Our vision:
A world where every person's right to a fair trial is respected.

Policy Brief:

The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters

October 2018

Fair Trials

About Fair Trials

Fair Trials is a global criminal justice watchdog with offices in London, Brussels and Washington, D.C., focused on improving the right to a fair trial in accordance with international standards.

Fair Trials' work is premised on the belief that fair trials are one of the cornerstones of a just society: they prevent lives from being ruined by miscarriages of justice and make societies safer by contributing to transparent and reliable justice systems that maintain public trust. Although universally recognised in principle, in practice the basic human right to a fair trial is being routinely abused. Effective and efficient cross-border cooperation is necessary for a safer world. Technological advances have made it easier than ever to transfer information between countries. However, the rights of individuals can be overlooked at the expense of speed and efficiency.

Its work combines: (a) helping suspects to understand and exercise their rights; (b) building an engaged and informed network of fair trial defenders (including NGOs, lawyers and academics); and (c) fighting the underlying causes of unfair trials through research, litigation, political advocacy and campaigns.

In Europe, we coordinate the Legal Experts Advisory Panel- the leading criminal justice network in Europe consisting of over 180 criminal defence law firms, academic institutions and civil society organizations. More information about this network and its work on the right to a fair trial in Europe can be found at: https://www.fairtrials.org/legal-experts-advisory-panel.

Website: www.fairtrials.org
Twitter: @fairtrials

Contacts:

Rebecca Shaeffer
Senior Lawyer (Americas)
+1 (202) 790 2146
rebecca.shaeffer@fairtrials.net

Laure Baudrihaye-Gérard
Senior Lawyer (Europe)
+32 (0)2 894 99 55
laure.baudrihaye@fairtrials.net

This brief has been prepared in the context of the JUD-IT (Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network and academic partners, nor can they be taken to reflect the views of the European

Contents

List of abbreviations

CJEU	Court of Justice of the European Union
CLOUD Act	Clarifying Lawful Use of Overseas Data Act
DOJ	US Department of Justice
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EIO	European Investigation Order
EU Charter	European Union Charter of Fundamental Rights
ICCPR	International Covenant on Civil and Political Rights
LEAs	Law enforcement authorities
MLA	Mutual legal assistance
MLAT	Mutual legal assistance treaty
OIA	Office of International Affairs, DOJ
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Executive Summary

Evidence has always been at the heart of criminal justice systems, forming the building blocks of the criminal case, crucial to establishing the guilt (or innocence) of people accused of committing criminal offences. In an increasingly digitalised world, electronic data, such as the contents of communications exchanged on social media or personal information about the subscriber of an email account, may contain critical information that could be used to incriminate or exculpate a person investigated in relation to a criminal offence.

Where the electronic data is stored or held by a company in a country other than where the criminal investigation is taking place, law enforcement authorities (police, prosecutors, investigating judges) can turn to a range of tools to get hold of the data. There are formal cross-border judicial cooperation mechanisms in evidence gathering – including mutual legal assistance treaties between the EU or its Member States and third countries, as well as multilateral international agreements. There are also EU instruments for cooperation between EU Member States. Moreover, prosecuting and judicial authorities may seek to obtain electronic data directly from the private companies that hold it, or even without the help of any intermediary at all by using a suspect's phone, for instance, to access data held in the cloud (known as "direct access") through a power under national law or even outside any formal legal framework.

The aim of this paper is to analyse the impact of the current mechanisms for the cross-border access to electronic data on the fairness of criminal proceedings.

The accused's perspective – electronic data and the right to a fair trial

Criminal prosecutions and convictions have severe implications on the accused: resulting in long-lasting stigma, loss of employment prospects, family relationships, and civil liberties in addition to the potential for loss of liberty and the imposition of severe penalties. This is one of harshest measures a state can take against a person and, for this to be a legitimate use of state power, international and European law require key principles of fairness to be respected. In criminal trials, where the prosecution has all the machinery of the state behind it, the principle of equality of arms is an essential guarantee of an accused's right to defend themselves. It ensures the accused has a genuine opportunity to prepare and present their case, and to contest the arguments and evidence put before the court, on a footing equal to that of the prosecution. These principles are designed to ensure a fair outcome (to limit the risk of people being wrongly convicted) and to ensure a fair process (in which the accused person is able to participate effectively).

These key fair trial principles apply in the digital world in the same way as they do in the physical world. Yet the creation of the mechanisms for the cross-border exchange of electronic data has been driven by the needs of law enforcement authorities and these tools are fundamentally one-sided:

- The wide implications of lack of notification to the suspect: the right to keep requests for data confidential is recognised in cross-border cooperation mechanisms but there is a concern that "gag orders" are excessively used as a matter of course, rather than exceptionally when strictly required. This is an acute concern due to the sometimes transient nature of electronic data and the fact that the accused may not learn about the obtaining of the electronic data until shortly before the trial. Moreover, electronic data may be obtained illegally and may ultimately not be formally admissible in court proceedings. With prior notification, this legality could be challenged before the harm is done, but leaving these arguments to the trial (or shortly before it) may not provide a satisfactory remedy.
- The lack of access to evidence-gathering tools for the defence: in practice, it is extremely difficult, if not impossible, for the defence to use the cross-border evidence gathering mechanisms to gather evidence abroad. As such, the cross-border data exchange mechanisms

require a high level of trust in the objectivity of law enforcement authorities to gather both incriminatory and exculpatory information.

- Capacity of the defence to obtain early access to the case file, understand and manage electronic data: in practice, in many EU Member States, the investigating authorities do not disclose the case file until after the investigation is complete and sometimes only shortly before trial. Yet where electronic data has been obtained, the quantity available on the file may make it impossible for the defence to assess in an effective manner. Without specialist training, a defence lawyer may not be aware of the significance of the electronic data provided and may not know what kind of exculpatory electronic data might exist or where it is located. Reviewing electronic data is a time-consuming and onerous task, especially where the defence has limited resources and when a client is in detention and cannot assist with the review of the data, creating a risk that potentially relevant data is overlooked.

Electronic data and the rule of law

The fairness of criminal justice systems is defined in human rights law primarily by reference to fairness for the accused; however, it has broader ramifications. A fair criminal justice system is a core building block of the rule of law, ensuring the fair and proportionate exercise of state power; it helps build public trust in the justice system; and can contribute to respect for (or violation of) a range of other human rights. States have legitimate reasons to give law enforcement authorities legal powers to investigate and prosecute crimes, but this does not mean they have a blank cheque to do whatever they like. Assessing whether law enforcement authorities have acted within their legal powers is a key element of a fair criminal justice process.

The report flags key concerns with respect to the checks on the legality of the actions of law enforcement authorities in the existing mechanisms:

- Difficulties in holding law enforcement authorities to account for unlawful or disproportionate uses of cross-border evidence gathering tools: the fact that electronic data requests will frequently be secret (often for legitimate reasons) makes legal challenges by the suspect difficult in respect of the lawfulness or proportionality of the request before the evidence is obtained and shared.
- Ineffective remedies: the existing legal mechanisms do not prescribe the remedies that are required where electronic data has been gathered illegally, instead leaving these as a matter of national law. The diversity of rules on the admissibility of evidence across states challenges the fundamental key check on the legality of evidence-gathering by law enforcement authorities at trial.
- Lack of protections against the risk of politically-motivated prosecutions and human rights abuses: there is no doubt that some states abuse criminal procedure to pursue politically-motivated prosecutions. This runs contrary to the rule of law, which is based on the concept that the law is applied equally and impartially. High-profile cases have shown how cross-border cooperation by law enforcement authorities has been misused for political purposes. Yet the existing mechanisms for the gathering of cross-border evidence exchange do not contain adequate safeguards to prevent this risk. Specifically, there is very limited public information about the use of the cross-border evidence gathering mechanisms, which is necessary to inform public debates about the appropriateness of their actions.

Recommendations

To mitigate the key risks for the fairness of the criminal justice system inherent in the cross-border gathering and exchange of evidence, we recommend the following reforms to law and practice:

- A presumption of prior notification of people whose personal data is being gathered (rebuttable only where clear justifications are provided) and, where this is not possible, prompt ex-post

notification. This mitigates the risks that the defence cannot challenge the legality of cross-border evidence gathering and that the accused does not have the time and information to prepare the defence.

- Electronic data of relevance to the accused should be included in evidence gathering requests (or preservation) by law enforcement authorities in order to avoid the loss or destruction of exculpatory electronic data due to delays.
- Electronic data should be promptly disclosed to the defence with sufficient time for the defence to process electronic data and request exculpatory materials. These measures would mitigate the risk of the accused not having enough time and information to prepare the defence as well as exculpatory electronic data being lost or deleted due to delays. Also, it would avoid that vast quantities of electronic data are dumped on the defence shortly before trial.
- The defence should be granted clear rights to use cross-border evidence gathering powers on equal terms with prosecutors so as to have sufficient time and facilities to prepare the defence.
- A right for the defence to challenge the admissibility and probity of electronic data should be included to keep law enforcement authorities from undermining the fairness of the trial and the rule of law.
- The ability for the defence to appoint lawyers in the prosecuting country and the country which is the source of electronic data would enable the defence to assess whether electronic data was gathered lawfully and how exculpatory evidence can be obtained.
- Funding should be made available to the defence to acquire the tools needed to process electronic data, specialist training for defence lawyers and mechanisms to enable lawyers to access technical expertise in order to understand and process large quantities of electronic data required to prepare a defence.
- Introducing protections in law and practice against electronic data including legally privileged materials would be important to safeguard the right of the accused to confidential communications with their lawyer.
- Judicial authorisation should be obtained before requests or orders for electronic data are issued to prevent abusive requests for electronic data.
- Greater clarity on the appropriate legal remedies is needed where electronic data has been obtained illegally in order to deter law enforcement authorities from making inappropriate use of cross-border evidence gathering tools.
- Law enforcement authorities, the European Commission and service providers should publish data regularly on the use of cross-border evidence gathering tools to allow for a better understanding of how mechanisms are being used in practice, and enable the identification of misuse and to ensure accountability.
- A requirement for an appropriate evidential test to be passed before cross-border evidence gathering tools can be used and for requests for electronic data to be limited in scope to avoid that cross-border evidence gathering tools are used disproportionately, undermining the right to privacy.
- In order to maintain trust in service providers and in cross-border evidence gathering mechanisms, meaningful powers should be granted for those receiving electronic data requests (whether law enforcement authorities or service providers) to refuse to comply where the requests are disproportionate, politically-motivated or would violate human rights.
- A requirement for requests for electronic data to contain sufficient information should be introduced to enable those receiving them to decide whether it is appropriate to comply, putting them in a position to assess the legality and proportionality of the request and to avoid violations of the accused's human rights.

Background

A) Electronic evidence and criminal justice

1. Evidence has always been at the heart of criminal justice systems, forming the building blocks of the criminal case, crucial to establishing the guilt (or innocence) of people accused of committing criminal offences. Law enforcement authorities (police, prosecutors, investigating judges) ("**LEAs**") cannot use the criminal justice system to combat crime without evidence.

2. In a globalised world (with people travelling, working and communicating across borders) obtaining evidence to investigate a crime and to build a criminal case is no longer a domestic matter. For example, prosecuting a drug smuggler is likely to require evidence from the countries of both import and export. Even in a case that may appear purely domestic – such as a murder – LEAs may need to obtain evidence of intent contained in electronic correspondence between the suspect and another person, which is held in another country. The only extraneous element in a case may be the fact that the correspondence is stored in another country.

3. LEAs need to be able to obtain evidence from other jurisdictions quickly and with minimum fuss. In principle, this may sound simple; in practice, it raises complicated questions from a legal and practical perspective. Is there a legal power to share personal information with an LEA in another country? Which country's laws apply to the gathering and sharing of this evidence? Is evidence obtained in one country admissible in the courts of another? How does an LEA in one country communicate the need for evidence to another country where, for example, another language is used?

4. Alongside the increasingly globalised nature of crime and of evidence, the use of cloud computing, social media and messaging and data exchange apps continues to rise. This means that electronically stored data is increasingly likely to be sought by LEAs and used as evidence in criminal proceedings. According to the European Commission (the "**Commission**"), electronic evidence in some form is relevant in around 85% of total criminal investigations:[1]

   > *An increasing number of criminal investigations … rely on electronic evidence that is not publicly available, e.g. information on the holder of an email account, messages exchanged via Facebook messenger or information on the timing of WhatsApp calls.*[2]

   The electronic nature of such evidence (and the organisations that "hold" it) adds further complexity to the ability of LEAs to obtain the data they need across borders. Can a private company be compelled to share data with an LEA? Where is data stored in an era of cloud-based computing? Which country's laws apply to that data and to the companies (often multi-nationals) that hold it? Crucially, what legal processes must be followed such that electronic data may be used as evidence in criminal proceedings?

5. Electronic data can take various forms. Definitions are complex and constantly changing. In its proposal of 17 April 2018 to create the European Production Order and European Preservation

[1] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 14 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

[2] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 5 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

Order (the **"E-evidence Proposal"**), the Commission suggests distinguishing between four categories of data:[3]

- Subscriber data: details relating to the user of a service and the nature of the service – such as evidence that a person is the user of a particular email or social media account;
- Access data: details about when a person uses a service – such as information on when a person has been accessing a particular website;
- Transactional data: information about the provision and use of a service - such as data on the device used for access and its location; and
- Content data: any stored data in a digital format – such as the content of videos, text messages, emails or other documents.

6. Such electronic data may become evidence in criminal proceedings. The concept of "evidence" has been defined elsewhere in EU law, as "all types of means of proof admissible before the national court seized, in particular documents and all other objects containing information, irrespective of the medium on which the information is stored".[4] In criminal matters, electronic data will equally become "evidence" once it is deemed admissible by the court seized with the proceedings. The admission of electronic data as evidence remains, in the absence of common EU standards, a matter of national law.

B) Overview of judicial cooperation mechanisms for gathering cross border data

7. There are a range of mechanisms for LEAs to obtain data across borders. An exhaustive overview of these is beyond the scope of this paper but the following summary provides an outline of the main mechanisms currently in use. These fall into three broad categories: formal cooperation mechanisms between LEAs; direct cooperation between a public authority and service provider; and direct access to electronic evidence by a public authority.

Formal LEA cooperation

8. Mutual legal assistance ("**MLA**") involves the emission of formal requests for evidence (including but not limited to electronic data) by one LEA to the appropriate public authority of the country where the evidence is located. The requesting LEA issues a formal request to the other country by means of an international Letter of Request or *Commission Rogatoire*.[5] LEAs in the receiving state then use domestic legal powers to obtain evidence and share it with the requesting country. These regimes typically allow states receiving requests to refuse them, in line with national law (discussed in the following chapters). Often those sending and ultimately processing requests are judicial authorities, but it is common for receiving states to create central authorities to receive

[3] Article 2 of the 'E-evidence Proposal', Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, 17 October 2018, 12113/1/18/REV 1.

[4] Article 2(13), Directive 2014/104/EU of 26 November 2014 on the rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union.

[5] Carrera, S., Gaonzalez-Fuster, G., Guild, E., Mitsilegas, V. (2015), Access to Electronic Data by Third-country Law Enforcement Agencies, Challenges to the Rule of Law and Fundamental Rights, Centre for European Policy Studies, Brussels, available at

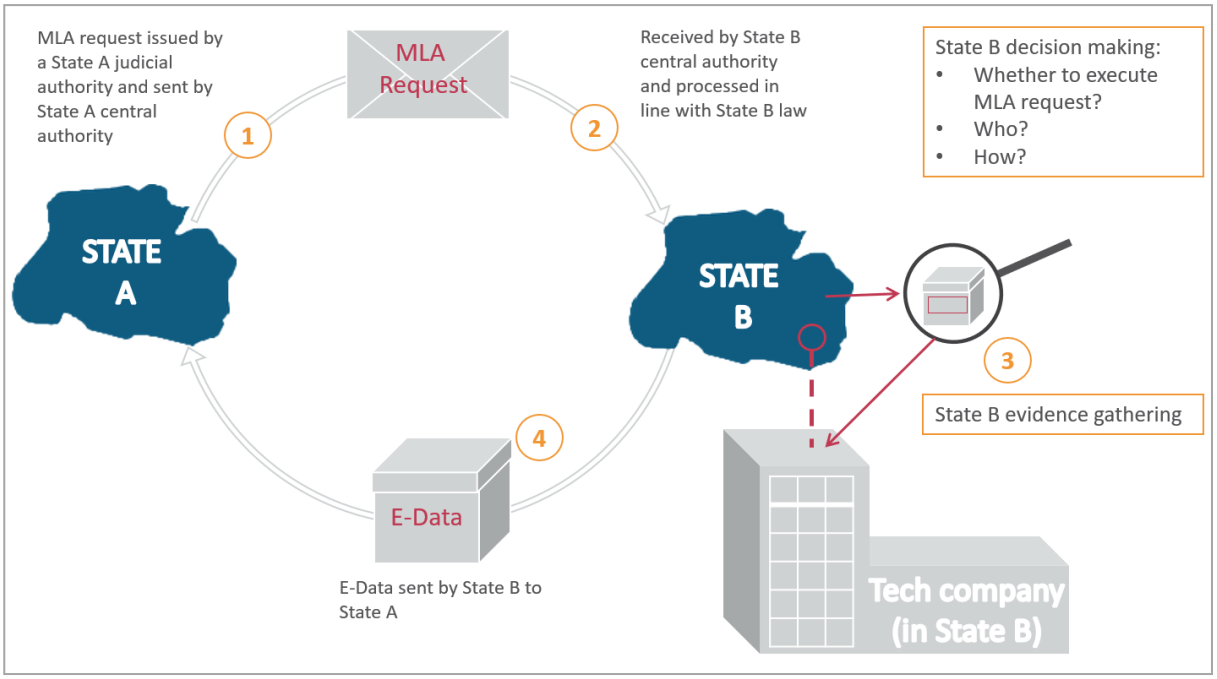
https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf.

and process requests. The complex process (involving numerous stages) was described by one participant at the Practitioners' workshop that Fair Trials organised on 3 July 2018 as follows:

> *Requests submitted by foreign governments to the US are first received from the police, who then pass them onto the prosecution, who then submit them to the central authority, who finally submit them to the DOJ OIA. Requests arriving in the US are received by the OIA, who then submits them to the US Attorney's office (but now not in respect of e-evidence, as such requests go to the OIA) who has to obtain a court order signed by a judge if content is requested or a police order when the request concerns bank records, subpoena… The producing party then sends that evidence to the DOJ.*[6]

The basic approach under MLA is shown below in Figure 1: MLA arrangements.

Figure 1: MLA arrangements:[7]



9. MLA is regulated by various bi-lateral treaties ("**MLATs**") and regional agreements:

   - **European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 of the Council of Europe ("MLA 1959")**[8] regulates requests for data between countries in the Council of Europe and third-countries that are party to MLA 1959.[9] It deals with a wide range of matters such as the examination of witnesses, service of official documents and judicial verdicts, summoning of witnesses and transmission of information from judicial records.[10] It establishes the requirements that requests for MLA have to meet and sets out rules for their enforcement by the authorities of the requested state.

[6] JUD-IT Practitioners' workshop, Amy Jeffress, Arnold & Porter.

[7] Thanks to Kingsley Napley and Rachel Scott (3 Raymond Buildings).

[8] European Convention on mutual assistance in criminal matters Council of Europe 1959, ETS No.030, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030.

[9] Brazil, Chile, Israel, Republic of Korea and South Africa.

[10] Mutual Legal Assistance Convention of 1959, Explanatory Report, available at http://www.worldlii.org/int/other/COETSER/1959/3.html.

- **Mutual Legal Assistance Convention of 29 May 2000 ("MLA 2000")**[11] was adopted by the Council of the European Union to modernise the traditional system of international cooperation in criminal matters. It introduced new technological possibilities such as the use of video and telephone conference as well as the interception of telecommunications. It applies between EU Member States.[12] It introduced a requirement for the state receiving the request for cooperation to comply with procedures specified in the request to ensure evidence meets the requirements of the court in which it will be presented.[13]
- **EU MLATs with third countries**: The EU has agreed MLATs with non-EU countries:
    - In 2003, the USA and the EU signed an MLAT which updated mechanisms for cooperation between US and EU LEAs, including on financial account information, authorizing the acquisition of testimony via video conferencing, and allowing joint US-EU investigative teams. It does not specifically cover E-evidence.
    - In 2010 the first MLAT was agreed between the EU and Japan. Before this, no EU Member State had a bilateral MLAT with Japan. The agreement provides for a wide range of measures, including taking evidence, seizing proceeds of crime, obtaining bank information and conducting hearings and video link testimony.
- **Bilateral MLATs**: Countries (including EU Member States) have entered into bilateral MLATs with non-EU countries. Examples of these are numerous and the terms of MLATs can differ.

10. The **Convention on Cybercrime of the Council of Europe** ("**Budapest Convention**") is the first international treaty concerning crimes committed via the Internet and other computer networks.[14] Chapter III of the Budapest Convention provides a framework for MLA, which is subsidiary of the national law of the requested Party or any other applicable MLATs.[15] It also introduces procedures such as the search and seizure of computer networks and interception.[16] It has been ratified by 61 countries within and beyond the borders of the EU.[17]

11. For the cross-border exchange of evidence within the EU, since 2003 the EU has adopted a series of mechanisms under the principle of mutual recognition. Under this regime, if the authorities in one Member State (the "**Issuing State**") demand electronic evidence from another Member State (the "**Executing State**") the authorities of the Executing State are required to act on it with the same priority as any national investigation.[18] These instruments allow for direct requests between judicial authorities (without the mediation of central authorities), are more prescriptive in terms of the format for demands, provide clear timeframes and allow for fewer grounds for the Executing State to refuse:

---

[11] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000F0712(02)&from=en.

[12] In 2001, the Council of Europe adopted the Second Additional Protocol to the MLA Convention of 1959 in order to introduce most of the modifications made by the MLA Convention of 2000 in its own legal framework.

[13] Van Wijk, M.C., *Cross-border evidence gathering: equality of arms within the EU?,* 2017, The Hague: Eleven International Publishing, page 73.

[14]Council of Europe, Convention on Cybercrime(CETS No 185), 2001, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[15] Budapest Convention, Article 25 (4) and Article 27.

[16] Budapest Convention, Articles 19-21.

[17] Council of Europe, Details on Treaty No. 185, Convention on Cybercrime, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[18] JUD-IT Practitioners' workshop, Dr. Marloes van Wijk, University of Maastricht.

- In 2008 the EU created the **European Evidence Warrant ("EEW")** which allowed for the demand for pre-existing objects, documents and data in the possession of foreign authorities.[19]
- The EEW was not considered a success and was superseded by **European Investigation Order ("EIO")** which Member States were required to have implemented by May 2017.[20] The EIO updated, and replaced to a large extent, the legal framework applicable to the gathering and transfer of evidence between Member States. It covers any investigative measure (except for joint investigation teams), which includes access to electronic data.[21] This was described as "great" by one expert at the practitioners' workshop:

> *In the past, the process for requesting MLA involved prosecutors sending polite letters explaining the importance of the collection of the particular piece of evidence. It very much depended on whether the receiving authority wanted to cooperate or not. With some countries you never knew what you were going to get back.*[22]

Direct cooperation between a public authority and a service provider

12. LEAs also make direct demands of the companies that hold electronic data. The LEA investigating a crime directly contacts a business which holds electronic data (established in its own country or in another country), in accordance with their own national laws, to demand electronic data held by the business. This is shown in Figure 2: Direct cooperation. Within the EU, the possibility of a service provider established in a EU country to comply with requests from LEAs from other countries is either not permitted under national law or unregulated.[23] Some service providers established in the US and, to a more limited extent, in Ireland, do however reply to direct requests from LEAs. For US service providers, this cooperation is voluntary as a matter of US law.[24] The Commission reported that the number of direct requests for electronic data from service providers has increased considerably in recent years.[25]

---

[19] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0978&from=EN).

[20] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, the **"EIO Directive"** (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=en).

[21] Specifically, Article 10(2)(e) of the EIO Directive covers: "the identification of persons holding a subscription of a specified phone number of IP address".

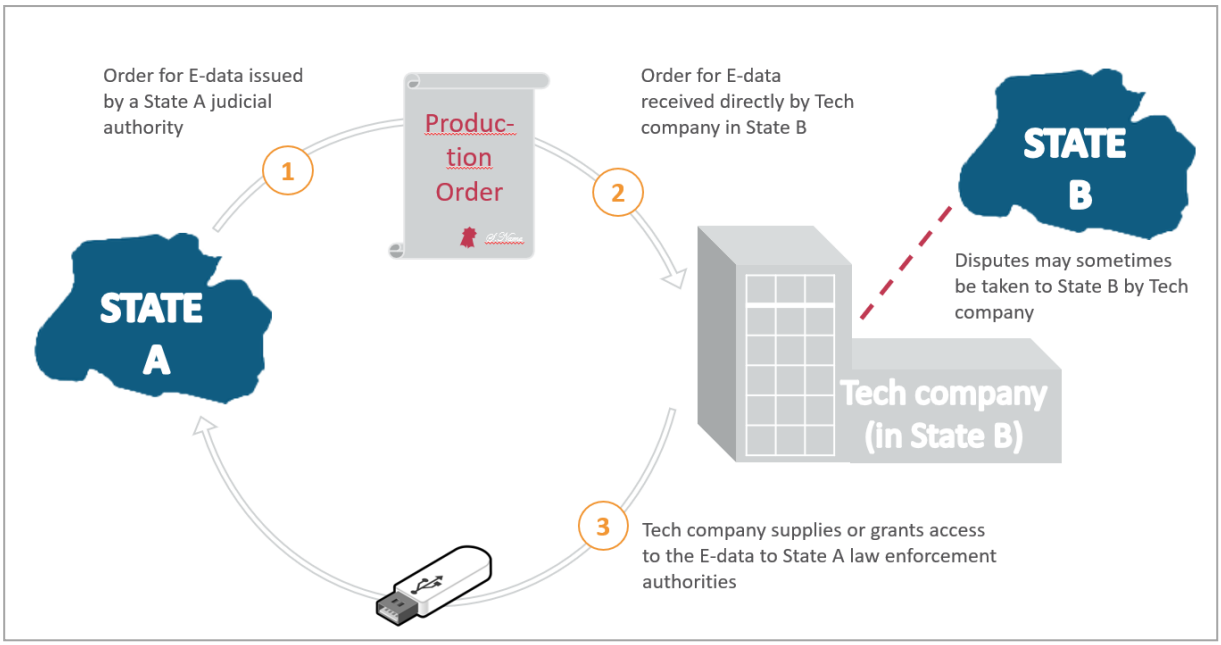
[22] JUD-IT Practitioners' workshop, Nick Vamos, Peters & Peters.

[23] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 26, (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN). Note that the European Commission survey conducted prior to the E-evidence Proposal indicates that the domestic law of only two Member States allow for direct cooperation. See: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf.

[24] US service providers are permitted to cooperate directly with European public authorities with regard to non-content data under section 2701(2) of the Electronic Communications and Privacy Act 1986 ("**ECPA"**), but not in respect of content data.

[25] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 14 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN). See also JUD-IT Practitioners' workshop, Achille Campagna, Studio Legale & Notarile Campagna.

Figure 2: Direct cooperation[26]



Direct access to electronic evidence by a public authority

13. In this case, LEAs access electronic data without the help of an intermediary such as a judicial authority of another state or a service provider. This could, for example, be done:

    - Following the seizure of a device which is then used to access data held in another country (such as using a suspect's laptop to access data held in the cloud) – according to the Commission most Member States allow this type of search by LEAs;[27] or
    - After acquiring access credentials to access electronic data (i.e. logging into a person's email account and accessing their emails held on a remove server) – the Commission states: "Only a few Member States allow their authorities to perform remote searches, although the number is increasing."[28]

14. Often, the location of this electronic data accessed in this way is not known to LEAs and may even be impossible to determine. As a result, it can be difficult to determine whether such searches have a cross-border component. Forms of direct access are regulated by domestic law if at all, and the approaches adopted differ. For example, where the location of evidence is unclear, some Member States treat it as being held domestically, while others seek to use judicial cooperation mechanisms to access it. Where the electronic evidence is known to be held outside of the country, Member States again apply different approaches: some allow their LEAs to access that data; while others require a formal judicial cooperation mechanism to be used. The safeguards which apply to these forms of direct access (discussed below) also vary from country to country.

[26] Thanks to Kingsley Napley and Rachel Scott (3 Raymond Buildings).

[27] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 33 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

[28] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 33 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

Limitations of existing mechanisms - legal reform

15. As one expert in the JUD-IT practitioners' workshop stated:

> *Before, evidence of a murder in Paris was located in Paris but now evidence is often held outside of France, in the "cloud". An ordinary crime becomes an international incident, placing great pressure on the previous MLA system.*[29]

In its evaluation of the current mechanisms, the Commission concludes that:

> *These channels suffer from a number of shortcomings…: judicial cooperation is often too slow for timely access to data and can entail a disproportionate expense of resources; direct cooperation can be unreliable, is only possible with a limited number of service providers which all apply different policies, is not transparent and lacks accountability; legal fragmentation abounds, increasing costs on all sides; and the size of the problem is steadily increasing, creating further delays.*[30]

16. It is beyond the scope of this paper to review these criticisms, however in broad terms:

- MLAT has been criticised for its inefficiency due to the fact that the public authorities in two countries are involved in the sharing of electronic data. Furthermore, in the context of multi-national holders of data and cloud-based computing, there is uncertainty about which country should receive the request, whether the LEAs in that country have the power to obtain the data[31] and what law applies to the holder of data.
- Although direct requests for cooperation by service providers have considerably increased, less than half of these requests are successful.[32] In particular, typically service providers will not provide content data.[33] The legal legitimacy of these direct requests has also been subject to legal disputes.[34] These arrangements can also create commercial challenges (such as a loss of trust from customers), costs and conflicts of law for the companies in question.
- Direct access is not always available and can often result in data being lost. For example, some forms of direct access can make the suspect aware of the investigation, creating a significant risk that data will be moved or deleted. The Commission has also highlighted challenges relating to the wide range of legal approaches to such access and to protecting the rights of people whose data is accessed. [35]

17. In response to these challenges and the growing need for LEAs to be able to access electronic data across borders, proposals for new mechanisms have recently been adopted[36] and are currently

[29] JUD-IT Practitioners' workshop, Professor Peter Swire, Georgia Institute of Technology.

[30] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 14 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

[31] *United States v. Microsoft Corp*, No. 14-2985 (2d Cir. 2016), JUD-IT Practitioners' workshop, Professor Peter Swire, Georgia Institute of Technology.

[32] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 14ff (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

[33] In the US, this is prohibited by ECPA (the US "blocking statute").

[34] *Hof van Cassatie of Belgium, YAHOO! Inc*., No. P.13.2082.N of 1 December 2015. *Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium*, No. ME20.F1.105151-12 of 27 October 2016.

[35] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 34 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

[36] US Clarifying Lawful Overseas Use of Data (**"CLOUD Act**"), S. 2383, HR 4943.

being considered.[37] Notably, on 17 April 2018, the Commission presented a proposal (the "**E-evidence Proposal**") to create a new cross-border cooperation mechanism to facilitate access to electronic evidence in the context of criminal investigations, through a "European Production Order" and a "European Preservation Order" (together, the "**Orders**"). The Orders would allow prosecutors and judicial authorities of EU Member States to request electronic data (both content and metadata) directly from service providers offering services within the EU, regardless of where the data is located or where the company is headquartered. It is not proposed that the Orders will replace the EIO for obtaining electronic data but will operate alongside it as additional tools for LEAs.

C) The JUD-IT Project

18. This paper is produced in the context of an EU-funded research project coordinated by the Centre for European Policy Studies ("**CEPS**"): "Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU" (the "**JUD-IT Project**").[38] The JUD-IT Project researches ways in which cross-border judicial cooperation directed at requesting, accessing, exchanging and using electronic information as evidence in the framework of criminal proceedings can be streamlined and made effective within the EU and in relations with third countries.[39]

19. The main aims are to:

- Develop a set of benchmarks ensuring that cross-border requests and access to electronic information in criminal proceedings are in line with the EU rule of law and fundamental rights standards;
- Deliver an in-depth comparative examination and assessment of the day-to-day practices and relevant legal challenges in securing, requesting, and obtaining digital information held by private companies;
- Identify promising practices that are established under clear EU legal basis and present the potential to make access and use of electronic information in the criminal justice domain more efficient and in line with the needs of relevant authorities and actors; and
- Produce sound and independent academic research and exchange expert knowledge among different communities of practice.

D) Current paper and methodology

20. The aim of the current paper (produced as part of the JUD-IT Project) is to analyse the impact of current mechanisms for the cross-border access to electronic data on the fairness of criminal proceedings. It seeks to:

- Identify the key fair trial principles (protected by international and regional human rights) which are affected by cross-border electronic data exchange;

---

[37] JUD-IT Practitioners' workshop, Dr. Wouter van Ballegooij, European Parliament, Directorate-General for Parliamentary Research Services (speaking in a personal capacity).

[38] Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust (JUD-IT), available at https://www.ceps.eu/juditproject.

[39] It provides an in-depth comparative assessment of promising practices and practical and legal challenges in accessing digital information held by IT companies in the context of: first, the implementation of the EU flagship mutual recognition instrument on the exchange of evidence in criminal justice, the European Investigation Order; and second, the application of EU Mutual Legal Assistance Treaties with third states like the USA and Japan.

- Identify areas in which current law and practice on electronic data exchange is in tension with these principles; and
- Recommend reforms to law and practice, including by highlighting rights-compliant practices, where they exist.

21. The paper draws on:
    - Desk-based research into existing and proposed legal instruments and secondary sources on electronic data exchange within the EU and between EU Member States and third countries, primarily the US.
    - In May 2018, Fair Trials disseminated a survey to the Legal Experts Advisory Panel (**LEAP**)[40] to gather expertise and knowledge from criminal law practitioners with experience in dealing with cross-border request for digital data in their daily practice. The survey questions are included in Annex 1: LEAP Survey and aimed to understand the obstacles faced by defence practitioners in the context of electronic data exchange.[41]
    - On 3 July 2018, Fair Trials organised a practitioners' workshop bringing together experts in cross-border justice cooperation from academia, the legal profession, civil society and industry to share experiences and perspectives and to identify the fundamental rights risks that arise in the context of electronic data exchange. Further information on the workshop is provided at Annex 2: practitioners' workshop.
    - With the aim of completing any gaps in the research, Fair Trials conducted follow-up interviews in person, or over the phone, with identified EU and US criminal justice stakeholders involved in MLA with European jurisdictions. The interview questions are included in Annex 3: interview questions.

22. In the following sections of the paper, we assess the compatibility of current law and practice on cross-border electronic data exchange with a fair criminal justice process. Before doing that, however, we identify the key principles of human rights law which are affected by electronic data exchange. Although interrelated, these are broken down into:
    - Those principles which determine the fairness of criminal proceedings from the perspective of the accused; and
    - More broadly, principles relating to the rule of law and the fairness of the criminal justice process from the perspective of people other than the accused.

[40] The leading criminal justice network in Europe consisting of over 180 criminal defence law firms, academic institutions and civil society organizations. More information about this network and its work on the right to a fair trial in Europe can be found at: https://www.fairtrials.org/legal-experts-advisory-panel.

[41] We received responses from six LEAP members in five countries: Belgium, Greece, Estonia, San Marino and the United Kingdom. The responses to this questionnaire have been incorporated in this paper but the identities of the respondents have been anonymised.

Electronic data and fair criminal justice

A) Electronic data and the rights of the accused: key principles

23. The creation of the mechanisms for the cross-border exchange of electronic data has been driven by the needs of LEAs and these tools are fundamentally one-sided:

> *What becomes clear from the analysis of the European treaties and legislation on cross-border evidence gathering is that both the traditional system and the enhanced system of international cooperation focus on the cooperation between authorities. There is little – if any – consideration for the interests of the defence in this procedure of international cooperation, and especially not for creating procedural equality between the parties with regard to preparing a case for trial. Only the Directive on the EIO recognises the interest of the defence in obtaining evidence through international cooperation by setting forth that the defence should be able to request that an EIO be issued.*[42]

24. These mechanisms (and the way they are applied in practice) also, however, have a significant impact on the rights of the accused person.[43]

25. International human rights law approaches the fairness of criminal proceedings primarily from the perspective of the accused. Article 6 of the European Convention on Human Rights (the "**ECHR**"), for example states:[44]

> *(1) In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law… (2) Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law. (3) Everyone charged with a criminal offence has the following minimum rights …*

This recognises the severe implications of a criminal prosecution and conviction on the accused: resulting in long-lasting stigma, loss of employment prospects, family relationships, and civil liberties in addition to the potential for loss of liberty and the imposition of severe penalties. This is one of harshest measures a state can take against a person and, for this to be a legitimate use of state power, international law requires key principles of fairness to be respected. These principles are designed to ensure a fair outcome (to limit the risk of people being wrongly convicted) and to ensure a fair process (in which the accused person is able to participate effectively).

26. Articles 47 and 48 of the EU Charter of Fundamental Rights (**"EU Charter" or CFR**) enshrine the right to a fair trial and to an effective remedy, and by virtue of Article 51 of the EU Charter, must

---

[42] Van Wijk, M.C., *Cross-border evidence gathering. Equality of arms within the EU?*, Eleven International Publishing, 2017, The Hague, p. 277.

[43] JUD-IT Practitioners' workshop, Jun.-Prof. Dr. Dominik Brodowski, Universität des Saarlandes.

[44] Similar fair trial protections exist in other regional and international human rights treaties, such as: UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171("**ICCPR**")(Article 14), Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02 (Chapter IV), Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969 (Article 8), Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982). (Article 7).

be respected by the EU institutions and the EU Member States when they apply or implement EU law:

> *This means that the CFR can be applicable to cases on a national, cross-border or transnational, and European level, provided that those cases concern the application of EU legislation or national legislation implementing EU law.*[45]

27. The creation of minimum standards in this area has been a key area of EU legislation in recent years, with EU directives protecting the right to information,[46] the right of access to a lawyer, [47] the right to legal aid,[48] the right to presumption of innocence and to be present at trial[49] and the rights of children in criminal proceedings[50] (together, the "**Roadmap Directives"**). The Roadmap Directives aim at facilitating mutual recognition in criminal matters[51] and it has also been argued that the Roadmap Directives are:

> *Necessary to address the effects of the operation of automatic inter-state cooperation, as expressed by mutual recognition, on the individual.*[52]

28. To understand the impact of cross-border electronic data exchange on the rights of the accused, it is crucial to bear in mind the principles, outlined below, which underpin the right to a fair trial. Although the concepts are widely-recognised, the way in which the rights apply varies significantly in different criminal justice systems.

---

[45] Van Wijk, M. C., *Cross-border evidence gathering. Equality of arms within the EU?*, Eleven International Publishing, 2017, The Hague, p. 49.

[46] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (OJ 2012 L 142, p. 1), the **"Right to Information Directive"**.

[47] Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ 2013 L 290, p. 1), the **"Access to a Lawyer Directive"**.

[48] Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ 2016 L 297, p.1).

[49] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, (OJ 2016 L 65, p. 1).

[50] Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, (OJ 2016 L 132, p.1).

[51] Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings 2009/C 295/01.

[52] Mitsilegas, V., "The Symbiotic Relation Between Mutual Trust and Fundamental Rights in Europe's Area of Criminal Justice", *New Journal of European Criminal Law,* Volume 6, 2015, p. 476 (available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2632892).

The presumption of innocence

29. At the heart of the right to a fair trial is the concept that "[e]veryone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to the law."[53] Some key aspects of this concept include:

- Responsibility falls on the state to prove guilt and discharge the presumption of innocence; not for the defendant to prove innocence;
- Because of the serious consequences of a criminal conviction, the state must prove guilt to a high standard: If doubt remains, the defendant must be given the benefit of the doubt;
- A person cannot normally be compelled to confess guilt or to give evidence against themselves;
- As discussed below, because of the impact of ongoing criminal proceedings on people who should be presumed innocent, an accused has the right to a trial within a reasonable time.

Key questions:

- Is the accused required to incriminate themselves, by for example being required to give access to passwords needed to access electronic data?
- As discussed below, does the accused person have the right to challenge whether the state has offered enough evidence to meet the burden of proof?
- Is reliance on electronic data causing unreasonable delays in criminal prosecutions?

Adequate time and facilities to prepare the defence

30. The accused is not merely a passive subject of criminal proceedings: they have the right to be active participants and to present a defence. This means the accused has the right to challenge evidence of guilt presented by the state (for example that it lacks strength or was unlawfully obtained) and to present evidence of innocence. Key aspects of this concept include the right to:

- Sufficient time to analyse the case against the accused and prepare a defence;
- As discussed further below, the right to advance notice of the evidence being relied on by the state and the right to gather evidence (whether directly or through an appropriate LEA) which counters the evidence relied on to prove guilt or which establishes innocence;
- Effective representation by a competent lawyer (paid for by the state where necessary) and to confidential communication with their lawyer (from which derives the concept of legal privilege); and
- Access to the technical facilities needed to build a defence.

Key questions:

- Does the accused have the time to analyse electronic data relied on by the state and to gather electronic data?
- Does the accused and their lawyer have the technical capacity to understand, identify and process electronic data?

[53] ICCPR, Article 14(2).

- Do mechanisms for gathering electronic data undermine the ability of an accused person to communicate confidentially with their lawyer?

The ability to access and contest evidence

31. Part of the concept of "adequate facilities", the right to access and contest evidence is crucial in this context. According to the UN Human Rights Committee, for example, the term "adequate facilities" must be interpreted to include:

> *[…] access to documents and other evidence; this access must include all materials that the prosecution plans to offer in court against the accused or that are exculpatory. Exculpatory material should be understood as including not only material establishing innocence but also other evidence that could assist the defence…"*[54]

An accused must have a genuine opportunity to challenge evidence presented against them and to present their own evidence.[55] The adversarial element in criminal proceedings generally requires disclosure to the defence of evidence for or against the accused:[56]

> *It is a matter for the defence to assess whether a submission deserves a reaction. It is therefore unfair for the prosecution to make submissions to a court without the knowledge of the defence.*[57]

Key questions:

- Does the accused know what electronic data the state is relying on to establish guilt and are they able to challenge the probity of that evidence?
- Does the accused know how electronic data has been obtained in order to be able to challenge its probity or its legality and/or admissibility in court?
- Does the accused have access to electronic data in the possession of the state which is exculpatory? Who determines what material is exculpatory?
- Is the accused able to gather electronic data which establishes their innocence or challenges the strength of evidence presented by the state as evidence of guilt?

Equality of arms

32. In criminal trials, where the prosecution has all the machinery of the state behind it, the principle of equality of arms is an essential guarantee of an accused's right to defend themselves. It ensures the accused has a genuine opportunity to prepare and present their case, and to contest the arguments and evidence put before the court, on a footing equal to that of the prosecution. The principle seeks to prevent the defendant being placed at a substantial disadvantage vis-à-vis their

[54] UN Human Rights Committee, General Comment No. 32, Article 14: Right to equality before courts and tribunals and to a fair trial, CCPR/C/GC/32, 21 August 2007.

[55] *Barberà, Messegué and Jabardo v. Spain*, 6 December 1988, Series A no. 146, para 78.

[56] *Edwards v. the United Kingdom*, 16 December 1992, Series A no. 247-B, para 33-39.

[57] *Bulut v. Austria*, 22 February 1996, Reports of Judgments and Decisions 1996-II.

opponent[58] and to ensure "procedural equality" between the parties.[59] In practice, this is difficult to achieve:

> *The principle of equality of arms represents the "functional principle that participants in criminal proceedings must have equal opportunities to influence its course and outcome", and superiority of the prosecutor must be offset by "effective defence capabilities". Therefore we are seeking fair balance between parties considering criminal procedure as whole and not only one part of it*.[60]

Key questions:

- Are the opportunities for the accused to access electronic data sufficient to ensure a fair balance with the rights of the prosecution to access such evidence?
- Does the defence have sufficient access to the technical facilities needed to process and understand electronic data to ensure a fair balance with the rights of the prosecution?

B) Electronic data and the rule of law

33. As outlined above, the fairness of criminal justice systems is defined in human rights law primarily by reference to fairness for the accused; however, it has broader ramifications. A fair criminal justice system is a core building block of the rule of law, ensuring the fair and proportionate exercise of state power; it helps build public trust in the justice system; and can contribute to respect for (or violation of) a range of other human rights. As the Commission recognises, the principles underlying the concept of rule of law in the EU include legal certainty; prohibition of arbitrariness of the executive powers; independent and impartial courts; effective judicial review including respect for fundamental rights; and equality before the law.[61]

34. The Court of Justice of the EU (**"CJEU"**) recently recognised that the execution of mutual recognition instruments in criminal matters may be suspended where there is evidence of deficiencies liable to affect the independence of the judiciary in the issuing Member State and therefore compromise the fundamental right to a fair trial, on the grounds that:

> *The European Union is a union based on the rule of law in which individuals have the right to challenge before the courts the legality of any decision or other national measure relating to the application to them of an EU act.*[62]

Accountability of law enforcement

[58] *Samokhvalov v Russia*, no. 3891/03, 12 February 2009, para 46; *Salov v Ukraine,* no. 65518/01, ECHR 2005-VIII (extracts), para 87; *Sabayev v Russia,* no. 11994/03, 8 April 2010, para. 35.

[59] Van Wijk, M.C., *Cross-border evidence gathering: equality of arms within the EU?*, The Hague: Eleven International Publishing, 2017, p. 5.

[60] Mrčela, M. , *Adversarial principle, the equality of arms and confrontational right – European Court of Human Rights recent jurisprudence,* Vol 1 (2017) Procedural Aspects of EU law, available at https://hrcak.srce.hr/ojs/index.php/eclic/article/view/6519)

[61] European Commission, Communication from the Commission to the European Parliament and the Council, *A New EU Framework to strengthen the Rule of Law,* 11 March 2014, COM (2014) 158 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0158&from=EN.

[62] Case C-216/18 PPU *Minister for Justice and Equality v LM (Deficiencies in the system of justice),* judgment of 25 July 2018 (Grand Chamber), para. 49.

35. States have legitimate reasons to give LEAs legal powers to investigate and prosecute crimes, but this does not mean they have a blank cheque to do whatever they like. Assessing whether LEAs have acted within their legal powers is a key element of a fair criminal justice process. Indeed, the individual criminal trial is the key point at which the behaviour of LEAs is exposed and tested. Broader public reporting and oversight on the activities of LEAs (including in the context of electronic data exchange) can inform public debates about the appropriateness of their actions.

Key questions:

- Are there effective mechanisms to ensure electronic data is not shared where it would be unlawful, for example, because the requesting LEA does not have the power to demand it?
- Can the legality of LEA actions in gathering and sharing electronic data be effectively challenged as part of the criminal process?
- Do mechanisms exist to publicise how LEAs are using cross-border mechanisms for gathering electronic data?

Proportionate use of law enforcement powers

36. Even where LEAs have the legal power to investigate a crime (for example by obtaining electronic data), in a fair criminal justice system those powers should be used in a proportionate way. For example, where there is no basis to suspect a person of having committed a crime, it would be a disproportionate interference with a person's right to privacy to intercept their communications. It is also important to bear in mind that it is not only electronic data relating to an accused that may be gathered and shared: a criminal investigation may establish that a person is not guilty of an offence; may involve gathering the electronic data of multiple people with a view to identifying one guilty person; or may incidentally result in the sharing of evidence with people who are not suspected of a crime.

Key questions:

- Do LEAs need to meet a threshold in terms of suspicion of criminality (and the severity of the offence) before they can request or obtain and share electronic data?
- Can the proportionality of LEA actions in gathering and sharing electronic data be effectively challenged either before electronic data is gathered and shared or during a criminal case?
- Do effective safeguards exist against fishing expeditions which have a disproportionate impact on privacy?

Preventing political abuse

37. There is no doubt that some states abuse criminal procedure to pursue politically-motivated prosecutions. This runs contrary to the rule of law which is based on the concept that the law is applied equally and impartially. High-profile cases have shown how cross-border cooperation by LEAs has been misused for political purposes.[63] Mechanisms for the gathering of cross-border evidence exchange are not immune from this risk: for example, a state may wish to obtain electronic data to find out about the plans of an opposing political party or the location of a human

[63] See for example, Fair Trials' work on abuse of INTERPOL wanted person alerts, available at: https://www.fairtrials.org/campaign/interpol.

rights defender who the state wants to silence. It cannot be assumed that such abuses would not occur even within the European Union.[64]

Key question:

- Do effective mechanisms exist to identify, prevent and expose politically-motivated abuses of cross-border electronic data sharing tools?

Protecting other human rights

38. This paper does not seek to address the considerable implications of cross-border electronic data exchange on privacy.[65] In addition to privacy, electronic data exchange can affect other human rights. For example, in the cross-border context, states bear responsibility for actions which result in or create a risk of human rights abuses in another country. For example, states should not extradite or deport people to countries where there is a real risk that their human rights will be violated, for example, because they will be tortured or subjected to the death penalty.[66] Likewise, states should not share electronic data which will result in human rights abuses – for example, where it is likely to be used to assist in an abusive interrogation or as the basis for a prosecution that could result in capital punishment.

Key question:

- Do effective mechanisms exist to identify and prevent the gathering and cross-border sharing of electronic data where this could result in human rights abuses?

Legal clarity/conflicts of law

39. In cross-border criminal cases (and for multinational companies) one key consideration is which laws apply. Where, for example, LEAs in one country unilaterally directly access electronic data which sits in another country, this can offend principles of national sovereignty. For service providers conflicts of law are a common occurrence. A service provider headquartered in the USA, for example, holding data in Ireland and operating in Belgium could, for example, find that Belgian law requires them to disclose evidence, that data protection law in Ireland prohibits this and that US law allows some level of disclosure but not complete disclosure. Similarly, an individual service-user is unable to determine whether their personal data is protected.

Key question:

- Does the relevant legal framework provide sufficient legal certainty and resolve conflicts of law?

[64] See, for example, the Commission: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/effective-justice/rule-law/rule-law-framework_en.

[65] See, for example, the work of the European Digital Rights (EDRi): *EU 'e-evidence' proposals turn service providers into judicial authorities*, 17 April 2018, available at: https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/.

[66] *Soering v. the United Kingdom*, 7 July 1989, Series A no. 161.

The accused's perspective – electronic data and the right to a fair trial

A) Notification

40. There will sometimes be legitimate law enforcement reasons to keep the fact of an investigation confidential. If a suspect that has not been arrested becomes aware that they are under investigation they might, for example, delete electronic data before it is gathered by LEAs or start using a different (perhaps encrypted) communication platform. This is akin to physical evidence-gathering such as a house search where LEAs would not give prior notification to a suspect that they are seeking a warrant for the search in advance of it happening to prevent the destruction of incriminating evidence before the search takes place. [67]

41. Not surprisingly, the right to keep the preliminary investigative phase confidential is recognised either directly or indirectly in legal mechanisms for E-evidence exchange:

    - The EIO Directive requires Member States to "take due account of the confidentiality of the investigation", and the Executing State not to "disclose any evidence or information provided by the executing authority" and to notify the Issuing State if it cannot comply with confidentiality requirements.[68]
    - Likewise, the EU/Japan MLAT provides "[t]he requested State shall make its best efforts to keep confidential the fact that a request has been made … if such confidentiality is requested … If a request cannot be executed without disclosure of such information, the requested State shall so inform the requesting State."[69]
    - The same provision exists in the EU/USA MLAT. During the JUD-OT practitioners' workshop, a defence lawyer (and former US prosecutor) confirmed that the MLA process happens in the US without notification to the defendant. Even where US laws requires notification (i.e. bank disclosure to customers) these may be bypassed.
    - Similarly, the current E-evidence Proposal includes a "gagging clause" preventing the service provider from "informing the person whose data is being sought in order not to obstruct the relevant criminal proceedings".[70]

42. Although there may sometimes be legitimate reasons for secrecy, the lack of notification is at the core of many of the challenges that electronic data poses to the fairness of the criminal process. Key concerns include that non-notification limits the ability of the accused to prepare their defence and to ensure exculpatory electronic data is preserved. This is an acute concern due to the sometimes-transient nature of electronic data and the fact that the accused may not learn about the obtaining of the electronic data until shortly before the trial.

43. Electronic data may be obtained illegally and may ultimately not be formally admissible in court proceedings. With prior notification this legality could be challenged before the harm is done. Leaving these arguments to the trial (or shortly before it) may not provide a satisfactory remedy because for example:

    - Where they have already received the evidence, the ultimate decision-maker cannot realistically remove the inadmissible evidence from their knowledge;

[67] Interview with US stakeholder.

[68] Article 19 of the EIO Directive.

[69] Article 10 (4) of the EU/Japan MLAT.

[70] Article 11 of the E-evidence Proposal.

- Unlawfully obtained evidence may have been used to obtain evidence indirectly which is ultimately admitted in court – the fact of the electronic data may never be made known;
- The case may never proceed to trial or the person whose data is collected and shared may not be the person who is prosecuted.[71]

44. There is a concern that "gag orders" are excessively used as a matter of course, rather than exceptionally when strictly required. The state or service provider receiving the request for electronic data is not always in a position to assess whether the request for secrecy is justified. For example, one of the experts we interviewed commented that gag orders are used even where the investigation starts after an arrest is made, making a "gag order" inappropriate.[72]

45. These are not just theoretical concerns. This was identified by the practitioners consulted as the biggest obstacle for ensuring equality of arms in electronic data sharing:[73]

> *In order to challenge a request for data, you have to be aware of the request and most requests are confidential and service providers have no real interest in notifying customers. Once the material has been transmitted, you have to be aware of its existence to be able to challenge it in the issuing state. Even if you are able to challenge it at that stage, you might not be able to have it excluded from the casefile or as evidence.*

46. It is impossible completely to resolve the tension between the legitimate law enforcement need for secrecy and the considerable implications of non-notification for a fair criminal process. This might, however, be mitigated by:

- Creating a clear presumption of notification with LEAs' power to use secrecy limited to an exceptional measure requiring specific justification, with sanctions for LEAs which misuse this designation relating, for example, to the admissibility of evidence obtained;[74]
- A requirement to give states (or service providers) clear and detailed reasons for non-notification, and a power for recipients of requests to refuse to comply (or to request further information) where they are not satisfied by the justifications;
- Clear time-limits for the imposition of secrecy;
- An obligation for prompt ex-post notification (not waiting until the full disclosure of the evidence in the case and regardless of whether the affected person is ultimately prosecuted) once the legitimate basis for secrecy no longer applies, with a right for the affected person to challenge the legality of the evidence gathering and use of secrecy;
- An obligation for LEAs requesting electronic data (in the context of secrecy) to extend the request to cover exculpatory evidence (discussed below).

47. There is considerable pressure for these concerns to be resolved if new laws in this area are agreed. Service providers recognise the value that users place in the security and privacy of information they store online and are concerned about the impact of secrecy on user trust. They have litigated to give users more information on the number of LEA orders they receive and respond to; and to limit the use of non-disclosure orders that prevent providers from notifying

[71] Human Rights Watch, "Dark Side: Secret Origins of Evidence in US Criminal Cases", January 2018 (available at https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases).

[72] Interview with US stakeholder (see Annex 2 for questionnaire).

[73] JUD-IT practitioners' workshop, Anand Doobay, Boutique Law.

[74] JUD-IT practitioners' workshop, Jens-Henrik Jeppesen, Center for Democracy and Technology (CDT).

users about LEAs demands for their data. For example, Google has commented in the context of the E-evidence Proposal:

> *We … welcome the steps towards requiring law enforcement to notify the users in certain circumstances, but we encourage legislators to go further. As noted by the Court of Justice of the European Union, notification of the person affected "is in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy." We would recommend … that authorities are required to notify the persons unless there are exceptional circumstances warranting confidentiality … Such notification should only be limited when authorities demonstrate that exceptional circumstances warrant confidentiality. Finally, any such gag order or confidentiality requirement should be governed by strict time limits.*[75]

B) Early access to the casefile

48. The right to access the casefile is a fundamental element of the right to an effective defence according to the principle of equality of arms. It is not possible for a defence lawyer to perform their job effectively without access to all of the inculpatory and exculpatory evidence gathered by the prosecution.[76] This affects key defence rights, including "organisation of the defence, collection of evidence favourable to the accused [and] preparation for questioning."[77] Equally, the Right to Information Directive provides, *inter alia*, that the defence should have access at least to all material evidence in the possession of the competent authorities "in due time to allow the effective exercise of the rights of the defence"[78] and "in order to safeguard the fairness of the proceedings and to prepare the defence."[79]

49. In practice, in many EU Member States, the investigating authorities do not disclose the case file until after the investigation is complete and sometimes only shortly before the trial. For instance, in Estonia, this only happens at the end of the pre-trial phase, which means that the defence will only become aware of what evidence has been gathered (and therefore what is missing and needs to be obtained using cross-border cooperation procedures) at the end of the pre-trial proceedings.[80]

50. Cross-border electronic data exchange does not affect the nature of the obligation to share evidence with the defence. Reliance on this evidence can, however, seriously exacerbate the impact on the defence of failures to comply with this right in a timely manner:

- The transient nature of electronic data can mean that associated exculpatory evidence is no longer available if there is a delay in disclosure; [81]
- The quantity of electronic data that has been obtained (and complexities in processing it to identify relevant evidence for the defence) can make it impossible in practice to exercise the rights of the defence if this is provided late; and

---

[75] Google's position on the E-evidence Proposal. See also Microsoft's position (available at: https://blogs.microsoft.com/eupolicy/2018/04/18/the-eevidence-proposal-a-positive-step-forward/).

[76] *Foucher v. France*, (1997), 18 March 1997, Reports of Judgments and Decisions 1997-II, para. 36; *Kuopila v. Finland*, no. 27752/95, 27 April 2000.

[77] *Dayanan v. Turkey*, no. 7377/03, 13 October 2009, para 32.

[78] Right to Information Directive, Article 7 (3).

[79] Right to Information Directive, Article 7 (2).

[80] LEAP survey.

[81] LEAP survey.

- Given the challenges that the defence face in obtaining their own electronic data (discussed below) late disclosure can result in delays in the case coming to court – this can mean further periods in pre-trial detention and unreasonable delays in resolving the case.

51. Early disclosure is crucial to the fairness of criminal proceedings which rely on electronic data. In addition to compliance with existing human rights standards in this area, measures to mitigate the impact of failures to comply with this right might include:

    - Courts being required to give additional time to the defence to enable them to process electronic data and to obtain exculpatory evidence, with a presumption that detained defendants be released during this additional time so that they do not pay the price of late disclosure;
    - Increased efficiency in collecting electronic data which is required by the defence and sufficient resources being made available to the defence (funded by the state where necessary to enable them to process large quantities of electronic data); and
    - A requirement for LEAs to formulate requests for electronic data in a way that will ensure that relevant exculpatory evidence is also obtained (or preserved).

C) Defence access to evidence-gathering tools

52. Mechanisms for electronic data exchange were designed to increase the capacity of LEAs to obtain evidence to prosecute alleged crimes. In many legal systems, broadly described as "inquisitorial", LEAs are solely responsible for conducting an investigation aimed at establishing the "truth". As such, there are obligations on LEAs to use investigatory powers to gather all relevant evidence, both incriminatory and exculpatory, and not just evidence which establishes guilt. In reality this is not, however, always the case and even an impartial investigator would be unable to know what evidence might be of use to the accused without consulting them to understand the nature of their defence, which cannot happen where the investigation is secret.

Case study – the Netherlands[82]

Terrorism case involving a person who was a citizen of another EU country, accused of being friendly to the cause of terrorism. The prosecution was founded on incriminating evidence from social media. But the data obtained was only inculpatory. The defence had to track down exculpatory evidence, to demonstrate that the person was an academic with an interest in terrorism organizations.

In adversarial models, the defence is expected to take on an active role in the preparation of its case, and autonomously gather information and materials.

53. However, the traditional MLA system does not recognise the possibility for defence practitioners to request cross-border electronic data. Therefore, "it depends on national law to what extent the defence has the opportunity to apply to the authorities to request international cooperation."[83] Although, some avenues may exist for the defence to obtain electronic data, and in any event,

[82] JUD-IT Practitioners' workshop, Frederieke Dolle, Prakken d'Oliviera. Note that the Netherlands is mainly an inquisitorial criminal justice system, and "the defence is not expected to seek to submit evidence independently from the prosecution": Van Wijk, M.C., *Cross-border evidence gathering: equality of arms within the EU?*, The Hague: Eleven International Publishing, 2017, p. 256.

[83] Van Wijk, M.C., *Cross-border evidence gathering: equality of arms within the EU?*, The Hague: Eleven International Publishing, 2017, p. 68.

electronic data obtained by LEAs (including exculpatory evidence) should ultimately be disclosed to the defence,[84] it is rare for countries to give an explicit right to the defence to make use of cross-border evidence gathering tools.

Case Study - Netherlands

The Dutch Code of Criminal Procedure does not contemplate the possibility that the defence may request foreign authorities directly to carry out an investigation, given that under Dutch law the prosecutor is in charge of the criminal investigation. Informally, the defence can apply to the competent national authorities to send a letter of request to have investigations carried out in another State but does not have a legal right to this.

54. The JUD-IT practitioners' workshop and survey of LEAP members suggest that in practice it is extremely difficult, if not impossible, for the defence to persuade a judicial authority to hear and grant a defence application for MLA.[85] The defence can only submit an application (letter of request) to the judicial authority for MLA and must demonstrate in detail how the data requested is relevant to the case, that it is necessary and proportionate in order to conduct the defence, as well as specify what data needs to be obtained, where the data is stored and who holds it.[86] However, it is difficult for defendants to track down the provenance and location of electronic data.[87]

Case Study - Belgium

A criminal investigation was being conducted in Belgium. LEAs (including tax and customs authorities) argued that they had obtained information from the Spanish authorities according to which emails received by the defendant from a Spanish enterprise had been forged by the defendant. During the investigation and criminal procedure, the defence team repeatedly requested the emails. Their own digital research from the emails indicated that the IP-address from which they had been sent was located in Spain, not Belgium (where the defendant resided). However, the defence's request for investigation and cooperation from Spain was dismissed by Belgian LEAs. In the end, the defence had no option but to file a complaint to start a new investigation during the proceedings before the first instance court. The defendant was not given access to the electronic evidence during the proceedings before the first instance court. However, at a later stage in the proceedings, the evidence cleared the defendant. Had the defence been given the opportunity to request electronic data from Spain from the outset, it would have been more time-efficient, and the defendant would not have been convicted at first instance.

55. The EIO is the first instrument explicitly to give a power for the defence to request that an EIO be issued.[88] Theoretically, under the EIO Directive, the court will issue a mandatory EIO which has the same force vis-à-vis the receiving Member State as an EIO issued on the request of the prosecution. A request of the defence should therefore be given more weight than previous MLA requests issued at the request of the defendants. The lack of detail in the EIO Directive has

[84] Interview with US stakeholder: In the US, adversarial system that the defence has the ability to request data by way of a Court order for foreign collection of evidence (cf. Statute 1782). Defence may also request letters rogatory, or obtain data themselves directly from service providers.

[85] JUD-IT practitioners' workshop.

[86] LEAP survey.

[87] JUD-IT practitioner's workshop, Frederieke Dolle, Prakken d'Oliviera.

[88] Article 1(3) of the EIO Directive: "the issuing of an EIO may be requested by a suspected or accused person, or by a lawyer on his behalf, within the framework of applicable defence rights in conformity with national criminal procedure".

however been criticised and does not, for example, provide for how the defence makes this request and to which authority. This will depend on the national criminal procedure of each Member State.

56. It remains to be seen whether this new provision will make a difference in practice – it is too early to assess.[89] By contrast to the EIO, the E-evidence Proposal does not expressly recognise the power of the defence to request the issuance of an Order to seek exculpatory evidence.

57. The situation in relation to defense access to stored electronic communications is fraught even when there is not the added challenge of a cross-border element. In the United States, where most electronic communications are stored, defense practitioners generally do not have to navigate cross-border mechanisms like MLAT or letters rogatory in order to access electronic data relevant to their cases. Yet they still struggle with obtaining such access. US courts have interpreted federal statutes governing access to stored electronic communications[90] such that governments (i.e. prosecutors) acting in the public interest may access such communications via search warrants, but defense lawyers are deemed to be acting in a "private" interest and do not enjoy such access.[91] Existing issues around insufficiency of evidence disclosure to the defense become intensified in the electronic data context, making reform of these laws to ensure that the defense are similarly situated to the prosecution more urgent than ever.

58. It is clear that the current level of defence access to cross-border evidence is one of the key threats to a fair criminal justice process, hindering the ability of the accused to prepare a defence, delaying proceedings and making it impossible to ensure procedural equality between the parties. Measures to redress this might include:
    - Powers to the defence to demand evidence gathering on equal terms with prosecutors, and obligations on states or service providers receiving such requests to process them with the same urgency as requests received from LEAs (as in the EIO Directive); and
    - Courts being required to give additional time to the defence to enable it to request electronic data, with a presumption that detained defendants be released during this additional time where delays are caused by non-notification and/or late disclosure.

D) Preserving evidence

59. Given the volatile nature of electronic data, by the time the defence finally obtains disclosure of the case file, exculpatory electronic data may already have been deleted. This is aggravated by the fact that pre-trial investigations (often secret) may run over the course several months and, in some cases, years. For example, an LEA may secure electronic data from a service provider which shows that an accused has been accessing extremist websites. The defence may wish to show that

---

[89] Van Wijk, M.C., *Cross-border evidence gathering: equality of arms within the EU?*, The Hague: Eleven International Publishing, 2017, p. 94. JUD-IT Practitioners' workshop, Dr. Marloes van Wijk, University of Maastricht: "The EIO Directive could have determined which authority (such as a judge) should decide on the request of the defence, time limits, the grounds on which a request must be accepted (in the interests of the defence rather than the investigation). But instead the EIO Directive refers to: "*in conformity with national criminal procedure*".

[90] Stored Communications Act (**"SCA"**), codified at 18 U.S.C. Chapter 121 §§ 2701–2712.

[91] *Facebook v Hunter, Facebook, Inc. v. Superior Court*, 240 Cal. App. 4th 203 (2015) available at: https://caselaw.findlaw.com/ca-court-of-appeal/1712734.html. For further commentary, see: Electronic Frontier Foundation, *A Constitutional Conundrum That's Not Going Away – Unequal Access to Social Media Posts, 31 May 2018*, available at: https://www.eff.org/deeplinks/2018/05/ca-supreme-court-leaves-scales-tipped-prosecutions-favor-defense-gets-access.

this was part of a broader pattern of internet use demonstrating that they were, in fact, undertaking an academic study of extremism (as in the Dutch case study above). However, by the time the accused is aware of the investigation, data relating to that broader internet search history may have been deleted by the service provider, making an effective defence impossible. Within the EU, privacy rights limit the amount of time service providers should retain data.[92]

60. Existing MLA instruments and the EIO do not foresee the possibility of the defence seeking to ensure the preservation of data that could support the defence. Likewise, the E-evidence Proposal, despite containing specific powers to require the preservation of electronic data, is silent as to the need to preserve exculpatory evidence. Furthermore, as discussed above, even if LEAs are required (by law) to obtain all relevant evidence (including exculpatory) they will not know what evidence the defence might wish to rely on without consulting them. This is clearly impossible in the context of a secret investigation. To ensure the net is cast sufficiently widely, an LEA would have to seek large quantities of data (raising other proportionality and privacy concerns).

61. Where exculpatory electronic data has been destroyed by the time the accused is in a position to request it, this denies the accused an effective defence creating the risk of miscarriages of justice. This problem, closely related to non-notification, might to some extent be mitigated by:

- Limiting the use of gagging orders as discussed previously;
- Ensuring LEAs are under a clear obligation to secure (or at least require the preservation of) all evidence of relevance to the case (both inculpatory and exculpatory); and
- Giving the benefit of the doubt to the defence during the trial where exculpatory electronic data is no longer available.

E) Challenging prosecution evidence

62. As well as obtaining and presenting their own exculpatory evidence, a fair trial requires the accused to be able to challenge evidence which is being used to establish guilt. This could, for example, be a challenge to the probity of the evidence (i.e. demonstrating that electronic data presented about websites an accused has visited does not in fact demonstrate that it was the accused who accessed the sites) or a challenge to the admissibility of the evidence on which the prosecution is seeking to rely (linked to the later discussion on the challenging unlawful actions by LEAs). Current systems for cross-border evidence exchange can make it hard for the defence to exercise this right.

63. For example, where evidence is gathered by LEAs in another country, it can be difficult to obtain information on how that evidence was gathered and to understand whether this was done in violation of local law or in a way which undermines its reliability. Courts considering electronic data obtained from foreign LEAs may be reluctant to question the legality or probity of the evidence-gathered by the foreign LEA for fear that the country may be less willing to cooperate with investigations in future if their methods and the legality of their actions are subject to judicial and public scrutiny.

64. The defence is likely to need legal assistance in the state providing the electronic data if they are to challenge the legality of how an MLA request is exercised and thereby to challenge the admissibility of the electronic data obtained:

[92] Cf: European Union Agency for Fundamental Rights, *Data retention across the EU*, available at: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention.

Most criminal cases are handled on the basis of legal aid and suspects often do not have the resources to assess US law and convince the judge that the data was not gathered legally.[93]

65. Some countries' laws create a "presumption of legality" in respect of information gathered abroad. This is, for example, the case in Belgium where defence lawyers bear the burden of demonstrating that due process has been violated and that the rights of the defendant have not been respected in the executing country.[94]

66. The inability for the defence effectively to challenge electronic data obtained from another country could be addressed by:

- Ensuring that sufficient information is provided by the requested LEA about the evidence gathered and the legality of its actions as part of the cooperation;
- Giving the defence a right to challenge prosecution evidence and prohibiting "presumptions of admissibility"; and
- Allowing the appointment (funded by the state where needed) of lawyers in the state from which the evidence was obtained.

F) Capacity of the defence to understand and manage electronic data

67. Even if an accused has a competent defence lawyer, which is not universally the case particularly for indigent defendants, the reliance on electronic data can make it hard for a lawyer to do their job. Electronic data can be technical in nature, requiring specialist skills and knowledge to analyse, understand and use. Without specialist training, a defence lawyer may not be aware of the significance of the electronic data provided and may not know what kind of exculpatory electronic data might exist or where it is located. For this reason, the US Federal Court Service has created a specialist team to assist public defenders: the National IT Operations Application Division.[95] We are not aware of similar mechanisms in EU Member States where the prevalence of private sector defence lawyers would make such an innovation challenging.

68. Reviewing electronic data is a time-consuming and onerous task, especially where the defence has limited resources and when a client is in detention and cannot assist with the review of the data, creating a risk that potentially relevant data is overlooked. These problems can be exacerbated by the quantity of electronic data defence lawyers are given (as discussed above, often shortly before trial and without notification).[96]

A particular problem that defence practitioners are facing is that requests for information are being used more often, and in many cases, the volume of material that the defence has to deal with has shot up. Moreover, the format in which data is handed over to the defence is such that defence practitioners cannot deal with it without sophisticated software applications (costing tens of thousands of euros). Legal aid cannot handle this. Even the most prominent law firms are struggling.[97]

[93] JUD-IT Practitioners' workshop, Anand Doobay, Boutique Law. Also Practitioners' workshop, Holger Matt, European Criminal Bar Association.

[94] JUD-IT Practitioners' workshop, Christophe Marchand, Jus Cogens.

[95] Interviews with US stakeholders. See: http://www.uscourts.gov/court-locator/national-it-operations-applications-division.

[96] Interviews with US stakeholders.

[97] JUD-IT practitioners' workshop, Jaanus Tehver, Law Office Tehver & Partners.

The US Federal Public Defender service has developed a protocol with the Department of Justice designed to address these challenges.[98] Furthermore, the format in which this type of evidence is included in the casefile can require the use of sophisticated software forensics viewers that are unaffordable for the defence.[99]

69. In practice, lawyers working under legal aid are not in a position to adequately deal with cases involving large quantities of electronic data. This is likely to contrast significantly with the tools available to LEAs, threatening equality of arms.

70. In order to overcome the challenges, the defence faces in understanding and processing electronic data in a way that ensures procedural equality with the prosecution, we recommend:

- The prompt notification of requests for electronic data and timely disclosure of evidence to the defence (discussed above);
- The development of protocols for the handling and sharing of electronic data between LEAs and the defence to ensure that it is provided in a way (and at a time) which increases the ability of the defence to process it;
- Funding for the defence to acquire the IT tools they need to process electronic data on an equal footing to LEAs;
- The development and delivery of specialist training for defence lawyers on technology and electronic data; and
- The creation of either specialist units to provide *ad hoc* assistance to lawyers handling electronic data (perhaps within Bar Associations) or the provision of financial support to enable lawyers to contract privately with experts to obtain this support.

G) Legal privilege

71. As the preamble to the Access to a Lawyer Directive explains, "Confidentiality of communication between suspects or accused persons and their lawyer is key to ensuring the effective exercise of the rights of the defence and is an essential part of the right to a fair trial."[100] This is recognised in a number of the legal mechanisms for cross-border evidence exchange. For example, lawyer-client privilege if referred to in the EIO Directive as a ground for non-execution of the EIO.[101] Although it is not proposed that there would be an executing judicial authority under the E-evidence Proposal, the current draft contains protections designed to address this including a requirement on the issuing Member State to take into account any such immunities or privileges.[102]

72. In the context of electronic data exchange, there is a higher risk than with physical evidence that lawyer-client communications will be obtained by LEAs.[103] For example, if electronic data is requested relating to an accused's communications, it may be hard to weed-out privileged

[98] Interviews with US stakeholders. Protocol, designed by the National Litigation Support Unit in collaboration with Department of Justice: United States Department of Justice (DOJ) and Administrative Office of the U.S Court (AO) Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG), *Recommendations for Electronically Stored Information (ESI) Discovery Production on Federal Criminal Cases*, February 2012, available at: http://www.uscourts.gov/sites/default/files/finalesiprotocolbookmarked.pdf.

[99] Interviews with US stakeholders.

[100] Recital 33, Access to a Lawyer Directive.

[101] Article 11(1)(a) of the EIO Directive.

[102] Article 6(7) of the E-evidence Proposal.

[103] JUD-IT Practitioners' workshop, Rebecca Niblock and Anand Doobay.

communication between a lawyer and the accused. This would likely be exacerbated in the context of the E-evidence Proposal:[104]

> *Another issue concerns the question of privilege. The proposal confirms that privilege will be protected but does not shed any light on who will assess whether material is privileged and how they will do this.*[105]

Added to this, countries apply very different approaches to legal privilege.[106] Some countries offer strong protections (Germany[107] or USA[108]); others take a narrower approach (UK[109]) or do not formally codify privilege at all. If privileged electronic data is provided to an LEA, it will not be straightforward for the state to provide an effective *ex post* remedy for violations of privilege.[110]

73. The risk of legal privilege being violated as a result of cross-border evidence exchange could be limited by:

- Clarifying the obligations on recipients of requests for electronic data regarding to respect legal privilege;
- Training for lawyers on practical mechanisms to ensure privileged communications are not inadvertently collected;
- Where a risk is identified that electronic data may contain privileged materials, LEAs should create independent teams (not connected to the investigation or prosecution) to filter out those materials; and
- Notification obligations and legal remedies where privileged information has been received by LEAs.

H) Trial within a reasonable time

74. The Commission has stated that: "the MLAT process with the US takes an average of 10 months, which is considered as too much time by all stakeholders."[111] All of our survey respondents highlighted the implications of cross-border requests for evidence on the length of the pre-trial proceedings. It can also delay the disclosure of the case file and the trial preparation process, which can have particularly grave implications if the accused is held in pre-trial detention. In Belgium, investigators will take this into account when deciding to request E-evidence. This is also problematic in Estonia, where the casefile is only disclosed at the end of the pre-trial investigation.[112]

---

[104] UK stakeholder, interview.

[105] JUD-IT practitioners' workshop, Anand Doobay, Boutique Law.

[106] Cleary Gottlieb, *Cross-Border Investigations: A Look Back on 2017, and Ahead to 2018*, 15 February 2018, available at: https://www.clearygottlieb.com/-/media/files/alert-memos-2018/crossborder-investigations-a-look-back-on-2017-and-ahead-to-2018-updated.pdf.

[107] Global Investigations Review, *German constitutional court blocks prosecutors from using seized Jones Day documents*, July 27, 2017, (available at https://globalinvestigationsreview.com/article/1145054/german-constitutional-court-blocks-prosecutors-from-using-seized-jones-day-documents).

[108] *SEC v. Herrera*, No. 17-cv-20301 (S.D. Fla. Dec. 5, 2017).

[109] *SFO v ENRC* 8 [2017] EWHC 1017. Currently under appeal.

[110] JUD-IT workshop, Anand Doobay, Boutique Law and Rebecca Niblock, Kingsley Napley.

[111] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 25 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

[112] LEAP survey.

75. Provided that the challenges outlined above are remedied in a satisfactory way, increased efficiency in cross-border electronic data exchange could help to protect fair trial rights (and serve the interests of the defence as well as victims) by speeding up the legal process. It is, however, crucial that the defence is able to use evidence gathering tools with equivalent speed and efficiency to LEAs to obtain electronic data. Furthermore, the increased efficiency gains will not be realised if they are not combined with prompt notification (where possible) and timely disclosure of evidence.

E-evidence and the rule of law

A) Checks on the legality of the actions by law enforcement authorities

76. LEAs do not have unlimited legal powers to obtain electronic data to investigate and prosecute suspected crimes: they are rightly required to operate within the law. Given the implications of electronic data gathering on privacy,[113] powers to interfere with those rights must be prescribed by law.[114] In the context of cross-border evidence exchange, the innovative approaches developed by LEAs to obtain evidence have raised considerable questions about their legality.[115] One of the functions of a fair and open criminal justice system is to expose whether LEAs have exceeded their legal powers. This is required to uphold the rule of law, ensure the fairness of the criminal trial and remove the incentive for LEAs to act outside of the law.

77. Mechanisms to challenge the legality of an LEA's requests for electronic data should exist before the evidence is obtained and shared. There are a number of benefits to assessing legality in advance of the electronic data being requested and shared: it prevents the illegality from occurring (rather than trying to remedy it later); it stops unlawfully obtained evidence making its way into the casefile (resulting in disputes at trial); and it can allow LEAs to find alternative, lawful ways to obtain the electronic data they need. A number of the legal frameworks on evidence exchange explicitly recognise the importance of this right to legal challenge. For example, the Budapest Convention gives the defence a right to challenge the procedure for issuing a request for cooperation.[116]

78. In practice, however, there are considerable challenges to challenging legality at this stage:

- As discussed above, secrecy is frequently applied in this context (often for legitimate law enforcement reasons) and it is impossible for a defendant who does not know about the evidence-gathering to challenge its legality;
- Even where a request is not secret, a defendant and their lawyer will assess whether a challenge at this stage is in their best interests – their goal is not to ensure the legality of LEAs' action but rather to win the case (by, for example, excluding evidence at trial) or resolving the case as quickly as possible (and not delaying the case through interim actions);
- Not all measures for evidence exchange envisage the right to challenge at this stage: the E-evidence Proposal, for example, only envisages a remedy after the evidence has been obtained.[117]

79. Another check on the legality of law enforcement actions in the context of electronic data is the requirement for judicial authorisation, akin to requiring a judicial warrant before searching a house. This is inherent in many cross-border legal mechanisms. For example, the EIO is defined in the EIO Directive as " a judicial decision which has been issued or validated by a judicial authority of a Member State ('the issuing State') to have one or several specific investigative measure(s) carried out in another Member State ('the executing State')."[118] The judge is supposed to ensure the legality of the action and to ensure independent oversight over law enforcement's actions. In

[113] Protected by, for example, Article 8 of the ECHR and Article 7 of the EU Charter.

[114] Cf *Silver and Others v United Kingdom*, 25 March 1983, Series A no. 61.

[115] Cf *United States v. Microsoft Corp*, No. 14-2985 (2d Cir. 2016).

[116] Article 27 of the Budapest Convention.

[117] Article 17 of the E-evidence Proposal.

[118] Article 1 of the EIO Directive; MLA 2000, Article 6.

the words of one participant in the JUD-IT practitioners' workshop: "involving judicial authorities means that you have independent bodies and critical thinkers who may and who should object if things get out of control."[119] Judicial authorisation is not, however, always required. For example, the E-evidence Proposal allows prosecutors to issue orders without judicial oversight (unless these are requesting transactional and content data).[120]

80. In traditional judicial cooperation mechanisms, the involvement of a judicial authority in the state that is asked to gather the evidence may provide an additional check on the legality of the evidence gathering. In the USA for example, where content data is requested from a US-based service provider, prior judicial authorisation in the form of a warrant may be required from a Federal judge.[121] In the context of the E-evidence Proposal, the second judicial authority would be removed, with responsibility for assessing whether there is a risk to the fundamental rights of the investigated person being transferred to the service provider. It is also proposed that, in the context of obtaining content data from US service providers, the requirement for judicial authorisation in the USA would be removed by a combination of recent US legislation,[122] an Executive Order with respect to the USA[123] and an agreement reached between the EU and USA.[124]

81. The final key check on the legality of evidence-gathering by LEAs occurs at trial (or shortly before, after the evidence has been gathered). This is the power for the accused to challenge the admissibility of evidence on which the state is seeking to rely to secure a conviction. In human rights terms this is typically envisaged as a mechanism for ensuring the overall fairness of the proceedings, but it also has an important role in ensuring that the accused is not prejudiced as a result of unlawful activity and in removing incentives for LEAs to violate the law to obtain electronic data. In Belgium, for example, the accused may challenge the validity of evidence and argue for exclusion from the case, but is required to demonstrate that: 1) the order did not comply with the legislation /rules of formal procedure and fundamental rights; and 2) it also violated the rights of the suspect or accused person or that the evidence obtained is inaccurate or is unreliable due to having been obtained illegally.[125]

82. This right is explicitly envisaged in some legal mechanisms on cross border evidence gathering. The E-evidence Proposal, for example, provides:

> *Suspects and accused persons whose data was obtained via a European Production Order shall have the right to effective remedies against the European Production Order during the criminal proceedings for which the Order was issued.*[126]

However, the E-evidence Proposal does not specify the remedies, leaving it up to the Member States to determine in national law the consequences of a violation of the procedural rules in obtaining electronic data.

---

[119] JUD-IT Practitioners workshop, Jun.-Prof. Dr. Dominik Brodowski, Universität des Saarlandes.

[120] Article 4 of the E-evidence Proposal.

[121] JUD-IT practitioner's workshop, Amy Jeffress, Arnold & Porter.

[122] Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018.

[123] *Ibid.*

[124] Explanatory Memorandum, E-evidence Proposal, page 11: "for cases relating to ECPA, access to content data might be prevented in certain situations at present, and MLA should therefore remain the main tool to access such data. However, with the changes brought about by the adoption of the US CLOUD Act; the blocking statute could be lifted if the EU were to conclude an agreement with the US."

[125] LEAP survey.

[126] Article 17(1) of the E-evidence Proposal.

83. In practical terms, this mechanism can be difficult to apply:

- Legal mechanisms for electronic data do not prescribe the remedies that are required where electronic data has been gathered illegally, instead leaving these as a matter for national law;
- Rules on the admissibility of evidence vary considerably across Member States and the practical approach also varies from court to court and judge to judge;
- The trial court will typically make an overall assessment of the fairness of the trial, which may result in a requirement on the accused to demonstrate that their defence rights have been prejudiced by the unlawful actions;
- It may not be known that the evidence-gathering was conducted illegally, whether in violation of the law of the requesting or requested state; and
- The LEA may use illegally obtained electronic data for the purposes of the investigation but then construct a case based on legal evidence that would not otherwise have been obtained – for example, unlawful surveillance could identify that a person is communicating with members of a criminal group resulting in the LEA then undertaking lawful investigative actions to establish criminal activity.[127]

84. "As a criminal defence lawyer, the biggest concern is the lack of legality checks."[128] In order to ensure that there are effective controls on the legality of LEAs' actions in the context of electronic data:

- Limits on the use of secrecy and prompt exchange of evidence are crucial to allow legal challenges: "The ability to challenge the request for data is another issue in the UK, because in order to challenge it you have to be aware of the request and most requests are confidential and service providers have no real interest in notifying customers";[129]
- Clear rights should be given to the accused to challenge the legality of requests for electronic data before a judge;
- Effective oversight by an independent judge should be required before demands for electronic data are issued;
- LEAs should not benefit from illegally obtained evidence in order to secure a conviction and greater clarity is needed in domestic and regional law (particularly within the EU) on the appropriate remedy where E-evidence has been obtained illegally.

B) Systemic oversight

85. Individual cases can provide a snapshot of how electronic data is being gathered; it cannot provide a broader overview of practices. A more systemic overview of how electronic data is being used may, for example, be needed to assess whether there is a basis for concern about a number of the matters discussed below, such as the use of mass fishing expeditions or compliance with requests from states known to pursue politically-motivated prosecutions. Sadly, there is currently very limited public information about the use of these mechanisms:

[127] Human Rights Watch, "Dark Side: Secret Origins of Evidence in US Criminal Cases", January 2018 (available at https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases).

[128] JUD-IT practitioners' workshop, Christophe Marchand, Jus Cogens.

[129] JUD-IT practitioners' workshop, Anand Doobay, Boutique Law.

Data at this level of detail is not collected by public authorities. There is no precise data available on the number of requests for judicial cooperation, direct cooperation, direct access or WHOIS lookups.[130]

86. A requirement to gather and publish data is, however, a feature of more recent legal frameworks on cross border evidence exchange. The EIO Directive, for example, requires a report to be published by the Commission by 2019 "on the application of this Directive, on the basis of both qualitative and quantitative information", although this is a one-off report and is designed for the purposes of evaluating the EIO Directive.[131] The reporting obligations under the E-evidence Proposal are annual and are more substantive. It requires Member States to "collect and maintain comprehensive statistics from the relevant authorities" and prescribes the information that must be provided.[132] It is, however, silent on whether this will result in data being published by the Commission. In addition, a number of service providers opt to publish transparency reports on the electronic data they have shared with LEAs.[133]

87. The greater gathering and sharing of data to provide a systemic picture of how electronic data is being gathered and shared in the E-evidence Proposal should be welcomed as should the voluntary production of transparency reports by service providers. Data provided to the Commission should however be collated and published annually.

C) Proportionality – probable cause

88. Even if LEAs have the legal power to gather electronic data, because of the impact this has on the right to private and family life, these powers should only be used when it is proportionate to do so.[134] One practical aspect of the principle of proportionality is the requirement that there is a sound basis to justify the request for electronic data. A vague and unsubstantiated suspicion that a person may have committed a criminal offence should not be enough. There are good practice examples in this area.

89. For example, in US law a court order is required approving the execution of a request for MLA as a fundamental step to ensure the protection of civil liberties of the suspects of accused persons.[135] This demands that "probable cause" exists, i.e. that specific and articulable facts must be shown to establish that there are reasonable grounds to believe that the contents of the communications are relevant and material to the investigation.[136] Ensuring compliance with these requirements is a key role of the central authority in the USA (the Office of International Affairs) that receives MLA requests.

---

[130] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 13 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

[131] Article 37 of the EIO Directive.

[132] Article 19 of the E-evidence Proposal.

[133] The transparency reports are available online: Google (https://transparencyreport.google.com/), Facebook (https://transparency.facebook.com/), Microsoft (https://www.microsoft.com/en-us/corporate-responsibility/reports-hub), Twitter (https://transparency.twitter.com/en.html) and Apple (https://www.apple.com/privacy/transparency-reports/) .

[134] Guide on Article 8 of the ECHR: Right to respect for private and family life, home and correspondence, ECtHR, August 2018 (available at: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf).

[135] JUD-IT practitioner's workshop, Amy Jeffress, Arnold & Porter.

[136] 18 US Code §2703(d) which requires a court order for the disclosure of contents of an electronic communication.

90. The EIO Directive requires authorities to conduct a proportionality and necessity assessment against the fundamental rights of the defendant before issuing an EIO.[137] The need to establish "probable cause" is not, however, specifically mentioned in the EIO Directive, although it does require that the issuing authorities explain the grounds for the seeking of evidence, a summary of the underlying facts and a description of the offence.[138] Remarkably, the EIO is the first instrument to include a risk to fundamental rights as a legitimate ground to refuse the execution of an EIO: an EIO may be refused in the executing State where "there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter".[139]

91. Sadly, despite the existence of good practice examples, these are not uniformly applied and are under threat. Member States have highlighted the US 'probable cause' evidence requirement as a key obstacle when cooperating with the US in the scope EU-US MLAT, which requires requesting authorities to provide a detailed statement of facts.[140] In a questionnaire leaked by Statewatch, some Member States admitted that in most cases, requests for content data are made during the pre-trial investigation, when the authorities do not have enough information to show "probable cause."[141] Traditional MLA arrangements do not require judicial authorities to establish probable cause. The result is that, in practice, often investigators have a "theory" on a case in the initial stages of the investigation and submit a speculative request in hope that the information they receive will bear out their theory.

92. Courts have not required reasonable cause to be shown when requests for MLA have been challenged. For example, in a judicial review of a letter of request sent by the Director of the Serious Fraud Office (SFO) to the authorities in Monaco, seeking their assistance in relation to a criminal investigation, the UK Court dismissed the claim and held:

> *[A] lthough the [letter of request] does not elaborate on the grounds for suspicion, we do not think that there can be an obligation […] to set out what those grounds were. We add that we would be surprised if there was any such obligation, as the material forming the basis of suspicion may well be sensitive, at least at this early stage of the investigation.*[142]

93. The E-evidence Proposal does not set out an evidential threshold requiring the issuance of an order only when there is reasonable suspicion/probable cause. Instead it refers to general principles of "necessity and proportionality" and requires only that it would be "available for the same criminal offence in a comparable domestic situation in the issuing State. "[143]

---

[137] Article 6 of the EIO Directive.

[138] EIO Directive, Annex 1 (form of EIO).

[139] Article 11(1)(f) of the EIO Directive, JUD-IT Practitioners' workshop, Dr. Marloes van Wijk, University of Maastricht.

[140] Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 24 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN).

[141] Council of the European Union, *Questionnaire in preparation for the workshop on the application of the mutual legal assistance (MLA) and extradition agreements between the European Union and the United States of America (Eurojust, 25-26 October 2012)*, 14253/2/12 REV 2, available at: http://www.statewatch.org/news/2012/nov/eu-council-eu-usa-mlarequests-14253-rev2-12.pdf.

[142] Pragraph 53(iii), judgment of the High Court on *Unaoil and others v. Director of the Serious Fraud Office*, 29 March 2017, 2017 EWHC 600 (Admin).

[143] Article 5(2) of the E-evidence Proposal. See JUD-IT practitioners' workshop, Jens-Henrik Jeppesen, Center for Democracy and Technology (CDT).

94. The absence from the E-evidence Proposal of an equivalent evidential threshold to the "probable cause" requirement in US law has caused considerable concern. Google LLC, for example, has argued:[144]

> *Beyond the safeguards already in the proposal, a material threshold for suspicion of a crime should also be set forth in the Regulation. The Electronic Communications Privacy Act ("ECPA") in the US contains such thresholds. Accordingly, when authorities request an ECPA court order, they must present specific and articulable facts to a judge or magistrate demonstrating that the requested information is relevant and material to an ongoing criminal investigation. When they seek a search warrant, they must meet an even higher burden of proof: demonstrating 'probable cause' to believe that contraband or evidence of a crime is present in the specific place to be searched. Similar thresholds should be set forth in the proposed Regulation.*

95. Although LEAs may find it frustrating, there is a good reason for a certain evidential threshold to be met before electronic data can be gathered. Part of the challenge for LEAs would appear to be the significant legal differences regarding what evidential threshold (if any) must be met and a lack of understanding of the law in the state that is being asked to share evidence. The EU could add significant value in this area by agreeing on minimum EU-wide requirements regarding this evidential threshold (to be applied at least in cross-border requests for evidence sharing). If linked to the US concept of "probable cause" this could facilitate the agreement and operation of any future executive agreement with the US under the CLOUD Act.[145]

D) Proportionality – the fishing expedition

96. Closely linked to the previous discussion is the concern that requests for electronic data could encompass large quantities of data, relating to large numbers of people over a long period of time: fishing expeditions. If LEAs use powers in this way, it would seriously undermine privacy (including the privacy of people who have never been suspected of a criminal offence). We understand from practitioners that, in practice, LEAs do sometimes send very broad requests which can be unlimited as to time and without specifying what is relevant and why it is important for the investigation.[146] In one case considered by the ECtHR, for example, Italy asked San Marino for extensive information (names, bank accounts, etc.) and San Marino executed the requests for 1000 people even though they were not suspects.[147] The ECtHR found this to be a violation of the right to privacy. One participant in the JUD-IT Practitioners' workshop highlighted that the E-evidence Proposal refers to "persons" (in plural):

> *How many people will a single order apply to? Will this allow "thematic warrants"? This is a big issue in the UK in respect of the new Investigatory Powers Act 2016 which allows warrants in respect of the interception of content to be applied to large groups, and then leaves it up to the prosecutor to decide who they want. Would the proposed production order allow this? It appears broad enough to allow for this. And are issuing states going to rely on service providers to do this?*[148]

97. The risk of electronic data requests being used for mass fishing expeditions is considerable. Key safeguards to ensure requests are appropriately targeted include:

---

[144] Google, position paper on E-evidence Proposal, not published.

[145] JUD-IT practitioners' workshop, Professor Peter Swire, Georgia Institute of Technology.

[146] JUD-IT practitioners' workshop, Anand Doobay, Boutique Law.

[147] *M.N. and Others v. San Marino*, no. 28005/12, 7 July 2015.

[148] JUD-IT practitioners' workshop, Caroline Wilson Palow, Privacy International.

- Clearly defined legal limits on the scope of electronic data requests, including a requirement to ensure proportionality, with effective judicial oversight;
- Clear powers for the recipient of a request for electronic data to refuse where this is not proportionate; and
- An obligation to notify as soon as possible people whose personal data has been requested and shared to ensure systemic oversight.

E) Political abuse and oppression

98. During the JUD-IT practitioners' workshop a sobering example was provided of how repressive states can use the collection of electronic data to create a "chilling effect" on civil society:

> *Amnesty went to Belarus to observe how some of the safeguards that were at issue in the case of Zakharov before the ECtHR[149] are observed in concrete terms. When you are in a fairly repressive legal environment, the effect becomes a lot more tangible. The system of direct access to communications data that the authorities have (KGB in this case), issues like data retention, the scope of allocation of the law, the accessibility of the law, authorisation, duration of surveillance, the requirements or a lack thereof for the destruction of data, might seem quite technical and legalistic when you take them as a whole package. However, as established in the ECtHR judgement, when you lack enough of these safeguards and you are in a situation where there is a real lack of clarity as to who can be targeted and when, and there is a widespread suspicion amongst the general public that secret surveillance powers are being abused, the menace of surveillance can be claimed in itself to restrict free communications. Clearly this is an interference with the right to privacy, such that people are constantly afraid of functioning, chilling the ability of ordinary people to live normal lives, and in particular activists.[150]*

In addition to creating a broader climate of fear, there is clear evidence of cross-border criminal justice cooperation tools being used to target exiled human rights activists, dissidents, political opponents and journalists.[151] This can result in arrest, detention and can create considerable political embarrassment for states which inadvertently act on politically-motivated requests for cooperation, undermining trust in the cooperation mechanisms themselves.

99. Many of the formal mechanisms on cross border evidence gathering contain specific language to protect against the misuse of the tools in political cases. For example MLA 1959 includes as a ground under which the authorities of the executing State may refuse assistance "if the request relates to a political offense".[152] Similarly, the Budapest Convention allows the requested State to refuse assistance where the request concerns an offence which the requested Party considers a political offence, or an offence connected with a political offence.[153] Under MLA 2000 the refusal ground relates to an investigation or prosecution which is politically motivated.[154] Some States have introduced specific grounds for refusal to comply with MLA requests in their national law. The UK, for example, would refuse if there are substantial grounds for believing that the request is intended to persecute the investigated person for its race, gender, sexual orientation, religion,

[149] *Roman Zakharov v. Russia [GC]*, no. 47143/06, ECHR 2015.

[150] JUD-IT Practitioners' workshop, Joshua Franco, Amnesty International.

[151] See for example: https://www.fairtrials.org/campaign/interpol.

[152] Article 2 of MLA 1959.

[153] Article 27 (4) of the Budapest Convention.

[154] Article 4(1) of MLA 2000.

nationality, ethnic origin or political opinions or that person's position may be prejudiced for any of those reasons. [155]

100. Mechanisms regulating the exchange of cross border evidence within the EU do not contain the same explicit refusal grounds, presumably on the basis that they operate on the basis of mutual recognition, in a legal area in which political abuse of criminal justice does not happen and in which Member States are bound by the same legal frameworks prohibiting this. The EIO Directive, for example, merely states that Member States can refuse to execute EIOs where "there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter."[156] In the current political climate in Europe, sadly, this cannot be assumed.[157] The E-evidence Proposal also allows the addressee of a production order or a preservation order to oppose enforcement where there it "manifestly violates the Charter" or where "it is manifestly abusive".[158]

101. In the context of systems for direct cooperation with service provides (as under the E-evidence Proposal) an additional concern is the fact the service provider receiving an Order may be ill-placed to refuse to cooperate. In particular, refusing to cooperate with a state's LEAs could make it harder (or impossible) for a business to continue to provide their services in the country in question. This risk was seen by the attempts of the Russian communications regulator to ban use of the encrypted messaging app "Telegram" after it refused the Russian government's demands for backdoor access to private communications.[159]

102. To prevent the risk of abuse, judicial cooperation mechanisms (including those which operate within the EU) should contain clear legal prohibitions on politically-motivated misuse and rights to refuse to execute a request on this basis. In order to overcome practical barriers to enforcing such rules:

- Notification should be given promptly to give an opportunity for an accused (or other person affected by data sharing) to challenge the request for electronic data on political motivation grounds;
- Systematic reporting of how mechanisms are being used in practice could demonstrate cooperation with countries known to abuse criminal justice powers for political purposes, this should include a requirement for private service providers to continue to issue transparency reports; and

[155] United Kingdom Home Office, *Requests for Mutual Legal Assistance in Criminal Matters Guidelines for Authorities Outside of the United Kingdom, 2015, 12th Edition*, London, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf).

[156] Article 11(1)(f) of the EIO Directive.

[157] European Commission, *Communication from the Commission to the European Parliament and the Council, A New EU Framework to strengthen the Rule of Law*, 11 March 2014, COM (2014) 158 final, available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/effective-justice/rule-law/rule-law-framework_en.

[158] Article 14(4)(f) and (5)(e) of the E-evidence Proposal.

[159] The Guardian, "Russia blocks millions of IP addresses in battle against Telegram app", 7 April 2018, available at: https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app.

- Judicial oversight of requests should take place to identify and prevent abuses and should be required in the requested country where a state is known to abuse criminal justice systems for political ends.

F) Electronic data contributes to human rights abuses

103. A fair criminal justice system does not support respect for the rule of law if it contributes indirectly to other human rights abuses. In the context of cross-border E-evidence exchange, there are a number of ways in which this might occur. Press freedom could be violated where, for example, LEAs gather E-evidence to identify a journalistic source, which has been recognised as "one of the basic conditions for press freedom".[160] There are also concerns in relation to issues such as freedom of speech, where for example a country criminalises speech which others would consider lawful:

> *Do we want the most restrictive European regimes to dictate what can be said and what cannot be said in Europe? For example, in the context of the Catalonian independence movement, in Spain you cannot write freely about it, but if you have a website somewhere in Europe and write about it you are safe. However, with this new legislation the ISP has to hand over your subscriber information. There are also issues in relation to election polls, as some countries criminalise the updating of polls during election day. Another area of concern is in respect of the criminalisation of abortion in some countries like Poland, or migration in Hungary.*[161]

104. Electronic data that is gathered and shared with requesting states could also contribute to activities which violate human rights. For example, this could be shared with LEAs who use the evidence to inform questions asked during the torture of a suspect or witness. Furthermore, electronic data could form the basis of criminal conviction for which the death penalty is imposed.[162]

105. The key tool available to protect against these risks in MLA and other cooperation arrangements is refusal by the country receiving the request to comply with it. This is sometimes encompassed within the general concept that the receiving country need not comply where it would be contrary to "its applicable legal principles, including where execution of the request would prejudice its sovereignty, security or *ordre public* or other essential interests."[163] This is also protected as a result of the power for states to require the offence to which the request related to be an offence in both countries.[164]

106. The approach has differed in EU cooperation mechanisms. The EEW Framework Decision, for example, contains a general provision calling on Member States to respect their obligation under Article 6 ECHR (right to a fair trial) when issuing and executing an EEW, but it certainly did not explicitly include the risk to fundamental rights as a legitimate ground to refuse the execution of

---

[160] Cf *Goodwin v. the United* Kingdom, ECtHR, App. No. 17488/90.

[161] JUD-IT practitioners' workshop, Alex de Joode, Nederland ICT (representing EuroISPA).

[162] *Soering v United Kingdom*, ECtHR, Application no. 14038/88.

[163] EU/US MLAT, Article 1.

[164] Article 29(4) of the Budapest Convention, for example, provides: "A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled."

a warrant.[165] The EIO Directive, in contrast, includes as an explicit ground for refusal where the executing Member State has substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the EU Charter.[166] The EIO Directive does not, however, contain robust safeguards on dual criminality, only allowing this as a right for refusal where "the EIO relates to a criminal offence which is alleged to have been committed outside the territory of the issuing State and wholly or partially on the territory of the executing State".[167]

107. In the context of direct cooperation with service providers, protecting against electronic data contributing to the violation of other human rights is more complex, since there is only one issue authority involved. The E-evidence Proposal, for example, recognises the right of the service provider to refer a case to the "competent enforcement authority" where "it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive".[168] In practical terms, however, it would be difficult for the service provider to make a meaningful assessment of this given that it can only make this decision "based on the sole information contained in the [order]".[169] Furthermore it is currently proposed that it would have very limited timeframes within which to make this assessment (10 days or 6 hours in urgent cases).[170] There are considerable questions about the institutional capacity of the service provider to perform this important role: they are not independent judicial authorities, experts on human rights or on law and practice in the issuing Member State, and (as discussed above) may have commercial interests which conflict with the proper exercise of this function.[171]

108. In order to ensure that the collection and exchange of electronic data does not result in other human rights violations, we recommend that:

- The ability for receiving states to refuse to cooperate where requirements of dual criminality are not met, except in the context of generally recognised serious offences;[172]
- Requests to gather and share electronic data should be accompanied by sufficient information to enable the recipient to make a meaningful assessment: such as information on the likely sentence if a person is convicted and on the nature of the offence;
- People affected by electronic data requests are notified in advance of the evidence gathering (when possible) and given an opportunity to challenge the request on human rights grounds; and
- Systemic information is published about the use of electronic data requests including details on the requesting country, the nature of the offence and decisions made to refuse cooperation on human rights grounds.

[165] Article 1(3) of the EEW Framework Decision.

[166] Articles 1(4), 6(1) (a), and 11 (1) (d) and (f) of the EIO Directive.

[167] Article 11(1) (e) of the EIO Directive.

[168] Article 9(5) of the E-evidence Proposal.

[169] Article 9(5) of the E-evidence Proposal.

[170] Article 9(1) and (2) of the E-evidence Proposal.

[171] Google LLC, for example, has however supported the right for service providers to raise alarms when a request violates fundamental rights or procedural safeguards.

[172] Cf the approach taken in the Framework Decision on the European Arrest Warrant, 2002/584/JHA, Article 2(2).

Conclusions and recommendations

109. There is no doubt that the cross-border gathering and exchange of evidence is crucial to effective law enforcement. It also, however, raises considerable challenges for the fairness of criminal justice systems, both from the perspective of the accused and of the rule of law in general. Although new legal proposals in this area (notably the E-evidence Proposal) create new and different challenges, it is clear that the current systems are not operating perfectly from the perspective of fairness.

110. In outline, key areas of concern in relation to existing and proposed law and practice include:

- Threats to the ability of the accused to prepare their defence on the basis of procedural equality, arising from *inter alia*:
  - The inability of the defence to use cross border evidence gathering tools in practice;
  - Practical challenges for the defence in understanding and processing large quantities of electronic data (often provided late in the criminal proceedings);
- The difficulty in holding LEAs to account for unlawful or disproportionate uses of cross border evidence gathering tools, arising from *inter alia*:
  - The fact that electronic data requests will frequently be secret (often for legitimate reasons), making legal challenges difficult;
  - A lack of timely disclosure of evidence and about the use of these tools in individual cases and at a systematic level;
- Difficulties in preventing politically-motivated abuse of cross border evidence gathering tools and in ensuring that electronic data does not result in violations of other human rights, exacerbated in the context of increased direct cooperation with service providers due to the removal of oversight by an independent body in the executing country.

111. Key recommendations made throughout this paper to mitigate these key risks include:

Recommendation	**Risk(s) mitigated**
A presumption of prior notification of people whose personal data is being gathered (rebuttable only where clear justifications are provided) and, where this is not possible, prompt ex-post notification.	• The defence cannot challenge the legality of cross border evidence gathering. • The accused does not have the time and information to prepare the defence.
Ensuring electronic data of relevance to the accused is included in evidence gathering (or preservation) by LEAs.	• Exculpatory electronic data is lost or deleted due to delays.
Prompt disclosure of electronic data to the defence with sufficient time for the defence to process electronic data and request exculpatory materials.	• The accused does not have the time and information to prepare the defence. • Vast quantities of electronic data are dumped on the defence shortly before trial. • Exculpatory electronic data is lost or deleted due to delays.

Clear powers for the defence to use cross border evidence gathering powers on equal terms with prosecutors.	• The accused does not have the time and facilities to prepare the defence on an equal basis with the prosecution.
A right for the defence to challenge the admissibility and probity of electronic data.	• LEAs act outside of the law undermining the fairness of the trial and the rule of law.
The ability for the defence to appoint lawyers in the prosecuting country and the country which is the source of electronic data.	• The defence is unable to assess whether electronic data was gathered lawfully and how exculpatory evidence can be obtained.
Funding for the defence to acquire the tools needed to process electronic data, specialist training for defence lawyers and mechanisms to enable lawyers to access technical expertise.	• The accused does not have the facilities to prepare the defence. • The defence cannot understand and process large quantities of electronic data.
Protections in law and practice against electronic data including legally privileged materials.	• The right of the accused to confidential communication with their lawyer is undermined.
Judicial authorisation before requests or orders for electronic data are issued.	• Inappropriate uses of electronic data are not identified by an independent arbiter.
Greater clarity on the appropriate legal remedies where electronic data has been obtained illegally.	• There is no disincentive for LEAs to avoid inappropriate use of cross border evidence gathering tools.
LEAs, the Commission and service providers should publish data regularly on the use of cross border evidence gathering tools.	• It is impossible to understand how mechanisms are being used in practice, including to identify misuse and ensure accountability.
A requirement for an appropriate evidential test to be passed before cross border evidence gathering tools can be used and for requests for electronic data to be limited in scope.	• Cross border evidence gathering tools are used disproportionately, undermining the right to privacy.
Meaningful powers for those receiving electronic data requests (whether LEAs or service providers) to refuse to comply where the requests are disproportionate, politically-motivated or would violate human rights.	• Cross border evidence gathering tools undermine the rule of law, are used in politically-motivated cases and in ways which violate human rights. • Trust in service providers and in cross border evidence gathering mechanisms is threatened.
A requirement for requests for electronic data to contain sufficient information to enable those receiving them to decide whether it is appropriate to comply.	• The entity receiving the request does not have the information it needs to assess legality, proportionality and human rights.

References

Table of Cases:

European Commission of Human Rights:

Goodwin v. the United Kingdom, no. 17488/90.

European Court of Human Rights:

Barberà, Messegué and Jabardo v. Spain, 6 December 1988, Series A no. 146.

Bulut v. Austria, 22 February 1996, Reports of Judgments and Decisions 1996-II.

Dayanan v. Turkey, no. 7377/03, 13 October 2009.

Edwards v. the United Kingdom, 16 December 1992, Series A no. 247-B.

Foucher v. France, (1997), 18 March 1997, Reports of Judgments and Decisions 1997-II.

Kuopila v. Finland, no. 27752/95, 27 April 2000.

M.N. and Others v. San Marino, no. 28005/12, 7 July 2015.

Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015.

Sabayev v Russia, no. 11994/03, 8 April 2010.

Salov v Ukraine, no. 65518/01, ECHR 2005-VIII (extracts).

Samokhvalov v Russia, no. 3891/03, 12 February 2009.

Silver and Others v United Kingdom, 25 March 1983, Series A no. 61.

Soering v. the United Kingdom, 7 July 1989, Series A no. 161.

Court of Justice of the European Union:

Case C-216/18, PPU *Minister for Justice and Equality v. LM* (Deficiencies in the system of justice), Court judgment of 25 July 2018 (Grand Chamber).

Belgium:

Hof van Cassatie of Belgium, *YAHOO! Inc.*, No. P.13.2082.N of 1 December 2015. Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016.

United Kingdom:

SFO v ENRC 8 [2017] EWHC 1017.

Unaoil and others v. Director of the Serious Fraud Office, 29 March 2017, 2017 EWHC 600 (Admin).

United States:

Facebook v Hunter, Facebook, Inc. v. Superior Court, 240 Cal. App. 4th 203 (2015).

SEC v. Herrera, No. 17-cv-20301 (S.D. Fla. Dec. 5, 2017).

United States v. Microsoft Corp, No. 14-2985 (2d Cir. 2016).

Legal documents:

Council of Europe:

Convention on Cybercrime, 2001, ETS No 185.

European Convention on mutual assistance in criminal matters Council of Europe 1959, ETS No.030.

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

European Union:

Agreement on mutual legal assistance between the European Union and the United States of America, [2003] OJ L181.

Agreement between the European Union and Japan on mutual legal assistance in criminal matters, [2010] OJ L39.

Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Council of the European Union, Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, [2000] OJ C 197.

Council of the European Union, Council Framework Decision 2002/584 on the European Arrest Warrant and the Surrender Procedures between Member States, [2002] OJ L 190.

Council of the European Union, Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, [2008] OJ L 350.

Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, [2012] OJ L 142.

Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, [2013] OJ L 290.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, [2014] OJ L 130.

Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (European Parliament) (Council of the European Union) 2014/104/EU, [2014] OJ L 349.

Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, [2016] OJ L 65.

Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, [2016] OJ L 132.

Directive (EU) 2016/1919 of the European Parliament and od the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, [2016] OJ L 297.

Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, 17 October 2018, 12113/1/18/REV 1.

Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, [2009] OJ 2009/C 295/01.

Untied States:

Clarifying Lawful Overseas Use of Data (“CLOUD Act”), S. 2383, H.R. 4943.

Stored Communications Act (“SCA”), codified at 18 U.S.C. Chapter 121, §§ 2701–2712.

Other:

Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).

Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969.

UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

Official documents:

Council of the European Union, *Questionnaire in preparation for the workshop on the application of the mutual legal assistance (MLA) and extradition agreements between the European Union and the United States of America (Eurojust, 25-26 October 2012)*, 14253/2/12 REV 2, available at: http://www.statewatch.org/news/2012/nov/eu-council-eu-usa-mlarequests-14253-rev2-12.pdf.

European Commission, *Communication from the Commission to the European Parliament and the Council, A New EU Framework to strengthen the Rule of Law*, 11 March 2014, COM (2014) 158 final.

European Commission, *Rule of law framework. In a crisis, the Commission can trigger the rule of law framework to address systemic threats in EU countries,* available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/effective-justice/rule-law/rule-law-framework_en.

European Commission, *Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings Commission Impact Assessment*, Brussels, 17.4.2018, SWD(2018) 118 final.

European Court of Human Rights, *Guide on Article 8 of the ECHR: Right to respect for private and family life, home and correspondence*, August 2018, available at: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

United Kingdom Home Office, *Requests for Mutual Legal Assistance in Criminal Matters Guidelines for Authorities Outside of the United Kingdom, 2015, 12th Edition*, London, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf.

United Nations Human Rights Committee, *General Comment No. 32*, Article 14: Right to equality before courts and tribunals and to a fair trial, CCPR/C/GC/32, 21 August 2007.

United States Department of Justice (DOJ) and Administrative Office of the U.S Court (AO) Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG), *Recommendations for Electronically Stored Information (ESI) Discovery Production on Federal Criminal Cases*, February 2012, available at: http://www.uscourts.gov/sites/default/files/finalesiprotocolbookmarked.pdf

Mutual Legal Assistance Convention of 1959, Explanatory Report, available at http://www.worldlii.org/int/other/COETSER/1959/3.html.

Position papers, articles, and transparency reports:

Apple, *Report history*, available at: https://www.apple.com/privacy/transparency-reports/.

Carrera, S., Gonzalez-Fuster, G., Guild, E., Mitsilegas, V., *Access to Electronic Data by Third-country Law Enforcement Agencies, Challenges to the Rule of Law and Fundamental Rights*, Centre for European Policy Studies, 2015, Brussels.

Cleary Gottlieb, *Cross-Border Investigations: A Look Back on 2017, and Ahead to 2018*, 15 February 2018, available at: https://www.clearygottlieb.com/-/media/files/alert-memos-2018/crossborder-investigations-a-look-back-on-2017-and-ahead-to-2018-updated.pdf.

Electronic Frontier Foundation, *A Constitutional Conundrum That's Not Going Away – Unequal Access to Social Media Posts, 31 May 2018*, available at: https://www.eff.org/deeplinks/2018/05/ca-supreme-court-leaves-scales-tipped-prosecutions-favor-defense-gets-access.

European Digital Rights (EDRi), EU 'e-evidence' proposals turn service providers into judicial authorities, 17 April 2018, available at: https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/.

European Union Agency for Fundamental Rights, *Data retention across the EU*, available at: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention.

Facebook, *Facebook Transparency Report*, available at: https://transparency.facebook.com/.

Global Investigations Review, *German constitutional court blocks prosecutors from using seized Jones Day documents*, July 27, 2017, (available at https://globalinvestigationsreview.com/article/1145054/german-constitutional-court-blocks-prosecutors-from-using-seized-jones-day-documents).

Google, Position on the E-evidence Proposal, not available online.

Google Transparency Report, *Sharing data that sheds light on how the policies and actions of governments and corporations affect privacy, security and access to information*, available at: https://transparencyreport.google.com/.

Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases*, January 2018, available at: https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

Microsoft, *The eEvidence Proposal – A positive step forward*, 18 April 2018, available at: https://blogs.microsoft.com/eupolicy/2018/04/18/the-eevidence-proposal-a-positive-step-forward/.

Microsoft, *Reports hub*, available at: https://www.microsoft.com/en-us/corporate-responsibility/reports-hub.

Mitsilegas, V., *The Symbiotic Relation Between Mutual Trust and Fundamental Rights in Europe's Area of Criminal Justice*, New Journal of European Criminal Law, Volume 6, 476, 2015, (available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2632892).

Mrčela, M. , *Adversarial principle, the equality of arms and confrontational right – European Court of Human Rights recent jurisprudence*, Vol 1 (2017) Procedural Aspects of EU law, 2017, available at https://hrcak.srce.hr/ojs/index.php/eclic/article/view/6519)

The Guardian, *Russia blocks millions of IP addresses in battle against Telegram app*, 7 April 2018, available at: https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app.

Twitter transparency report, available at: https://transparency.twitter.com/en.html.

Van Wijk, M.C., *Cross-border evidence gathering: equality of arms within the EU?*, 2017, The Hague: Eleven International Publishing.

ANNEX 1: LEAP Survey

Personal details

1. Name *
2. Surname *
3. Email address *
4. Country of expertise *
5. Professional background *
6. Number of years of experience *

Requesting cross-border digital data

If you have experience with making a cross-border request for digital data through a MLAT, in particular with the United States and/or Japan, the EIO and/or outside MLA channels, please specify the following:

7. The scope of the request (e.g. communications metadata, content of communications):*
8. The process to make such a request:
9. At what stage in the criminal proceedings the request was made: *
10. The grounds for the request and conditions that the request must meet: *
11. How long it took for the data to be obtained: *
12. Based on your experience, what are the prospects of a cross-border request for digital data made on behalf of the suspect/accused person being granted? *
13. In practice, what are the main obstacles for defence practitioners seeking to obtain cross-border digital data? Where possible, please refer to practical examples. *
14. In your view, how can access to cross-border digital data support the defence of the suspect or accused person? Where possible, please refer to practical examples. *

Challenging cross-border digital data

If you have experience challenging a cross-border request for digital information that was made by the investigating or prosecuting authorities based on a MLAT, EIO and/or outside MLA channels, please respond to the following questions.

15. Did you challenge the request by way of an action brought in the issuing State, the executing State, or both? * (Mark only one)
    - Issuing State

- Executing State
- Both
- I did not challenge the request

16. What was the procedure for bringing the challenge? *
17. At what stage can a challenge be brought (e.g. only before the requested data is sent to the requesting state)? *
18. What are the available remedies if such a challenge is successful? *
19. At what stage in the criminal proceedings are you made aware that an MLAT/EIO request has been issued? *
20. In your jurisdiction, what are the possible grounds to challenge a request for cross-border access to digital information? Please specify if there is any distinction between the grounds for challenging the issuance and the execution of such a request. *
21. In your experience, what are the practical difficulties in challenging a request for cross-border digital data made by the investigating or prosecuting authorities? Where possible, please refer to practical examples. *

The impact of cross-border digital data requests on the pre-trial procedure

22. What is the impact of cross-border digital requests on the pre-trial procedure (e.g. the length of pre-trial detention, the size of the case file, impact on legal fees and expenses)? *

ANNEX 2: JUD-IT Practitioners' workshop

JUD-IT PRACTITIONERS' WORKSHOP ON CROSS-BORDER EVIDENCE GATHERING Tuesday 3 July 2018, at 12.00 – 18.00 Arnold & Porter, 1 rue du Marquis, 1000 Brussels

Fair Trials organised a practitioners' workshop as part of an EU-funded research project, coordinated by the Centre for European Policy Studies, on the implementation of the European Investigation Order and the EU/US Mutual Legal Assistance Treaty.

The purpose of the workshop was to bring together experts in cross-border evidence gathering from academia, the legal profession and civil society (including industry) to share experiences and perspectives and identify the fundamental rights risks that arise in the context of cross border evidence gathering mechanisms, and any specific concerns in relation to electronic data.

The workshop has informed Fair Trials' policy paper on the impact of judicial cooperation and law enforcement access to electronic data on the procedural rights of defendants to help guide the JUD-IT research, as well as Fair Trials' position in respect of the new EU legislative proposals in relation to electronic evidence.

The discussion paper, agenda and meeting notes from the JUD-IT Practitioners' workshop will be made available on Fair Trials' website at www.fairtrials.org.

Attendees:

Surname	Name	Organization
Baudrihaye-Gérard	Laure	Fair Trials
Brodowski	Dominik	Universität des Saarlandes
Bunche	Ralph	Fair Trials
Bunyan	Tony	Statewatch
Campagna	Achille	Studio Legale Campagna
Cossette	Lani	Microsoft
De Joode	Alex	Nederland ICT (representing EuroISPA)
Dolle	Frederieke	Prakken d'Oliviera
Doobay	Anand	Boutique Law LLP

Surname	Name	Organization
Fernandez Perez	Maryant	European Digital Rights (EDRi)
Franco	Joshua	Amnesty International
Jeffress	Amy	Arnold & Porter
Jeppesen	Jens-Henrick	Centre for Democracy & Technology
Legrand	Emmanuelle	European Commission (DG JUST)
Lorenzo Perez	Silvia	Fair Trials
Marchand	Christophe	Jus Cogens avocats-advocaten
Matt	Holger	European Criminal Bar Association
McNamee	Joe	European Digital Rights (EDRi)
Niblock	Rebecca	Defence Extradition Lawyers Forum
Russell	Jago	Fair Trials
Shaeffer	Rebecca	Fair Trials
Stefan	Marco	CEPS
Swire	Peter	Georgia Tech *Joining remotely*
Tehver	Jaanus	Tehver & Partners
Trenor	Sofia	Amazon
Vamos	Nick	Peters & Peters

Surname	Name	Organization
Van De Heyning	Catherine	University of Antwerp/Eubelius Law firm
Van Wijk	Marloes	University of Maastricht
Vazquez Maymir	Sergi	Vrije Universiteit Brussel
Van Ballegooij	Wouter	European Parliament, Directorate-General for Parliamentary Research Services
Wilson Palow	Caroline	Privacy International

ANNEX 3: Interview questions

Interview questions for criminal defence practitioners

1. What were your frustrations about the pre-OIA reform system and what improvements have you seen in practice since the OIA reform?
2. What happens when you receive a request from an EUMS: what do you need to know from the issuing country?
3. What are the grounds for refusal to execute request and what steps do you take to refuse a request?
4. What steps do you need to take to execute a request? Do you give specific instructions to the IT company and check the data before it goes out to the requesting country?
5. Do requests for e-evidence cover both inculpatory and exculpatory data?
6. Do you assess any gag order requests? Do you know to what extent the person whose data is being requested is aware of the request?
7. Please identify particular challenges vis a vis EUMS?
8. What are your views on direct cooperation by service providers: do you get informed when direct cooperation requests are made ex-ante or ex-post? Do service providers ask you for guidance on whether to execute them?
9. What experience do you have (if any) of receiving requests for defence purposes?
10. Do you find that requests from EU MS have adequate specificities? If not, what steps do you take to clarify the request and how long does the process take before you're in a position to execute the request? Do you regularly engage in direct communications with your counterparts from the issuing country?

Interview questions for US stakeholders

MLAT requests from US to EU:

1. Number of MLAT requests made by the US to EUMS (overall/e-data)?
2. To what extent is the DoJ involved in facilitating the collection of e-evidence from abroad on behalf of defence practitioners?
3. If so, in what types of cases?
4. If not, how do you explain? How might the defence get hold of evidence?
5. Are you involved in letters rogatory by US defence attorneys directed at EU countries?
6. How is notice to the defence handled?
7. To what extent can the defence challenge the issuing of requests?
8. When collecting data, what is the process to review the data that is handed over?

9. What is the process where there is exculpatory data?

10. Is there a process in respect of legally privileged correspondence?

11. Timeframes for discovery?

12. What happens to unused data?

MLAT requests from the EU to the US

1. Number of MLAT requests from the EU to the US (overall/e-data)?

2. Scope of the requests (content data, metadata)?

3. Reasons to exclude requests?

4. To what extent is there room for improvement in terms of EU standards in criminal procedure?

5. What's the process – OIA rejects request, or DC magistrate judges?

6. To what extent do the courts use their inherent power to try to push the government to either forgo obtaining certain evidence or limit its request to core, essential evidence to ensure that requests are processed expeditiously and are answered as quickly as possible?

7. To what extent can the defence challenge the execution of requests?

Legislative developments:

1. Changes foreseen with the Cloud Act?

2. How are colleagues from EU MS reacting to the Cloud Act allowing US law enforcement to compel US based technology companies to provide data even if stored in the EU?