Access Now key recommendations on the Commission's Technical Document Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace
Presented in June 2017

Intro

Access Now welcomes the European Commission's expert process and the effort to improve mechanisms for cross-border access to electronic evidence. This paper aims to provide the Commission with key recommendations for the upcoming discussions and legislative process.

1. Need for legal certainty and clarity

Beyond recognising the main underlying issue of jurisdiction and conflicting laws and obligations we note that the existing **parallel processes** make it difficult to end on a unified approach and result. The discrepancies not only decrease the effectiveness of law enforcement and create extra burden for companies, but also undermine transparency, fundamental rights and the rule of law.

The Technical Document sets out different objectives and different solutions for measures aiming to facilitate cross border access to evidence within the EU and with third countries. Although this approach is nothing but natural, it puts into question the impact on the effectivity of any of the proposed measures having in mind the global cross-border nature of the problem. As the Technical Documents states, some of the proposed frameworks "would create **a new dimension in cooperation in criminal matters among member states**". The political willingness for stronger cooperation must be accompanied with appropriate safeguards for fundamental rights in line with the Charter.

The material scope of the described solutions include different types of electronic evidence. **The categorization of data and definitions must be in line with the EU's data protection regime** including the Charter, the General Data Protection Regulation (GDPR), and the proposal for e-Privacy Regulation. We would like to point out the **sensitivity of data beyond content** which is downplayed by the Technical Paper at the moment. The protection of user metadata has often been overlooked and its impact on privacy minimised. However, in recent years, its relevance has been clearly established. Studies indicate that metadata is just as revealing as the content of communications itself. Given its relevance, the protection of metadata, beyond just traffic and location indicators, must meet the same standard as for requesting content. Generally, we urge stakeholders to follow the categories of personal and sensitive data with the highest level of protection possible.

Regarding **direct cooperation between authorities and service providers,** current reform proposals, implementing a limited mechanism designed to supplement MLATs could make the

situation better, so long as it is built from the ground up with necessary human rights protections and strictly limited to situations where the use of extraordinary process is justifiable. (For a discussion of necessary elements of an MLAT bypass regime *see* How to make an MLAT "safe harbor" safe for users https://www.accessnow.org/make-mlat-safe-harbor-safe-users/).

2. Key recommendations for cross-border access to evidence within the EU

2.1 Direct cooperation

Access Now opposes the development of frameworks within the EU that are built on direct cooperation between law enforcement or judicial authorities and service providers. The advantages of production orders would undermine fundamental rights safeguards such as Article 11 "Grounds for non-recognition or non-execution" of the European Investigation Order (EIO).

The recent adoption and applicability of the EIO has not provided with enough experience and time to assess its impact, and a proposal for a new framework with a similar objective questions the purpose and viability of the EIO in the first place. In addition to that, there is no guarantee for member states not to opt out the same way which would lead to regenerating the same problems again.

2.2 Direct access

As a part of possible legislative measures, the technical paper suggests the establishment of an EU framework for direct access to e-evidence. The need for and the scope of this measure is derived from existing practices by Member States where often neither the affected individual(s), service providers nor external law enforcement authorities are contacted. There should be no doubt that the process described by the MS and the Commission in its paper, de facto, amounts to government hacking; a virtually invisible process which Access Now has repeatedly argued desperately needs to be subject to human rights scrutiny, transparency and accountability.The Commission correctly identifies the need to notify other affected countries if and when the MS law enforcement engages in such an operation, yet it fails to acknowledge and to address the potential unlawfulness of such a process . Instead, the Commission exempts itself of responsibility by stating that the [government hacking] framework "would essentially leave it to each Member State to provide for a competence of its authorities to perform extended or remote searches." However it is the responsibility of the Commission as Guardian of the Treaties, to investigate national practices and potential violations against the European Charter of Fundamental Rights in this matter.

All government hacking substantially interferes with human rights, including the right to privacy and freedom of expression. The nature of hacking creates new threats to human rights

as it can provide access to protected information, both stored or in transit, or even while it is being created or drafted. Exploits used in operations can act unpredictably, damaging hardware or software or infecting non-targets and compromising their information. Even when a particular hack is narrowly designed, it can have unexpected and unforeseen impact. Based on our analysis of human rights law, we conclude that there must be a **presumptive prohibition** on all government hacking. While the Commission proposal attempts to shield itself and Member States of responsibility regarding the violation of territorial jurisdiction in such operations, it is unacceptable that such a framework be established without due integration of fundamental rights in national legislation on this matter. (For a necessary human rights safeguards *See* Appendix: Ten Human Rights Safeguards for Government Hacking https://www.accessnow.org/governmenthackingdoc/)

Potential harm to cybersecurity. In addition to these safeguards, which represent only what is necessary from a human rights perspective, the judicial authority authorizing hacking activity must consider the entire range of potential harm that could be caused by the operation, particularly the potential harm to cybersecurity as well as incidental harms that could be caused to other users or generally to any segment of the population. To that end, it is worth noting how closely this process is intertwined with the ongoing global conversation around intelligence agencies and law enforcement stockpiling vulnerabilities and zero-day exploits (much to the detriment of the health of the internet, as evidenced for instance by the recent Wannacry attacks). The Commission needs to acknowledge the broader impact of their proposed legislative measures and point out deficiencies in Member State laws in this area.

3. Key recommendations for cross-border access to evidence beyond the EU

Prioritizing the reform of MLAT process over direct cooperation. Any proposal to reform the MLAT process must find a way to address these shortcomings for law enforcement and for our rights. Given the number of issues entangled in the MLAT imbroglio, it's important to articulate what the priorities are for any reform effort. We believe it's critical to (1) improve efficiency for lawful government requests, (2) reduce incentives for government interference with private sector platforms and networks, (3) provide clarity for users, governments, and companies, on the treatment of user data, (4) ensure the system for cross border data requests protects user rights. https://www.accessnow.org/whats-wrong-system-cross-border-access-data/

We need to fix the broken system for cross-border access to data. At Access Now, we fight for the right to privacy across the globe. That means opposing over-broad, unaccountable, and secret government surveillance programs. It also means recognizing that when lawful processes for access to users' data fail, it can be bad for privacy, the integrity of the internet, and digital security.

https://www.accessnow.org/need-fix-broken-system-cross-border-data-access/

Access Now is seeing governments look to **non-MLAT bilateral or multilateral options to bypass the MLAT process**. For instance the Council of Europe is in the early stages of negotiations to grant greater direct access to the countries party to the Convention of Cybercrime (Budapest Convention). MLAT bypass agreements (1) will bring only limited efficiency gains for lawful government requests, (2) don't adequately reduce incentives for governments to interfere with private-sector platforms and networks, (3) won't give users, governments, or companies clarity on how user data will or should be treated, (4) won't provide adequate protections for our rights.
https://www.accessnow.org/diagnosis-current-proposals-fix-mlat-system-wont-work/

Transfer of personal data to a third country. Access Now reminds the stakeholders for Article 48 of the GDPR which says that "any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter". We are also seeking clarification on the point the Technical Document makes on the Police Directive and how it would solve the issue of cross border access to evidence when the competent authority is allowed to transfer data to a service provider established in a third country.

Conclusion

Access Now recognises the need for systematic reform and modernization of cross border access to evidence. We urge the Commission and other decision makers to implement an evidence-based approach and to focus the reform on the MLAT process and prioritize MLAT over direct cooperation. While exploring practical and legislative solutions to cross border access to evidence within and beyond the European Union, the Commission must ensure that a highest level of protection for fundamental rights are ensured following international human rights principles.

For more information, please contact:

Fanny Hidvégi, European Policy Manager (fanny@accessnow.org)
Lucie Krahulcova, Policy Associate (lucie@accessnow.org)