CENTER FOR DEMOCRACY & TECHNOLOGY

CDT Recommendations for Improving the European Commission's E-Evidence Proposals

August 2018

Introduction

This paper sets out CDT's views on the European Commission's E-Evidence proposals.[1] Immediately after the proposals were published, we posted a set of blogs about the proposals,[2,3] and this paper builds on the views expressed in these blogs by incorporating additional ideas and analysis.

CDT recognises the validity of the concerns that motivated the drafting of the proposals. There is evidence that law enforcement authorities have difficulty accessing electronic information that can be useful for criminal investigations, and that more and more investigations require access to electronic data. Further, the Commission's proposals attempt to address the fact that there are no EU-wide rules governing the processes and conditions for law enforcement authorities to obtain data from communications providers. It is in the interest of law enforcement authorities, citizens and users, and communications providers to have predictable and stable EU-wide legislation in this area.

For several years CDT has engaged in discussions about policy solutions in the EU, the U.S. and around the world that could help address this question. Our starting point was to consider a criminal investigation that is "wholly domestic",[4] by which we mean a crime committed in one country, against a victim located in that country, with an investigation focused on suspects also located in that country. In such a case, electronic evidence, such as communications data, could be relevant and could be held by communications in other countries. Given the domestic nature of such an investigation, it would be sensible to consider exceptions to the principle that law enforcement data requests should be made through Mutual Legal Assistance Treaty (MLAT) procedures, given the time and efficiency constraints

[1] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD) 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 COM/2018/226 final - 2018/0107 (COD). https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[2] https://cdt.org/blog/initial-observations-on-the-european-commissions-e-evidence-proposals/

[3] https://cdt.org/blog/assessing-the-e-evidence-directive-on-ten-human-rights-criteria/

[4] https://cdt.org/insight/mlat-reform-a-straw-man-proposal/

associated with them, and provided that the exceptional process had strong human rights protections built in.

However, the E-Evidence proposals take a much broader approach than this. The proposals give European law enforcement unprecedented and almost unlimited access to data, regardless of the nationality and location of the people whose data is sought, and regardless of the location of the provider holding the data. The approach is broader with regard to jurisdiction and connecting factors than the primary international legal instrument in this field: The Council of Europe Budapest Convention.[5] Developing countries could well take inspiration from this very broad assertion of jurisdiction, which could expose European companies to similar demands from countries with a lower rule of law and human rights standards for data they hold about Europeans or people in other countries. This could create new and serious risks to privacy.

The Regulation and Directive will effectively give each EU Member State access for law enforcement purposes to the data of internet users worldwide. Each provider in the scope of the Proposals can be compelled to disclose its users' data no matter where those users are located and regardless of their country of citizenship. The definition of providers is broad. It encompasses not only electronic communications providers but a wide range of hosting services, online marketplaces and domain and numbering providers. Further, the range of crimes and investigations the European Production Orders (EPO) and Preservation Orders can be used for is also broad. The EPO can be used in a much broader set of criminal investigations than existing criminal justice instruments enabling cross border cooperation, such as the European Investigation Order (EIO) and the European Arrest Warrant.

An instrument that gives authorities such extensive possibilities to access data must be accompanied by very strong privacy and procedural safeguards. Although EU Member States are committed to upholding the European Convention on Human Rights and the EU Charter of Fundamental Rights, it is a fact that States have different national laws that provide different levels of protection.[6] Yet, the proposals assume a very high level of confidence that courts and authorities (which can issue EPOs) meet European standards, with very limited possibilities for authorities in other countries or providers to whom EPOs are addressed.

---

[5] Article 18 of the Convention allows an authority to issue a production order when four conditions are met: (1) the criminal justice authority has jurisdiction over the offence; (2) the service provider is in possession or control of the subscriber information; (3) the person or service provider is in the territory of the party, or the party considers that a service provider offers a service in its territory; (4) the subscriber information to be submitted relates to a service of the provider offered in the territory of the Party. https://www.coe.int/en/web/cybercrime/home

[6] The European Commission is running infringement proceedings against one Member State (Poland) for failure to uphold rule of law standards. http://europa.eu/rapid/press-release_IP-18-4987_en.htm

In conclusion, CDT acknowledges that legislative and policy solutions are required to update existing MLAT-based frameworks. We also recognise several constructive and positive elements in the E-Evidence proposals. However, we believe they must strike a better balance between the legitimate interests of law enforcement authorities, users and citizens, and international communications providers. The suggestions in this paper are intended to help create a solution that strikes such a balance. Primarily, we suggest ways to enhance the review and oversight of EPOs, both by authorities in executing Member States and by providers. Further, we suggest that EPOs should replace the existing, informal and voluntary cooperation schemes that law enforcement authorities currently use to obtain data from providers. We also propose limiting the use of EPOs to a more restricted set of criminal investigations, consistent with the approach taken in existing EU instruments for judicial cooperation. In addition, we propose stronger rules on notification and transparency, more realistic deadlines for compliance with EPOs, harmonised reimbursement, and a requirement to use a central portal for channeling EPOS, or alternatively single points of contact.

I. Strengthen the Necessity and Proportionality Test and Provide Possibilities for Additional Review

A fundamental concern with the E-evidence proposals is that only the authority issuing an EPO is in a position to assess whether it violates immunities and privileges under the laws of the Member State, meets the necessary and proportionate threshold, or violates the Charter of Fundamental Rights. The service provider to which the order is issued will not be able to conduct assessments based on the very limited information provided in the EPO Certificate, and has limited grounds for challenging it. No authority in the Member State where the EPO is executed will be aware that an order has been issued unless the issuing authority proactively seeks clarification, or in the unlikely event that the service provider challenges the order.

As mentioned, the EPO process makes it mandatory for any service provider judged to be active on the territory of an EU Member State to disclose information on any user, regardless of whether the user is located in the Member State, in another Member State or outside the European Union. This creates potentially significant privacy risks that need mitigation. Member State policies, processes and traditions in criminal justice differ widely. As drafted, the Regulation does not provide for oversight or review of the necessity and proportionality of issued EPOs. Only the issuing authority makes the determination of necessity and proportionality, unless that authority explicitly requests a review by an authority in the executing state. The provider who issued the order will not be able to conduct a review based on the very limited information in the EPO Certificate. The approach in the regulation assumes a

very high degree of confidence in the judgment of the issuing authority, and assumes that procedural protections and safeguards are uniform. Both assumptions are debatable.

These types of solutions can help address this problem:

First, when an EPO is issued, the issuing authority should provide notice to the competent authorities of the country of execution in order for the latter to be able to review the order and ensure charter compliance. The additional review of orders is especially relevant when data requests concern people located outside the issuing state. This additional review is less essential when the investigation can be considered wholly domestic: that is, when the crime being investigated has taken place in the territory of the issuing authority and when the authority only requests data on people known or believed to be located in its own territory.

Second, when competent authorities issue EPOs, they should demonstrate in some detail how the Order meets the necessity and proportionality test. This can be done by providing additional justification of reasonable suspicion. The Order should explain why the data requested is likely to contain evidence of a crime, and how the information will contribute to the investigation. A layered approach could be developed, whereby requests for more sensitive data, notably transactional and content data, are required to meet a higher standard than subscriber and access data. Language from existing MLATs could be used to develop such criteria.

Third, the Regulation should require issuing authorities to provide more information to service providers that would enable them to conduct fundamental rights assessments and establish whether a compliance with an order violates the laws of the executing state, developing countries or the rights of the provider's users. This would be particularly relevant for large companies with resources and processes that enable them to conduct such assessments. The scope of review a provider could seek in the executing country should be broadened to permit consideration of such information.

II. Make the EPO the Exclusive Process for Seeking Data from Service Providers Outside the Issuing Country's Territory

The Regulation should require law enforcement authorities to use European Production Orders (EPO) as the exclusive means to address direct requests for electronic data held by communications providers based outside of the territory of the Member State of the authority requesting the data. This way, the EPO process could replace a plethora of existing informal processes by which law enforcement authorities in different Member States request data from service providers. This would

be consistent with the objectives of the E-Evidence proposals: to improve legal certainty for authorities, service providers and people whose data is sought. Clearly, MLAT procedures or European Investigation Orders remain in place and are available for Member State authorities to use. These mechanisms differ from the the E-Evidence proposals in that they are instruments for cooperation between law enforcement authorities in different countries, not between authorities and private entities.

III. Limit the Scope of EPOs Along the Lines of the EIO / Dual Criminality

The EPO process foreseen in the proposals can be used for a very broad range of investigations. Access data and subscriber information can be sought for any type of investigation. Transactional and content data orders can be issued for crimes that carry a sentence of no less than three years, in addition to offences that are categorised under legislation on terrorism, cybercrime and child sexual exploitation. The intent is to limit the use of EPOs to serious crimes; however, we would argue that the three-year threshold is not sufficient limit the use of the measure to crimes that are considered serious in all Member States. For example, Germany's Criminal Code applies a 3-year sentence to acts that are deemed to insult religions and ideologies.[7] However, most Member States have revoked laws against blasphemy. Including such speech "offences" in a crossborder measure seems disproportionate and a threat to free expression. There is likely to be many examples of conduct that carries a heavy prison sentence in one Member State but is not even a criminal offence in another. A solution to this problem could be to limit the use of EPOs to the scope of crimes for which a European Investigation Order can be issued under Directive 2014/41.[8] Under the EIO process, the executing state can refuse to carry out the EIO if the conduct being investigated is not illegal in the country of execution, among other things.

IV. Make Authorities Responsible for Notifying People Whose Data is Sought Unless There are Compelling Reasons Why Notifying Would Jeopardise the Investigation

It is and should remain the norm that when a person's data is requested in connection with an investigation the person is notified, unless the court or other issuing authority finds there is reason to believe that contemporaneous notification could jeopardise the investigation. If notice is to be delayed, the authority has to justify that delay is necessary to avoid obstruction of investigation. The Regulation should state clearly that issuing authorities are under obligation to provide notice to the

[7] https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041

individuals involved, when an order is issued. The provider holding the requested data should have permission to notify the user. The system should be such that immediate notification is the default position, and that notification can only be delayed in exceptional circumstances, and for clearly defined periods of time.

V. Establish a Central Electronic Portal for Processing EPOs, and Make it Mandatory for Issuing Authorities to Use it or Require Member States to Set Up SPOCs

The European Commission has said that it is working on establishing a secure portal for electronic transfers of EPOs. The Regulation should require issuing authorities to use this facility once it is available. Absent such a requirement, dozens or maybe hundreds of authorities might issue orders by mail, fax, email, etc. Service providers would need to ensure orders are valid and genuine. Authentication of orders would be much easier with a single portal; it would make the process far more efficient, reliable and trustworthy, as well as enabling more effective oversight and review. As an alternative, and until a central portal is established, the Regulation could require Member States to nominate a Single Point of Contact (one per Member State). Both options would serve to make the EPO system work more efficiently and enable effective authentication of orders.

VI. Amend Deadlines for Complying with EPOs, and Sanctions for Not Complying

The proposals set tight deadlines for service providers to comply with orders, and call for dissuasive sanctions for service providers that do not comply. The intent is to put in place strong incentives for compliance within the deadlines. Combined with the broad scope of investigations for which orders can be issued, and the lack of review by authorities in the state of execution or by the service provider, strong incentives for rapid compliance create additional risks that orders are issued without the necessary conditions having been met. A more balanced approach should be developed to mitigate this risk.

VII. Make Reimbursement Mandatory and Harmonised

The Regulation does not require that Member States reimburse providers for costs incurred in reviewing and executing orders. Article 12 says that if a Member State reimburses domestic service providers for their costs, it must reimburse providers elsewhere for their compliance costs. Instead, reimbursement of costs should be mandatory. This would serve a dual purpose of, in particular,

protecting small providers against excessive costs, and even more importantly, it would have a privacy-protective effect by making it less likely that EPOs are issued unless there is a clear need and justification. This might be particularly relevant with respect to orders for access data and subscriber data, which can be sought in an investigation of any crime without exception.

VIII. Enhance Transparency and Accountability by Requiring the European Commission to Publish Numbers of Data Demands Made and Granted, and Types of Offences Specified

Article 19 obliges Member States to maintain comprehensive statistics and report them to the European Commission annually. However, it does not oblige the Commission to publish this information. This should be amended, and the publication of data and statistics about the use of EPOs should be made mandatory. It is particularly essential that Data Protection Authorities have full access to the data and can assess the use of the instrument to verify that privacy rules are respected.