European Convention on Human Rights, the interference,

- must be prescribed by law and the law must meet the requirements of precision, clarity, accessibility and foreseeability;
- must pursue a legitimate aim;
- must be necessary, that is, it must respond to a pressing social need in a democratic society and thus be proportionate;
- must allow for effective remedies;
- must be subject to guarantees against abuse.

[27] See conclusions in http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf

[28] http://www.coe.int/en/web/deputy-secretary-general/-/increasing-co-operation-against-cyberterrorism-and-other

[29] http://curia.europa.eu/juris/document/document.jsf?text=Data%2BRetention&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=305870#ctx1

Moreover, cooperation by cloud service providers and other industry with criminal justice often depends on their own internal policies and they may change these unilaterally at any time.

2.4 Types of data needed for criminal justice purposes

For the purposes of a criminal investigation, three types of data may be needed:

- Subscriber information;
- Traffic data;
- Content data.

In many jurisdictions, conditions for access to subscriber information tend to be lower than for traffic data and the strictest regime applies to content data.

2.4.1 Subscriber information[30]

Subscriber information is essential to identify the user of a specific Internet Protocol (IP) address or, vice versa, the IP addresses used by a specific person. Identifying the subscriber of an IP address is the most often sought information in domestic and international criminal investigations related to cybercrime and electronic evidence. Without this information, it is often impossible to proceed with an investigation.[31]

The term "subscriber information" is defined in Article 18.3 Budapest Convention:

> 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider,[32] relating to subscribers of its services other than traffic or content data and by which can be established:
> a the type of communication service used, the technical provisions taken thereto and the period of service;
> b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
> c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

[30] See appendix for additional notes.
[31] The T-CY in December 2014 adopted a study on the "rules on obtaining subscriber information", pointed out that subscriber information is the most sought information in domestic and international investigations. The T-CY noted diverse rules for obtaining subscriber information whereby in some Parties subscriber information is treated in the same way as traffic data – in particular in relation to dynamic IP addresses – while in others requirements for obtaining subscriber information are lower. The T-CY thus recommended "greater harmonization between the Parties on the conditions, rules and procedures for obtaining subscriber information."
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)17_Report_Sub_Info_v7adopted.pdf
See page123 of http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf
[32] For the purposes of this paper, the term "service provider" is used in the meaning of Article 1.c Budapest Convention.

As a result of the assessment of the mutual legal assistance provisions, the T-CY recommended to consider a light regime for international requests for a limited set of subscriber information:[33]

> Recommendation 19: Parties should consider allowing – via legal domestic amendments and international agreement – for the expedited disclosure of the identity and physical address of the subscriber of a specific IP address or user account.

Subscriber information also comprises data from registrars on registrants of domains.[34]

Subscriber information is likely to be held by service providers "offering its services in the territory" of a Party although the information may actually be stored on servers in other jurisdictions.[35] It may thus not always be clear to whom to address a request for subscriber information. However, Article 18.1.b Budapest Convention offers a practical solution in that competent authorities of a Party should be able to request subscriber information from a service provider offering a service on its territory irrespective of where the information is actually stored:

> Article 18 – Production order
> 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
> a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
> b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

In Belgium, this power is reflected in Article 46bis (§2) of the Belgian Code of Criminal Procedure and is being tested in the "Belgian Yahoo! case".[36]

2.4.2 Traffic data

Log files that record activities of the operating system of a computer system or of other software or of communications between computers are essential for computer forensic and cybercrime investigations. This includes in particular "traffic data" as defined in Article 1.d Budapest Convention:

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

Traffic data may also help determine the physical location of computer systems and thus of users.

[33] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf
[34] For issues in this connection see the discussion on law enforcement recommendations to ICANN and on the question of WHO-IS accuracy. For an explanation of the domain registration process see http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter2.pdf
[35] For example, Google has also several data centres in Europe (http://www.google.com/about/datacenters/inside/locations/index.html), Microsoft has "more than 100 datacenters" including in Amsterdam and Dublin http://download.microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_Cloud_Infrastructure_Datacenter_and_Network_Fact_Sheet.pdf, and Facebook also has a datacentre in Sweden https://www.facebook.com/LuleaDataCenter
[36] http://www.stibbe.com/en/news/2014/july/benelux-ict-law-newsletter-49-court-of-appeal-of-antwerp-confirms-yahoo-obligation

Traffic data as well is likely to be held by service providers providing services in the territory of a Party although the data may actually be stored on servers in other jurisdictions.

Article 5 of European Union Directive 2006/24/EC[37] on data retention provided more details on the data considered necessary and combined subscriber information and traffic data (see appendix).

2.4.3 Content data

Furthermore content data is often needed in a criminal investigation. According to paragraph 209 of the Explanatory Report of the Budapest Convention:

> 'Content data' is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).

Content data – such as an email, images, movies, music, documents or other files – in a cloud context is held by service providers providing services on the territory of a Party although the information may actually be stored on servers in other jurisdictions.

A distinction should be made between "stored" content data, that is, data already available on a computer system and "future" content data that is not yet available and that needs to be gathered, for example, through the interception of a communication.

The interception of communications may be carried out upon a court order either by the police or by a specialised body directly, or with the assistance of a service provider. Its use is often restricted to serious crimes.

2.5 Cloud computing

An often quoted definition of "cloud computing" is the following:

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware.[38]

"Cloud computing" means that data is less held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions:

[37] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=EN.
The Directive was declared invalid by the European Court of Justice in 2014.
[38] http://www.nist.gov/itl/cloud/
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

In traditional computer forensics, due to the centralized nature of the information technology system, investigators can have full control over the forensic artefacts (router, process logs, hard disks). However, in the cloud eco system, due to the distributed nature of the information technology systems, control over the functional layers varies among cloud actors, depending on the service model. Therefore, investigators have reduced visibility and control over the forensic artefacts.[39]

3 Challenges for criminal justice

3.1 The scale and quantity of cybercrime, devices, users and victims

Cybercrime, the number of devices, services and users (including of mobile devices and services) and with these the number of victims have reached proportions so that only a minuscule share of cybercrime or other offences involving electronic evidence will ever be recorded and investigated. The vast majority of victims of cybercrime cannot expect that justice will be served. This raises questions regarding the rule of law in cyberspace and the ability of governments to meet their obligations to protect society against crime and to protect the rights of victims.[40]

3.2 Technical challenges

In addition to challenges related to cloud computing, criminal justice authorities are faced with a range of other challenges that render investigations highly complex:

- Peer-to-peer/Virtual Private Networks;
- Anonymizers (TOR, I2P);
- Encryption;[41]
- VOIP;[42]
- IPv4 to IPv6 transition and Carrier-grade Network Addressing Translators (CGN).[43]

These are major challenges and would need to be discussed in detail separately.

3.3 Cloud computing, territoriality and jurisdiction

Cloud computing raises a number of challenges for criminal justice, in particular with regard to the applicable law and the jurisdiction to enforce. Issues include:

- Independence of location is a key characteristic of cloud computing. Therefore:
  - It is often not obvious for criminal justice authorities in which jurisdiction the data is stored and/or which legal regime applies to data. A service provider may have its headquarters in one jurisdiction and apply the legal regime of a second jurisdiction while the data is stored in a third jurisdiction. Data may be mirrored in several or

[39] NIST cloud computing forensic science challenges (draft) June 2014 http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

[40] On the positive obligation to protect individuals see the K.U. v Finland judgment of the European Court of Human Rights http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"]}

[41] See Sarah Lowman (2010) at http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf

[42] See Muhammad Tayyab Ashraf, John N. Davies and Vic Grout (2011) at http://www.glyndwr.ac.uk/computing/research/pubs/SEIN_ADG.pdf

[43] See Appendix for additional notes.

move between jurisdictions. If the location of data determines the jurisdiction, it is conceivable that a cloud service provider systematically moves data to prevent criminal justice access.

- Even if theoretically data may always have a location also when stored on cloud servers,[44] it is far from clear which rules apply for lawful access by criminal justice authorities.[45] It may be argued that the location of the headquarters of the service provider, or of its subsidiary, or the location of the data and server, or the law of the State where the suspect has subscribed to a service, or the location or citizenship of the suspect may determine jurisdiction.
- It is often not clear whether a cloud provider is the "controller" or the "processor"[46] of the data of a user and thus which rules apply.
- Additional jurisdiction issues arise, for example, when the data owner is unknown or when the data is stored via transnational co-hosting solutions.

▪ A service provider may be under different layers of jurisdictions for various legal aspects related to its service at the same time. For example:

- For data protection purposes, within EU member States, jurisdiction[47] seems to be decided by the location of the data controller, not by the location of the international HQ, the location of the servers, the location of the business area (customers) or other criteria.[48] However, some companies do not have data controllers in the EU, even if

---

[44] https://www.eff.org/files/2014/12/15/computer_science_experts_microsoft_ireland_amicus_brief.pdf. However this *amicus brief* seems not to fully analyse the impact on jurisdiction rules when "secondary copies of data are saved to remote servers or data centers for disaster-recovery purposes" (p. 21), as it usually happens for business continuity reasons.

[45] See the pending Microsoft/Ireland case
http://www.lexology.com/library/detail.aspx?g=ce97dcac-949b-4004-9ae8-8ea716b1e6a5
http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/Government%27s%20Memorandum%20of%20Law%20in%20Opposition%20to%20Motion%20to%20Vacate%20%28doc%2097....pdf
http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/Government%27s%20Memorandum%20of%20Law%20in%20Opposition%20to%20Motion%20to%20Vacate%20%28doc%2097....pdf
https://s3.amazonaws.com/s3.documentcloud.org/documents/1149373/in-re-matter-of-warrant.pdf
https://www.eff.org/files/2014/12/12/microsoft_opening_brief.pdf
http://digitalconstitution.com/wp-content/uploads/2014/12/Ireland-Amicus-Brief.pdf

[46] See art. 2 EU Directive 95/46: "Definitions. For the purposes of this Directive:
[…]
(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;"

[47] See art. 4 EU Directive 95/46: "National law applicable.
1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself".

[48] One example: Facebook has a data controller office in Ireland, and is considered to be under jurisdiction of the Irish data protection agency. However, their international HQ is in the USA, and the company has a large

they have a number of European users. In these cases, it appears unclear what if any jurisdiction European data protection agencies have over these services.[49] The "right to be forgotten" case regarding Google in Spain on the other hand was based on different criteria for jurisdiction than the location of international HQ, the location of servers or the location of data controllers.[50]

- For tax purposes, jurisdiction seems not decided by the location of the international HQ, servers or data controllers, but on several other criteria, such as the location of the subsidiary doing business.[51]
- With regard to consumer protection, the location of the consumer seems decisive.[52]
- For intellectual property rights in civil cases the location of the business seems to determine jurisdiction,[53] while for intellectual property in criminal law the location of the perpetrator may be decisive.[54]

---

server farm in Sweden for their European business. At the same time, in a criminal case, police or prosecutors in Europe need to send a request for mutual legal assistance to the US when they seek content data. They cannot file a request to the Irish office of Facebook, referring to Irish law, or to the Swedish Facebook server farm office, referring to Swedish law.
However, see also the following situation involving the Netherlands Data Protection Agency and Facebook which illustrates the multiple models of jurisdiction applied or claimed.
https://www.cbpweb.nl/en/news/facebook-provides-information-after-formal-demand-dutch-dpa

[49] Some examples: VK.com (HQ: Russia), Baidu (HQ: China), Snapchat (HQ: United States) and Hushmail (HQ: Canada). All these companies handle and process personal data. VK and Snapchat offer localized services for several European markets.

[50] See European Court of Justice in Google Spain versus Costeja and in particular the question of the territorial application of EU Directive 95/46
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN:
"Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State".

[51] See the judgement regarding GOOGLE IRELAND LTD et GOOGLE France and fiscal administration
»Le juge des libertés et de la détention a autorisé des agents de l'administration fiscale à procéder à des visites et saisies, sur le fondement de l'article L. 16 B du livre des procédures fiscales, dans des locaux susceptibles d'être occupés par les sociétés Google France et (ou) Google Ireland Limited, en vue de rechercher la preuve de la fraude de cette dernière. Google souhaite faire annuler la procédure. Google estime que les documents saisis, car saisis à partir de l'interconnexion entre les machines se trouvant dans les locaux en France et à l'étranger, qu'il s'agit d'une saisine extra territoriale et de ce fait non valable. Le Juge estime toutefois que les données saisies sont supposées être situées à l'adresse où est localisé l'ordinateur alors même que les données sont situées sur un serveur étranger. »
http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028209493&fastReqId=2089348476&fastPos=2

[52] In 2006, the Nordic Consumer Protection Agencies complained to Apple iTunes, an American company with a subsidiary in Luxembourg, regarding the practice of selling services to Nordic consumers, without using Nordic consumer protection laws. One point of content, was the use of DRM. The consumer protection agencies claimed that this was unfair to consumers. In the general terms, Apple iTunes referred to Luxembourg laws and Luxembourg as the venue for any legal complaints. The Nordic Consumer Protection Agencies argued that this was in violation of local laws regarding distance sales. The iTunes services were localised for the various Nordic markets, as regards language, contents and currency for payment. Eventually, Apple iTunes changed their policies (2009). In the end, jurisdiction was decided by the location of the consumer/end user.
http://www.twobirds.com/en/news/articles/2006/itunes-terms-service-scrutiny-nordic-consumer-ombudsmen

[53] Google decided in 2014 to shut down their Spanish Google News service, based on complaints from Spanish news publishers. They claimed that Google News violated their intellectual property, and that Google should pay for creating and running a service based on their information. The arguments claiming Spanish jurisdiction were quite similar to the jurisdiction arguments in the "right to be forgotten" case, basically that Google was running a business in Spain.
http://www.wsj.com/articles/google-shuts-spanish-news-service-ahead-of-new-law-1418728149

[54] The Swedish "Pirate Bay" case is one of several examples. Like in many other criminal cases, the location of the perpetrator was the deciding factor. If the arguments from the Google Spain-case had been usable in a criminal case, the Pirate Bay company and managers could have been prosecuted in any jurisdiction where they were running a business. Like Google News, part of the income to Pirate Bay was advertising.
http://www.theguardian.com/technology/2009/apr/17/the-pirate-bay-trial-guilty-verdict
http://en.wikipedia.org/wiki/The_Pirate_Bay_trial

- The sharing and pooling of resources is a key characteristic of cloud computing. Cloud services may entail a combination of service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)). It is often unclear which service provider when providing one or more types of services is in possession or control of which type of data (subscriber information, traffic data, content data) so as to be served a production order.

- It is often unclear whether data is stored or in transit and thus whether production orders, search and seizure orders, interception or real-time collection orders are to be served.

- It is not always clear whether different types of cloud services are considered and regulated as "electronic communication services"[55] or "information society services". This has implications on the type of and conditions for procedural law powers that can be applied.[56]

- Regarding interceptions, specific problems arise. For example:

  - A court order served to a service provider domestically to intercept an electronic communication between two suspects on its territory and/or its nationals, is often not executable in real time because the server where the interception is to take place is located in a foreign jurisdiction or the communication is routed via a foreign jurisdiction. The foreign authorities are unlikely to respond to an MLA request in real time, given the duration of procedures and the requirements for interception in that country, unless emergency procedures are in place.
  - A court order may be served for the interception of a communication of a national suspect. However, the suspect moves to another country or moves between different

[55] See Court of Appeal in Antwerp, 12th chamber, 2012/CO/1054, 20 November 2013 (Belgian Yahoo! case):
"The defendant keeps arguing, in vain, that she does not offer services that partially or mainly consist of transmitting signals via electronic communication networks. The defendant offers in Belgium, amongst other things, a (web)mail service which enables someone that registers electronically to communicate via the Internet using an IP-address from an internet access provider and the defendant provides the transmission of this electronic communication (see further). This differs from the actual operations of internet access providers (such as Telenet, Belgacom), which only provide access to the Internet using an IP-address. The IP-address granted is, however, only known by the internet service provider (such as Yahoo!). The defendant has consciously chosen for commercial purposes as was, rightly found by the first judge: if the defendant does not want to be subjected to the obligations in Article 46bis §2 of the Code of Criminal Procedure the defendant is free to exclude the IP-range in Belgium (see number in margin 4.3 of the opposed judgment).
The Public Prosecution shows, using documents 2 and 9, and there is no reason to doubt the credibility and objectivity of these documents, that sending an email from sender to receiver occurs mainly if not only via the mail servers of the defendant and that in case that an email is sent from one Yahoo! account to another Yahoo! account no other services are even used, which proves that the defendant mainly or even is the only provider of her mail service for transmitting signals via electronic communication networks. These conclusions are not disputed by the defendant's expert, Jonas Mariën or by the dissenting arguments of the defendant.
In contract to the statements of the defendant's conclusion on p. 6, the defendant was clearly able to defend herself against the argument of the Public Prosecution (amongst other things, by consulting her own expert), so there is no violation of the defendant's rights (Art. 6 ECHR).
The fact that the defendant offers her webmail services in Belgium is reinforced because she sends advertisement messages, taking into account the location and language. Also, www.yahoo.be seems to offer the same services as www.yahoo.com did in the past.
The facts have, thus, been proven".

[56] While the Budapest Convention does not make this distinction and considers all to be "service providers" (see Article 1.c, the Electronic Commerce Directive 2000/31/EC covers "information society services" whereas the Communications Privacy Directive and the (now invalid) Data Retention Directive cover "electronic communication services". For example, webmail services are not necessarily considered electronic communication services and thus did not fall under the Data Retention Directive.
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=en
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

countries. It may be unclear whether the interception is legally possible when the suspect is in roaming.[57]

- The non-localised nature of cloud computing causes problems for live forensics (online forensics) and searches because of the architecture of the cloud (multi tenancy, distribution and segregation of data) as well as legal challenges related to the integrity and validity of the data collection, evidence control, ownership of the data or jurisdiction. [58]

3.4 Mutual legal assistance

Mutual legal assistance remains the principal means to obtain evidence from foreign jurisdictions for use in criminal proceedings. In December 2014, the Cybercrime Convention Committee (T-CY) completed an assessment of the functioning of mutual legal assistance provisions. [59] It concluded, among other things, that:

> The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.

The Committee adopted a set of recommendations to make the process more efficient. These recommendations should be implemented.

At the same time, MLA is not always a realistic solution to access evidence in the cloud context for the reasons indicated above.

[57] See Article 20 of the EU Convention on Mutual Legal Assistance in Criminal Matters which provides for a post factum notification and validation.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF
[58] NIST cloud computing forensic science challenges (draft) June 2014
http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf
[59] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

4 Questions

The present discussion paper points at the complex challenges that criminal justice authorities are confronted with when seeking access to electronic evidence in a cloud context.

A number of issues need to be clarified and additional solutions may need to be agreed upon if criminal justice authorities are expected to protect society and individuals as well as their rights against crime.

Discussion of the following questions may help advance matters:

4.1 Jurisdiction

1. Which government would be the addressee of a lawful request for data by a country attacked in a cloud context where the territorial origin of a cyber offence is not clear, the controller of data is hidden behind layers of service providers, or data is moving, fragmented or mirrored in multiple jurisdictions?

2. What governs jurisdiction to enforce for criminal justice purposes: Location of data? Nationality of owner of data? Location of owner of data? Nationality of data owner? Location of data controller? Headquarters of a cloud service provider? Subsidiary of a cloud service provider? Territory where a cloud provider is offering its services? Laws of the territory where the data owner has subscribed to a service? Territory of the criminal justice authority?

3. What does it mean "offering its services in a territory" (see Article 18.1.b Budapest Convention)[60]?

4. If a domestic court order authorizes the interception of a communication between two nationals or persons on its territory, why would MLA be required even if technically the provider would carry out the interception on a server on a foreign country? To what extent would the sovereignty of that foreign country be affected? To what extent would the rights of the defendants not be protected? Similar for production orders regarding content data?

4.2 Mutual legal assistance

5. Is it realistic that the number of MLA requests sent, received and processed can be increased by a factor of hundred or thousand or ten thousand? Are governments able to dramatically increase the resources available for the efficient processing of mutual legal assistance requests not only at the level of competent central authorities but also at the level of local courts, prosecution and police offices where MLA requests are prepared and executed?

[60] Article 18 – Production order
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

6. What would be a reasonable timeframe to obtain data from a foreign authority? Could this be defined in a binding agreement?

7. Is it conceivable to develop a light regime for subscriber information, e.g. expedited disclosure?

8. What additional international legally binding solutions could be considered to allow for efficient criminal justice access to specified data in foreign or unknown jurisdictions within the framework of specific criminal investigations?[61] For example:

   - Rec 19 Parties should consider allowing – via legal domestic amendments and international agreement – for the expedited disclosure of the identity and physical address of the subscriber of a specific IP address or user account.

   - Rec 20 Interested Parties may consider the possibility and scope of an international production order to be directly sent by the authorities of a Party to the law enforcement authorities of another Party.

   - Rec 21 Parties should consider enhancing direct cooperation between judicial authorities in mutual legal assistance requests.

   - Rec 22 Parties may consider addressing the practice of law enforcement and prosecution services obtaining information directly from foreign service providers, and related safeguards and conditions.

   - Rec 23 Parties should consider joint investigations and/or the establishment of joint investigation teams between Parties.

   - Rec 24 Parties should consider allowing for requests to be sent in English language. Parties should in particular allow for preservation requests to be sent in English.

   - Solutions already available or principles already agreed upon in other international instruments.[62]

These questions are in particular to guide discussions at the Octopus Conference on Cooperation against Cybercrime from 17 to 19 June 2015 (www.coe.int/octopus2015).

---

[61] See, for example, Recommendations 19 to 24 on page 127 of http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[62] For example in the:
2nd Additional Protocol on Mutual Legal Assistance in Criminal Matters (ETS 182) of the Council of Europe http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=182&CM=8&DF=&CL=ENG
Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF
European Investigation Order in Criminal Matters of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN

5 Appendix

5.1 Cloud Evidence Group: Terms of Reference

Name	Working group on criminal justice access to evidence stored in the cloud, including through mutual legal assistance ("Cloud evidence group")
Origin	T-CY Working Group under Article 1.1.j of the Rules of Procedure[63] established by decision of the T-CY adopted at the 12th Plenary (2-3 December 2014)
Duration	1 January 2015 – 31 December 2016
Main tasks	To explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance. The Working Group shall prepare a report for consideration by the T-CY taking into account: ▪ The recommendations of the T-CY assessment report on the mutual legal assistance provisions of the Budapest Convention on Cybercrime (document T-CY(2013)17rev). ▪ The work of the Ad-hoc Sub-group on transborder access to data and jurisdiction. ▪ A detailed description of the current situation and problems as well as emerging challenges regarding criminal justice access to data in the cloud and foreign jurisdiction. The report shall contain draft options and recommendations for further action by the T-CY.
Benchmarks and deliverables	▪ June 2015: Discussion paper with description of current and emerging challenges as basis for an exchange of views with service providers and other stakeholders at Octopus Conference 2015. ▪ June 2015: Workshop at Octopus Conference. ▪ December 2015: Interim report for consideration by the T-CY. ▪ June 2016: Draft report for consideration by the T-CY. ▪ December 2016: Final report for consideration by the T-CY.
Working methods	The Working Group shall hold its meetings back-to-back with meetings of the T-CY Bureau and in camera. The Working Group may hold public hearings, publish interim results and consult other stakeholders.
Composition	• Bureau members participate ex-officio with defrayal of cost[64] • Up to 5 additional members with defrayal of cost[65] • Additional T-CY members (State Parties) at their own cost.

[63] http://www.coe.int/t/dqhl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2925%20rules_v15.pdf
[64] Subject to the availability of funds.
[65] Subject to the availability of funds.

5.2 Notes on "subscriber information"

Subscriber information is essential to identify the user of a specific Internet Protocol (IP) address or, vice versa, the IP addresses used by a specific person.

> Identifying the subscriber of an IP address is the most often sought information in domestic and international criminal investigations related to cybercrime and electronic evidence and it is, most of the time, crucial to ascertain the truth. Without this preliminary information, it is often impossible to proceed with an investigation.[66]

The term "subscriber information" is defined in Article 18.3 Budapest Convention:

> 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
> a the type of communication service used, the technical provisions taken thereto and the period of service;
> b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
> c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Paragraph 178 of the Explanatory Report to the Budapest Convention explains that subscriber information may be needed within a criminal investigation "primarily in two specific situations":

> – First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile), type of other associated services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address).
> – Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned.

Paragraph 178 goes on stating that:

> Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes.

Paragraph 180 of the Explanatory Report clarifies the range of data to be considered as subscriber information:

> Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone, and other

[66] http://www.coe.int/t/dqhl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)17_Report_Sub_Info_v7adopted.pdf
See page123 of http://www.coe.int/t/dqhl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

> access number, and billing and payment information, which is available on the basis of the agreement or arrangement between the subscriber and the service provider.

The T-CY in December 2014 adopted a study on the "rules on obtaining subscriber information", pointed out that subscriber information is the most sought information in domestic and international investigations.[67] The T-CY noted diverse rules for obtaining subscriber information whereby in some Parties subscriber information is treated in the same way as traffic data – in particular in relation to dynamic IP addresses – while in others requirements for obtaining subscriber information are lower.

The T-CY thus recommended "greater harmonization between the Parties on the conditions, rules and procedures for obtaining subscriber information."

As a result of the assessment of the mutual legal assistance provisions, the T-CY recommended to consider a light regime for international requests for a limited set of subscriber information:[68]

> Recommendation 19: Parties should consider allowing – via legal domestic amendments and international agreement – for the expedited disclosure of the identity and physical address of the subscriber of a specific IP address or user account.

Subscriber information is held by service providers providing services on the territory of a Party although the information may actually be stored on servers in other jurisdictions.[69] It may thus not always be clear to whom to address a request for subscriber information. However, Article 18.1.b Budapest Convention offers a practical solution in that competent authorities of a Party should be able to request subscriber information from a service provider offering a service on its territory irrespective of where the information is actually stored:

> Article 18 – Production order
> 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
> a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
> b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

In Belgium this power is reflected in Article 46bis (§2) of the Belgian Code of Criminal Procedure and is being tested in the Belgian Yahoo! case.

[67] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)17_Report_Sub_Info_v7adopted.pdf
See page123 of http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf
[68] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf
[69] For example, Google has also several data centres in Europe (http://www.google.com/about/datacenters/inside/locations/index.html), Microsoft has "more than 100 datacenters" including in Amsterdam and Dublin http://download.microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_Cloud_Infrastructure_Datacenter_and_Network_Fact_Sheet.pdf, and Facebook also has a datacentre in Sweden https://www.facebook.com/LuleaDataCenter

5.3 Categories of data to be retained (Article 5 of EU Directive 2006/24/EC[70]

Article 5 Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

[70] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=EN.
The Directive was declared invalid by the European Court of Justice in 2014.

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;
(iv) the IMSI of the called party;
(v) the IMEI of the called party;
(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:
(i) the calling telephone number for dial-up access;
(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:
(1) the location label (Cell ID) at the start of the communication;
(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

5.4 IPv4 to IPv6 transition and Carrier-grade Network Addressing Translators (CGN) [71]

Internet Service Providers keep logs of IP addresses assigned to a connected device. IP addresses, in principle, allow the identification of a connected device in a network. Such a traceback to a device and through the device to a user is essential in a criminal investigation.

Given the limited number of available addresses under Internet Protocol Version 4 (IPv4), for many years now, ISPs often do not allocate a stable (static) IP address to a specific device of an end-customer, but a range of IP addresses is assigned to an edge-network where IP addresses are then dynamically assigned to devices as they log on to the edge-network. This dynamic allocation of IP addresses is made possible through Network Address Translators (edge-NATs). In order to identify the device and thus the customer, not only the IP address but also "time stamps" are needed to determine which device used an IP address at a given moment in time.

The spread of mobile devices capable of accessing the Internet accelerated the exhaustion of IPv4 addresses. Over time, this problem is to be solved through Internet Protocol Version 6 (IPv6). The transition from IPv4 to IPv6 is taking longer than anticipated and it is unclear how long this transition will last. In the absence of backward compatibility, hosts need to operate both protocols in parallel during this transition period. ISPs overcome the shortage of IPv4 addresses by generalizing NATs.

These "Carrier-grade NATs" (CGN) complicate the traceback to identify the connected device. IP addresses and time stamps are not sufficient and only allow to determine the ISP. Additional information, including in particular the source and destination port addresses, would be required. Logs generated by CGN are very large and difficult to keep by ISPs. It would seem that under current data retention regulations ports are not covered.

The matter is further complicated in that providers use different solutions during the IPv4 to IPv6 transition period while operating both protocols in parallel (dual stack transition).

In short, identifying a device and a user through that device is highly complex in a CGN environment.

[71] See Geoff Huston (2013) at https://labs.apnic.net/?p=433