FAIR TRIALS' CONSULTATION PAPER ON E-EVIDENCE

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 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.

In Europe, Fair Trials coordinate the Legal Experts Advisory Panel (LEAP) – the leading criminal justice network in Europe consisting of over 200 criminal defence law firms, academic institutions and civil society organisations. More information about this network and its work on the right to a fair trial in Europe can be found at: www.fairtrials.org/legal-experts-advisory-panel.

@fairtrials @fairtrials Fair Trials fairtrials.org

Contents

Contact:

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

Published in 2019

This publication was funded by the European Union's Justice Programme (2014–2020). The content of this report represents the views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Executive summary

Faced with increasing use of electronic evidence in the context of criminal investigations, both the US and the EU have expressed the willingness to modernise the tools enabling cross-border access to electronic data for law enforcement authorities, and to cooperate further in the exchange of electronic data. This is an opportunity for the EU and the US to set a gold standard for the world.

It is proposed that the new form of cooperation would, effectively, enable law enforcement authorities directly to seek the preservation or production of electronic data held by private companies overseas. Given the impact of cooperation measures on human rights, it will be crucial for the fair long-term functioning of any future mechanism that it is underpinned by human rights protections. To date, this has been recognised by vague and uncertain principles, but any failure to ensure adequate human rights protections is likely to have a negative impact on the fairness, effectiveness and long-term sustainability of the new mechanism. We recognise the concerns expressed by other stakeholders about the rationale itself of the proposed new mechanism, but in view of the political pressure to make this happen, we would like to focus on four key safeguards required to preserve the fundamental fair trial protections for people accused of crime:

Prior notification to the suspect: In criminal trials, where the prosecution has 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 that the accused has a genuine opportunity to obtain evidence to support its defence, prepare and present their case, and contest evidence put before the court, on equal footing with the prosecution. However, this is threatened by (inter alia) the lack of notification about the gathering of data. Although we recognise that specific stages of some investigations may, exceptionally, require secrecy, notification is key to enable challenges to requests and ensure that evidence supporting a person's innocence is preserved as is other evidence.

Robust prior judicial authorisation procedure: In view of the implications of the new tools on privacy and other fundamental rights, the new tools must require that law enforcement authorities meet a sufficiently high threshold in terms of suspicion of criminality (and the severity of the offence) as well as the relevance and materiality of the evidence sought, before they can request or obtain and share electronic data. In addition, requests must be subject to prior meaningful judicial oversight to avoid overbroad and disproportionate requests being issued.

Meaningful remedies in the event of a trial: A key check on the legality of evidence-gathering by law enforcement authorities 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. The accused person must have the right to challenge the request and use of data at trial, and seek specified appropriate legal remedies where electronic data has been obtained illegally. And in order to be in a position to exercise the right to challenge, accused persons must be able to obtain disclosure of the sources of the electronic evidence.

Effective and systemic oversight on the use of the measures by law enforcement authorities: If the new tools are used fairly and proportionately, they are more likely to maintain public trust in criminal justice systems and law enforcement authorities. Effective oversight mechanisms will ensure that we insulate against the risk of improper use, and help protect both the reputation of legitimate law enforcement activity and those who could become victims of abuse of the tools.

Background

1. Further to the 2015 European Agenda on Security which identified cross-border access to electronic evidence as an obstacle to investigations into cyber-enabled crimes,[1] the European Commission (**Commission**) presented on 17 April 2018 a proposal for a Regulation on European Production and Preservation orders for electronic evidence in criminal matters (the proposed **E-evidence Regulation**) and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (together, the **E-evidence Package**).[2] The proposal is being discussed at the European Parliament Committee on Civil Liberties, Justice and Home Affairs (**LIBE Committee**).

2. The proposed E-evidence Package aims to lay down "the rules under which an authority of a Member State may order a service provider offering electronic communications and other information services[3] in the Union, to produce or preserve electronic evidence, regardless of the location of the data".[4] Two new tools (the European Production Order and the European Preservation Order) would enable investigating authorities to require the production or preservation of electronic data from service providers established in another Member State or outside the EU, but offer electronic communication services in the EU, without the involvement of the authorities in the country where the service provider is located. It is proposed that service providers may oppose the enforcement of a European Production Order in the state where they are based only in specified circumstances.

3. The E-evidence Package needs to be analysed in parallel with US legislative developments. The US Congress adopted on 23 March 2018 the Clarifying Lawful Overseas Use of Data (**CLOUD Act**) which, amongst other things, allows for the conclusion of 'executive agreements' with foreign 'governments', on the basis of which US service providers would be allowed to share content data directly with these foreign governments – lifting the existing prohibition[5] on service providers from disclosing content data to foreign law enforcement authorities.[6]

4. Fair Trials is an independent and non-partisan non-governmental organisation. With offices in Brussels, London and Washington DC, Fair Trials has developed in-depth expertise on the functioning of cross-border cooperation mechanisms in criminal justice matters. We recognise the need for efficient cross-border cooperation between judicial authorities. In line with our mission, we focus on the human rights concerns raised in the context of the current proposal to facilitate cross-border access to electronic evidence and the impact which the adoption of the E-evidence Package in its current form may have for the rights of persons whose data are being gathered, shared and potentially used as evidence on which to base a conviction in criminal proceedings.

1 The European Agenda on Security, 28 April 2015, COM(2015) 185 final (available here).
2 Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. On 7 December 2018, the Council agreed a general approach and proposed a revised draft Regulation.
3 Defined in Article 2(3) of the E-evidence Regulation.
4 Article 1 of the proposed E-evidence Regulation.
5 Pursuant to the Electronic Communications and Privacy Act 1986 (**ECPA**, the US "blocking statute").
6 On 5 February 2019, the Commission issued a Recommendation for a Council decision to launch negotiations between the EU and the US for an agreement on cross-border access to electronic evidence directly from service providers for use in criminal proceedings. An executive agreement between the US and the EU could address the potential conflict of law for US service providers between an order to share content data under the E-evidence Regulation and the US blocking statute.

Introduction

5. 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. 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 law enforcement authorities and used as evidence in criminal proceedings. According to the Commission, electronic evidence in some form is relevant in around 85% of total criminal investigations.[7] That electronic data may be stored or held by a company in a country other than where the criminal investigation is taking place.

6. Currently, law enforcement authorities (police, prosecutors, investigating judges) can turn to a range of tools to gather objects and information, including electronic data, located abroad that may later be used as evidence at trial. There are formal cross border judicial cooperation mechanisms in evidence gathering – including mutual legal assistance treaties (**MLATs**) between the EU or its Member States and third countries and international agreements. There are also EU instruments for cooperation between EU Member States.[8] Moreover, prosecuting and judicial authorities may seek to obtain electronic data directly from the private companies that hold it, through a power under national law or even outside any formal legal framework.

7. As expressed in its Explanatory Memorandum to the E-evidence Package, the Commission considers that the current legal framework is "fragmented" and that there is a need to put forward a new obligation on service providers to respond to EU law enforcement requests. The proposed E-evidence Regulation seeks to introduce a new tool for law enforcement authorities to obtain electronic data from service providers who are established in another Member State or even in non-EU Member States, but offer services in the EU, without the involvement of the authorities in the country where the service provider is established or represented. The scope of the proposal would be limited to stored data and does not extend to real time interception. However, the new tool would cover both metadata and content data.[9]

8. With many of the world's largest tech companies based in the US (including Google, Amazon, Facebook, Apple and Microsoft), one of the aims of the Commission's proposal is to secure EU law enforcement authorities' access to electronic evidence that is held by service providers operating under US jurisdiction. However, although US service providers are permitted to cooperate directly with European public authorities with regard to non-content data on a voluntary basis, they are prohibited from sharing content data with foreign law enforcement authorities.[10] There is a clear conflict of law for US companies with a presence in the EU between the obligation to comply with a request under the proposed EU Production Order for content data and the prohibition to share data with foreign law enforcement agencies under US law. In this respect, a cross-Atlantic agreement, whether in the form of an executive agreement as foreseen by the CLOUD Act or another form, is a central component of the equation.

9. Law enforcement authorities have an understandable need for modern tools to enable them to collect the digital evidence that they need to investigate and prosecute crime. Yet 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 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). Key fair trial principles apply in the digital world in the same way as they do in the physical world.

10. Fair Trials welcomes the concerns voiced by experts and civil society representatives[11] and seeks to bring into the debate the principles of fair criminal justice, while recognising that the E-evidence Package and CLOUD Act raise a wider range of issues[12] starting with the appropriateness of its legal basis.[13] The aim of this paper is, therefore, to outline four key sets of safeguards that any new cooperation mechanism for cross-border access to electronic data needs to integrate in order to uphold the fairness of criminal proceedings, and, ultimately, function effectively in the long term:

    - First, the principle of notification to the suspect of the request for data unless a gag order is justified on an exceptional basis;
    - Second, safeguards before data is gathered and transferred to the requesting state (ex-ante safeguards);
    - Third, making it possible for the person whose data has been disclosed to challenge the request, make requests for data and obtain remedies after the data has been transferred to the requesting state (ex-post safeguards); and
    - Fourth, implementing an effective oversight mechanism over law enforcement authorities' use of the new tool, and of the data obtained.

7 Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 14 (available here).
8 In particular, the European Investigation Order, which EU Member States were due to implement by 22 May 2017.
9 Article 2(7)-(10) of the E-evidence Regulation distinguishes between four types of data: (i) subscriber data (relating to the identity of the subscriber and the type of service) (ii) access data (related to the commencement and termination of a user access to a service; (iii) transactional data (context or additional information about the service, such as data on the location of the device used to access the service); and (iv) content data (any stored data in a digital format such as text, voice, videos, images and sound).
10 Pursuant to Section 2701(2) of the Electronic Communications and Privacy Act 1986 (ECPA).
11 See, for instance, the letter of 5 December 2018 from 18 civil society organisations, including Fair Trials.
12 In particular, this paper does not seek to address the considerable implications of cross-border electronic data exchange on privacy or legal professional privilege.
13 See, for instance, the report from CEPS (available here) as well as the comments from the Meijers Committee (available here), CCBE (available here) and ECBA (available here).

Figures: Current and proposed mechanisms[14]

Figure 1: MLA arrangements

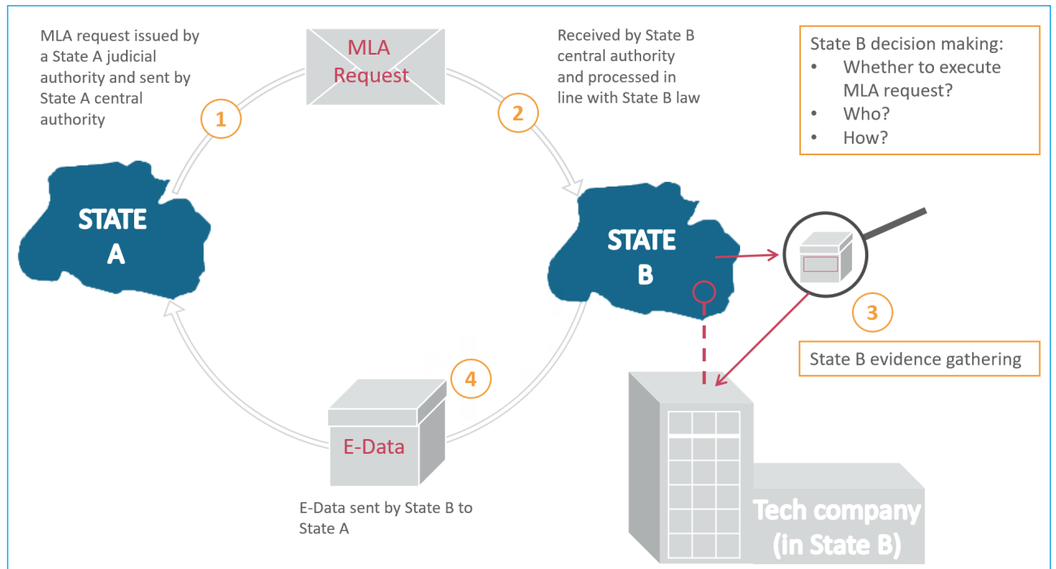
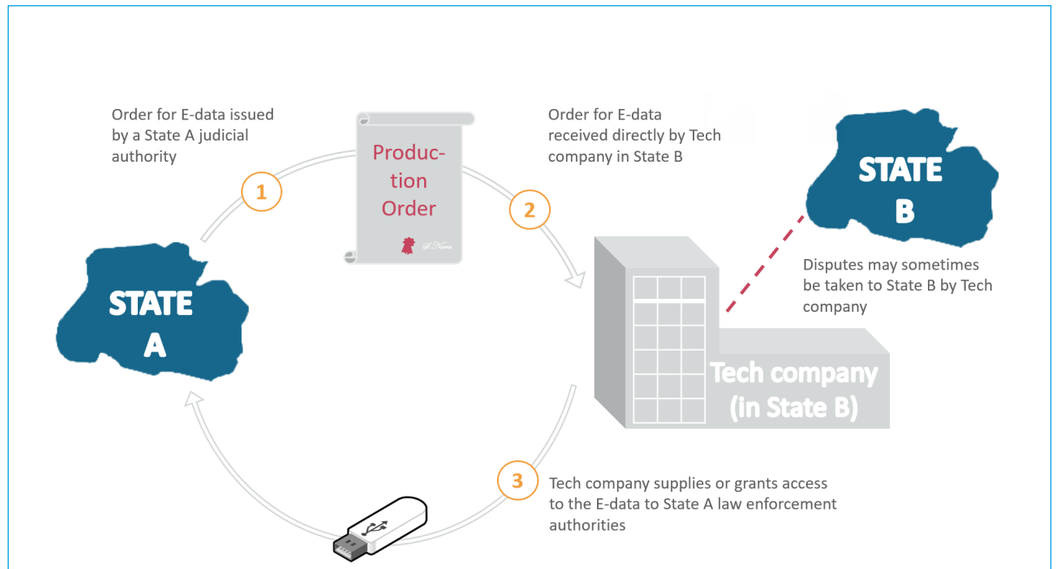


Figure 2: Direct cooperation



14 Thanks to Kingsley Napley and Rachel Scott (3 Raymond Buildings).

Safeguard 1: Notification to the suspect

11. 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 that the accused has a genuine opportunity to prepare and present their case, and to contest arguments and evidence to put before the court, on equal footing with the prosecution. However, the principle of equality of arms is threatened by (inter alia) the secrecy of the preliminary investigation phase and the lack of notification about the gathering of personal data.

12. In adversarial models, such as in the US, the defence is expected to take on an active role in the preparation of its case, and autonomously gather information and materials. In many legal systems in the EU, broadly described as "inquisitorial", law enforcement authorities are solely responsible for conducting an investigation aimed at establishing the "truth". As such, there are obligations on law enforcement authorities 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.

13. Prior notification of the accused is key to ensure that:

    - Exculpatory electronic data is preserved. 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.

    - The accused may have the possibility to challenge the legality of electronic data that may have been obtained illegally or may not be admissible in court proceedings before electronic data is gathered and shared, and harm is done. The ultimate decision-maker cannot realistically remove the inadmissible evidence from their knowledge and unlawfully obtained evidence may have been used to obtain evidence indirectly which is ultimately admitted in court.

14. However, the proposed E-evidence Regulation would prevent the service provider from informing the person whose data is sought "in order to avoid obstructing the relevant criminal proceedings".[15] The requesting authority may delay such notification "as long as it constitutes a measure necessary and proportionate to avoid obstructing criminal proceedings".[16] Although there may sometimes be legitimate reasons for secrecy, there is a concern that "gag orders" are excessively used as a matter of course, rather than exceptionally when strictly required. And without tight limitations and oversight over the use of gag orders, the mechanism will create significant risks of injustice.

15. 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 law enforcement authorities' power to use secrecy limited to an exceptional measure requiring specific justification, with sanctions for law enforcement authorities which misuse this designation relating, for example, to the admissibility of evidence obtained;

    - Judicial oversight over the use of gagging orders by law enforcement authorities;

    - A requirement that the issuing authority give 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 law enforcement authorities requesting electronic data (in the context of secrecy) to extend the request to cover exculpatory evidence (discussed below).

15 Article 11(1) of the proposed E-evidence Regulation.
16 Article 11(2) of the proposed E-evidence Regulation.

Safeguard 1 – Notification to the suspect

Notification is key to enable challenges to requests, but also to ensure that exculpatory evidence is preserved in the same way as inculpatory evidence. The new mechanism must contain a clear presumption of notification and limit law enforcement authorities' power to use secrecy to an exceptional measure requiring specific justification, which is subject to judicial oversight.

"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."
– lawyer, UK

Case study – the Netherlands[17]

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 organisations.

17 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.

Safeguard 2: Prior judicial authorisation (legality of requests)

16. Even where law enforcement authorities have the legal power to gather electronic data, because of the impact this has on the right to private and family life, 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. Moreover, 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 suspect; or may incidentally result in the sharing of evidence with people who are not suspected of a crime.

17. 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 data may contain evidence that a person committed a criminal offence should not be enough. There are good practice examples in this area. For example, in US law a court order is required approving the execution of a request for mutual legal assistance as a fundamental step to ensure the protection of civil liberties of the suspects of accused persons. 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.[17] Ensuring compliance with these requirements is a key role of the central authority in the US (the Office of International Affairs) that receives MLA requests

18. Although law enforcement authorities may find it frustrating,[18] there is a good reason for a certain evidential threshold to be met before electronic data can be gathered. Part of the challenge for law enforcement authorities would appear to be the significant legal differences regarding what evidential threshold (if any) must be met in different national systems. 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.

19. However, the proposed E-evidence Regulation requires that the request be "necessary and proportionate for the purpose of the proceedings"[19] and may only be issued if a similar measure would be available for the same criminal offence in a comparable domestic situation in the issuing State. However, there is no threshold requiring that the issuance of an order be based upon a sufficient degree of suspicion that the contents of the communications are relevant and material to the investigation. In contrast, the CLOUD Act requires that the order be based on a "reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation".[20]

20. Additionally, the CLOUD Act seeks to limit the use of such cross-border requests to "serious crime, including terrorism"[21] whereas the proposed E-evidence Regulation does not set out any threshold for requesting subscriber data and access data, even though such data can be highly sensitive. Production Orders for transactional or content data may be issued for criminal offences punishable in the issuing state by a custodial sentence of a maximum of at least three years.[22] This threshold is, in practice, easy to meet, and the proposal does not contain any requirement that the investigated offence must also be a recognised offence in the country from which the data is sought (dual criminality).

21. The absence from the E-evidence Proposal and the CLOUD Act of an equivalent evidential threshold to the "probable cause" requirement in US law causes considerable concern. The new tools must require that law enforcement authorities meet a threshold in terms of suspicion of criminality (and the severity of the offence) as well as the relevance and materiality of the evidence before they can request or obtain and share electronic data.

18 Member States report that the US 'probable cause' evidence requirement is a key obstacle when cooperating with the US in the scope EU-US Mutual Legal Assistance Treaty, which requires requesting authorities to provide a detailed statement of facts: Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 24 (available here).
19 Article 5(2) of the proposed E-evidence Regulation.
20 Section 5, §2523(b)(B)(3)(iv) of the CLOUD Act.
21 Section 5, §2523(b)(B)(3)(i) of the CLOUD Act.
22 Article 5(4) of the proposed E-evidence Regulation.

22. In addition to a sufficiently robust standard for the issuing of requests for data, the new tools must put in place meaningful judicial oversight to avoid overbroad and disproportionate requests being issued. Prior judicial authorisation should be required to ensure the legality of the action and independent oversight over law enforcement authorities' use of the tools. This safeguard is all the more important if the proposed new cross-border cooperation mechanism, as envisaged in both the E-evidence Package and the CLOUD Act, is to remove the oversight of the judicial authority in the country from which the data is being sought, as is provided in the existing MLA mechanisms.

23. Moreover, the new mechanism should require that the authorisation (warrant) and its basis is disclosed to the suspect in order to enable the person concerned to test the legality of the authorisation.

Safeguard 2 – Tighter control on the issuing of requests

Prior judicial authorisation should be required before the evidence is obtained and shared, and must be disclosed to the suspect to enable challenge. Requests must also be limited to specified serious offences and meet an appropriate evidence test, such as a robust threshold of suspicion that the electronic data sought is relevant to the investigation.

The fishing expedition: ECtHR case study

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.[23] The ECtHR found this to be a violation of the right to privacy.

Often investigators have a "theory" on a case in the initial stages of the investigation and submit a request in hope that the information they receive will bear out their theory. However, this may mean the evidence to support requests may not be there and a request may be so wide as to constitute "fishing". Investigators understandably current send very wide requests which can be unlimited as to time and without specifying what is relevant and why it is important for the investigation.
– lawyer, UK

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

Safeguard 3: Remedies at trial (admissibility of evidence)

24. A key check on the legality of evidence-gathering by law enforcement authorities 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 more generally in removing incentives for law enforcement authorities to violate the law to obtain electronic data.

25. This right is explicitly envisaged in Article 17(1) of the proposed E-evidence Regulation, which gives the accused person the right to challenge the request before the court of the issuing country "during the criminal proceedings" in which the data is being used. However, the proposal does not specify the remedies, leaving it up to Member States to determine as a matter of national law the consequences of a violation of the procedural rules in obtaining electronic data. In practical terms, this mechanism can be difficult to apply:

- 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 law enforcement authority 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, through direct access.[24]

26. The new mechanism must specify the appropriate remedy that applies where electronic evidence has been obtained illegally. Further, in order to prevent law enforcement authorities from benefitting from illegally obtained evidence in order to secure a conviction, the proposed new tools need to enable a review of the way in which evidence was gathered. The underlying source of the electronic data must be disclosed to the reviewing court and to the defence to enable an assessment as to whether electronic data was gathered lawfully and how exculpatory evidence can be obtained.[25]

24 Human Rights Watch, "Dark Side: Secret Origins of Evidence in US Criminal Cases", January 2018 (available here).
25 In this respect, the Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings recommend that courts "consider all relevant factors concerning the source and authenticity of electronic evidence" (paragraph 19). In the light of the implications of a criminal process, the same principle should apply in a criminal justice context.

Safeguard 3 – Right to challenge and meaningful remedies

The accused person must have the right to challenge the request and use of data at trial, and seek specified appropriate legal remedies where electronic data has been obtained illegally. In order to be in a position to exercise the right to challenge, accused persons must be able to obtain disclosure of the sources of the electronic data.

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.[26]

– The Court of Justice of the EU

26 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.

Safeguard 4: Systemic oversight

27. 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. Law enforcement authorities are rightly required to operate within the law. In the context of cross-border evidence exchange, the innovative approaches developed by law enforcement authorities to obtain evidence have raised considerable questions about their legality. One of the functions of a fair and open criminal justice system is to expose whether law enforcement authorities 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 law enforcement authorities to act outside of the law.

28. 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. There is clear evidence of cross-border criminal justice cooperation tools being used to target exiled human rights activists, dissidents, political opponents and journalists.[27] 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 rights defender whom the state wants to silence. It cannot be assumed that such abuses would not occur even within the EU.[28] The new mechanism is an opportunity for the EU and the US to champion a gold standard in preventing such misuse of international judicial cooperation tools.

29. Assessing whether law enforcement authorities have acted within their legal powers is a key element of a fair criminal justice process. The individual criminal trial is the key point at which the behaviour of law enforcement authorities is exposed and tested. Individual cases can provide a snapshot of how electronic data is being gathered, but cannot provide a broader overview of practices. For instance, is a country using the measure more than any other? If so, for what types of offences? Critically, all criminal investigations will not end up in court proceedings and even where they do, all electronic data collected will not necessarily be used as evidence at trial. Allowing challenges in court is not sufficient to assess the legality of the use of the measure by law enforcement authorities.

30. Instead, a more systemic overview of how electronic data is being used is needed to assess whether there is a basis for concern, such as the use of mass fishing expeditions or compliance with requests from states known to pursue politically-motivated prosecutions. There is currently very limited public information about the use of cross-border cooperation mechanisms[29] and it is critical that the proposed new tools incorporate effective mechanisms to collect information 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 needs to be published.

31. The reporting obligations under the proposed E-evidence Package require Member States to "collect and maintain comprehensive statistics from the relevant authorities"[30] on an annual basis and prescribe the information that must be provided. It is, however, silent on whether this will result in data being published by the Commission. The CLOUD Act requires a foreign government to demonstrate "sufficient mechanisms to provide accountability and transparency regarding the collection and use of electronic data".[31] The proposed accountability mechanisms need to be more robust in terms of reporting by law enforcement authorities on the use of the tools, and of the data that is obtained. Moreover, the information should be published regularly.

27 See for example: https://www.fairtrials.org/campaign/interpol.
28 As recognised by the Commission (see here).
29 Commission Impact Assessment, Brussels, 17.4.2018, SWD(2018) 118 final, page 13 (available here).
30 Article 19(2) of the E-evidence Regulation.
31 Section 5, §2523(b)(1)(B)(v) of the CLOUD Act.

Safeguard 4 – Effective oversight mechanism

Law enforcement authorities, the US government, EU Member States and service providers should be required to 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.

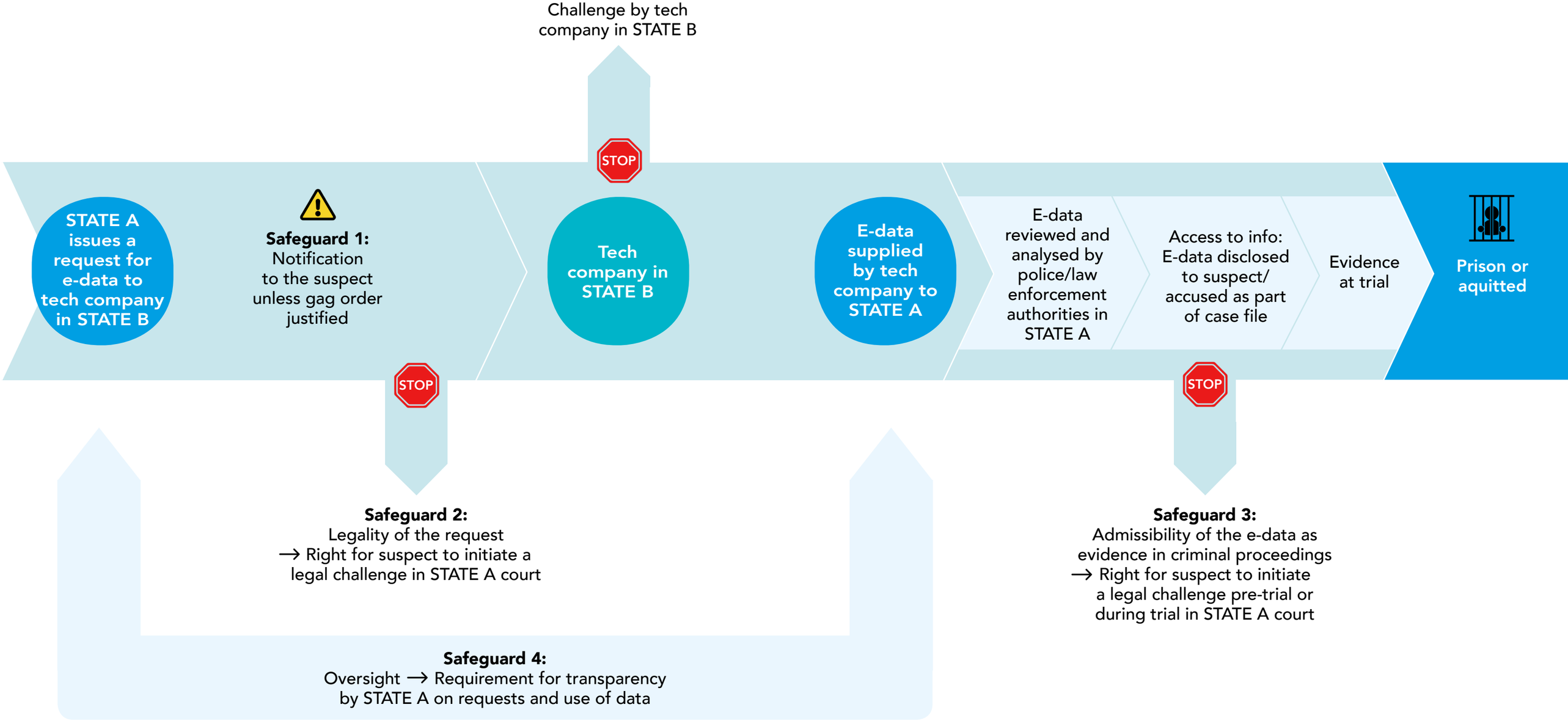
Chilling effect: Amnesty in Belarus

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.

Required Fairness Safeguards

Getting hold of e-data

E-data becomes evidence



Conclusion

32. 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.

33. 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, increasing legal certainty for law enforcement authorities, service providers and defence lawyers, and limiting recourse by law enforcement authorities to measures outside an establishing legal framework, such as, in some countries, direct access. However, such benefits will only be possible if the key safeguards are incorporated into the new cross border cooperation mechanisms.

34. In this respect, the new E-evidence Package, the CLOUD Act and the agreement that will be negotiated between the US and the EU on the exchange of electronic evidence in criminal matters will serve as a model for the rest of the world. This represents a key opportunity to set high standards and uphold the fairness of criminal proceedings through real and meaningful safeguards. In the absence of such safeguards, the new cross-border cooperation mechanism is likely to fail, causing injustice to the persons concerned and undermining public trust in law enforcement authorities.

Notes

Fair Trials