European Commission

INCEPTION IMPACT ASSESSMENT	
TITLE OF THE INITIATIVE	Improving cross-border access to electronic evidence in criminal matters
LEAD DG – RESPONSIBLE UNIT	JUST.B2 / HOME.D4
LIKELY TYPE OF INITIATIVE	Directive
INDICATIVE PLANNING	1st quarter 2018
ADDITIONAL INFORMATION	https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

This Inception Impact Assessment aims to inform stakeholders about the Commission's work in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to make available any relevant information that they may have, including on possible impacts of the different options. The Inception Impact Assessment is provided for information purposes only and its content may change. This Inception Impact Assessment does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content.

A. Context, Problem definition and Subsidiarity Check

Context

As a consequence of the growing use of electronic communication tools such as social media, webmail, messaging services and apps, an increasing number of criminal investigations have to rely on electronic evidence, such as information on the holder of an email account, messages exchanged via Facebook messenger or information on the timing of WhatsApp calls. Law enforcement and judicial authorities experience difficulties to access such data,[1] including in cases where the criminal activity is located in one single country, as the relevant service providers and infrastructure are often located in other EU Member States or third countries such as the United States (U.S.).

In the European Agenda on Security,[2] the Commission committed to review obstacles to criminal investigations on cybercrime, notably on cross-border access to electronic evidence. In its June 2016 Conclusions, the Justice and Home Affairs Council asked the Commission to explore possible solutions, including legislative options.[3] The Commission subsequently announced an initiative on access to electronic evidence in its 2017 Work Programme[4] and presented a non-paper in June 2017.[5]

Problem the initiative aims to tackle

Obstacles to accessing electronic evidence complicate criminal investigations and therefore affect criminal justice. Criminal procedural measures to gather evidence as part of a criminal investigation[6] are usually national in scope. By contrast, obtaining electronic evidence frequently has cross-border implications. Therefore, authorities have to rely on judicial cooperation mechanisms like mutual legal assistance (MLA) or, within the EU, mutual recognition,[7] on the direct cooperation of service providers, or on direct access to obtain electronic information. All three channels raise different types of issues

[1] Frequently categorised as account subscriber information, metadata, or content data. Definitions of these data categories can be found in the Council of Europe Budapest Convention (CETS No 185) and in the proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final.

[2] COM(2015) 185 final.

[3] Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST 9579/16.

[4] COM(2016) 710 final.

[5] All documents and more information are available at https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

[6] The tools most frequently used are measures requesting a service provider to provide information on a user of the services ("production requests/orders") and measures allowing direct access to the said information.

[7] Since May 2017, the European Investigation Order: Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L130 of 1.5.2014, p. 1.

affecting the investigations, that may result in abandoned and unsuccessful cases and, ultimately, in a less effective criminal justice.

In view of the increasing number of requests for e-evidence, especially in the frequent cases where the storage location of the data or the seat of the provider form the only link to the other country, law enforcement and judicial officials often consider the procedures for judicial cooperation as too slow, disproportionately cumbersome also in view of the limited interest of the receiving country, and thus inadequate. While a national request to service providers takes in general a few days at most, MLA requests to the U.S. as the main recipient take around 10 months on average and require a significant resources. In such cases, the evidence transmitted is often outdated or comes too late. For requests between Member States, the European Investigation Order provides for deadlines of 120 days, which is faster than MLA, but still quite slow compared to direct cooperation.

Through direct cooperation between authorities in EU Member States and service providers in the U.S., which is possible under U.S. law for non-content data, the latter receive more than 100,000 requests per year,[8] compared to about 4,000 requests under the EU-U.S. MLA Convention.[9] While appreciating the relative efficiency of direct cooperation, practitioners find this voluntary mechanism opaque and unreliable as a result of varying policies put in place by service providers. Service providers face conflicting interests and legal uncertainty; on the one hand, they have to protect their users' privacy; on the other, they are expected to cooperate with law enforcement to ensure the success of criminal investigations. Moreover, such cooperation is not possible between EU Member States in most cases, as Member States' legislation prevents service providers from responding to requests from foreign authorities. Furthermore, at times the location of data or infrastructure cannot be established by law enforcement or judicial authorities, adding further complications.

A number of Member States provide for possibilities to access data directly from an information system.[10] Nevertheless, such direct access measures frequently have a cross-border aspect which is not taken into account, as the data may be stored or the service provider may be located in another country, and the respective safeguards vary between Member States.

Subsidiarity check (and legal basis)

Accessing e-evidence in criminal investigations is often cross-border and cannot satisfactorily be dealt with by individual Member States alone. In the absence of EU action, Member States would have to update their national laws to respond to new and emerging challenges with the likely consequence of further fragmentation and/or conflicts of law. Given the diversity of legal approaches, the number of policy areas concerned by the matter (security, criminal law, fundamental rights including data protection, economic issues) and the large range of stakeholders, the EU seems the most appropriate level to address the identified problems.

The legal basis for EU action is Art. 82 (1) and (2) TFEU,which specifies that judicial cooperation in criminal matters shall be based on the principle of mutual recognition.

B. Objectives and Policy options

[8] U.S. legislation on electronic communications permits service providers to respond to foreign law enforcement requests for non-content data but does not specify any requirements or procedures.

[9] The indicated number of requests received by service providers is not limited to requests from Member States, meaning the two figures are not directly comparable, but the figures nevertheless give an indication of the importance direct cooperation with service providers now has.

[10] A more detailed problem definition is set out in the Commission's December 2016 Progress Report and in its June 2017 Technical Paper.

The initiative aims to address obstacles in cross-border access to electronic evidence in criminal investigations. Access should become more efficient and faster, while ensuring at the same time transparency and accountability, a high level of protection of fundamental rights including individuals' rights in criminal proceedings, data protection and privacy. It aims at the same time to ensure legal certainty by eliminating or at least reducing fragmentation and conflicts of law. It would also provide an alternative to data localisation requirements that could be imposed by Member States if data in other Member States is too difficult to access.

Baseline scenario – no legislative change and a set of practical measures

Practical measures as agreed by JHA Council in June 2017[11] are in the process of being implemented and can improve both judicial cooperation and cooperation with service providers within the existing framework. However, they cannot address the legal fragmentation and conflicts of laws that exists today, nor can they provide legal certainty, transparency and accountability in direct cross-border cooperation between authorities and service providers.

Legislative options

The impact assessment will develop various policy options based on the further analysis, focusing in particular on the following possible measures at EU level.

1. A legal framework authorising authorities to directly request or compel a service provider in another Member State to disclose e-evidence processed in the Union, including appropriate safeguards and conditions. This framework can leave to the discretion of the service provider a decision on whether to provide a response ("production request") or can obligate service providers to respond ("production order"). This could also be considered with respect to service providers located outside of the Union and/or data stored outside of the Union. This system could be complemented by an obligation for service providers established in third countries but offering services in the EU to designate a legal representative in the EU for the purpose of the cooperation on the basis of production requests/orders.

2. A legal framework for law enforcement to access e-evidence pursuant to a set of safeguards and measures to mitigate cross-border effects, without cooperation of a service provider or the owner of the data, through a seized device or an information system. This could also be considered with respect to data whose storage place is not known or data which is stored outside of the Union.

3. A legal framework to provide for a common understanding of types of electronic evidence and service providers that fall within the scope of the measures proposed.

As the problems described above reach beyond the EU, the above measures could be complemented by measures in relation to third countries, notably in relation to possible conflicts of law:

4. Initiating negotiations with key partner countries such as the U.S. in order to enable reciprocal cross-border access to electronic evidence, in particular on content data, and including appropriate safeguards.

5. Assessing the role of the EU towards the Council of Europe Budapest Convention on Cybercrime[12], in view of the negotiations on a second Additional Protocol to the Convention.

C. Preliminary Assessment of Expected Impacts

Likely economic impacts

Subject to further assessment, the likely economic impacts could include:

- For both the public and the private sector, administrative and compliance costs arise from implementing new legislation.
- For the public sector, efficiency gains are to be expected because of leaner procedures and a partial

[11] Such as an electronic platform for requests between Member States, training of practitioners, setting up Single Points of Contacts on the Law Enforcement side, streamlining service providers' policies. For details see the Commission's June 2017 Technical Paper.

[12] The Convention on Cybercrime of the Council of Europe (CETS No 185).

removal of double checks. This should be reflected in a decrease of administrative resources expended on cases with limited connections to the local jurisdiction.

- For service providers not established in the EU, further costs could arise e.g. from having to designate a legal representative in the EU. Such costs may be more relevant for small(er) and medium-sized providers, but mitigating measures could be considered. At the same time, the creation of a harmonized framework should also decrease the need to have legal expertise available on up to 28 different national regimes and result in lower expenditure on legal assessments.
- With a view to direct access, costs could also result from investment in strengthened IT security, in particular if direct access increases the risk of subsequent data breaches from private parties/foreign governments (for reasons other than law enforcement).
- Improved access by EU authorities to e-evidence could affect business models chosen by service providers, in particular where data location and access to this data is an important factor for customers.
- A more efficient system would likely lead to an increase of cross-border requests, meaning additional costs for the service providers having to provide more data.
- By streamlining the production requests/orders the costs and the administrative burden for the public sector relating to requests to service providers that are not replied or replied with a notable delay will be significantly diminished.
- Furthermore, both the public and the private sector would benefit from a common framework creating more legal certainty and mutual trust between the public and the private sector.

Likely social impacts

- The initiative would considerably contribute to preventing and fighting crime more efficiently in the European Union through a better evidence base in criminal proceedings. It would result in more convictions of criminals, to the benefit of victims of crime and society as a whole. It would also contribute to fighting terrorism more efficiently and enhancing security in the Union.
- Reducing complexity and fragmentation as well as reducing situations of conflicts of law would also create more legal certainty for service providers and public authorities.
- Introducing provisions on direct access would better protect the rights of individuals concerned by such measures and address possible cross-border impacts.

Likely environmental impacts

While there are no direct environmental impacts, the initiative could also help to investigate and prosecute environmental crime.

Likely impacts on fundamental rights

Accessing electronic evidence across borders serves the interest of effective detection and prosecution of crimes, and the protection of victims of crime. At the same time, contemplating measures to facilitate cross-border access to electronic evidence, raises questions of international law, in particular with regard to territorial jurisdiction, and of impact on fundamental rights.

As regards the protection of individuals' rights, the right to fair trial is of particular importance when it comes to criminal proceedings. Any legislative initiative must respect this principle and include safeguards to protect the rights of the persons affected, including the rights of the defence, the right to an effective remedy as well as other procedural rights. Given that the possible measures could require individuals to challenge measures in a court of a Member State other than their own, the possibilities of effective judicial redress for persons who may be affected by such measures would also have to be addressed.

Another important aspect is the impact on the fundamental rights to data protection and privacy. Subscriber information, traffic data, metadata, and content data are personal data, and are thus covered by the safeguards under the EU data protection acquis. Respect of data protection rules is paramount both for law enforcement when sending requests and for service providers when responding to requests. The measure will also have to consider how to address cases where the evidence was processed by the service provider in violation of other legal frameworks.

Expanding the possibilities for Member States' authorities to request, or directly access, e-evidence

stored outside the EU in foreign jurisdictions creates a risk of triggering reciprocal reactions from third countries, with possible implications for the protection of the fundamental rights of persons in the European Union, for instance as regards due process, data protection and privacy. This could also negatively affect the trust of consumers when using services that offer to store data in the EU, and put European companies in a conflict of law situation.

Likely impacts on simplification and/or administrative burden

The public sector would incur administrative and compliance costs associated with negotiating, transposing and implementing new legislation, including trainings etc. On the other hand, the initiative is expected to improve the efficiency of criminal investigations. It would foster the cooperation between relevant authorities and service providers – depending on the selected policy option –by simplifying and streamlining the current different channels and policies largely set by service providers themselves to deal with the requests of law enforcement and judicial authorities. It would reduce the efforts required to implement cross-border investigation measures and could result in swifter and more successful prosecution of cases.

D. Data Collection and Better Regulation Instruments

Impact assessment

An impact assessment is being prepared examining the possible policy options and analysing the potential economic, social and fundamental rights impacts of this initiative. The assessment will support the preparation of this initiative and inform the Commission's decision.

Data collection

The Commission has conducted an expert consultation starting in July 2016 and issued in September 2016 a questionnaire to Member States. The results are set out in the documents available on the e-evidence homepage and will feed into the impact assessment.

Statistics can also be derived from the transparency reports of the major service providers and other publicly available sources.[13] Furthermore, a large number of studies have been conducted on the problem of access to evidence across borders, including the recently concluded and EU-funded EVIDENCE project, which provides further data for the impact assessment.

Additional data is needed in particular on the fundamental rights and economic aspects of the options considered by the Commission. This will be gathered partly through the Joint Research Centre. The targeted consultation will also be used to collect information from relevant stakeholders, including industry associations and service providers.

Consultation strategy

The consultation aims to ensure that citizens and stakeholders, including those who will be directly affected by this initiative, can provide their views and input. This will also improve the evidence base underpinning the initiative. The consultation targets all relevant stakeholders: industry, civil society and public authorities, but also citizens.
Between July 2016 and April 2017 the Commission has already held a number of targeted small expert meetings and workshops with academics, civil society, practitioners and the private sector, as well as meetings with experts from all EU Member States. In September 2016 it also issued a questionnaire to Member States and invited stakeholders to submit information on concrete challenges and cases. Commission representatives also participated in various workshops and conferences organised by third parties to provide information on the ongoing work and gather additional input. Future consultation activities will complete the information that has already been collected as part of this expert consultation process. They will comprise a 12-week public consultation, expected to be launched in early August in English, with other EU official languages being added as soon as possible. Replies will be possible in all official EU languages. The public consultation will be accessible via the Commission's central public consultations page. A specific questionnaire to Industry to collect information and data in the framework

[13] Cf. e.g. https://www.google.com/transparencyreport with links to transparency reports of other companies.

of the current legal and factual status quo and on the impact of the possible measures will also be sent in August. Further targeted expert meetings and workshops with relevant stakeholders will be organised in September/October. At the end of this consultation process, an overall synopsis report will be drawn up covering the results of the different consultation activities that took place.
Will an Implementation plan be established?
Depending on the complexity of the final proposal an implementation plan may be established.