Access Now comments on the Commission's Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace

May 2017

Table of content

Key recommendations

- There is a need for systematic reform and modernization of the MLAT process;
- Prioritizing the reform of the MLAT process over direct cooperation;
- A human rights impact assessment must precede any new legislation in this matter;
- An evaluation of the European Investigation Order should be mandatory prior to the legislative action tied to this investigation;
- There must be an evidence-based approach to cross-border legal cooperation.

Introduction

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[1] By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. Based in Brussels since 2010, our European team focuses on a broad range of issues at the EU level, including privacy and data protection, surveillance and cybersecurity, privatised enforcement, trade agreements, and Net Neutrality. The protection of digital rights is an important issue worldwide, but because the EU is a global standard setter, furthering these rights in Europe is critical for people in all parts of the world. Access Now's unique positioning in Europe reflects a regionally focused expertise combined with a global vision brought about through close cooperation with colleagues based in India, Tunisia, the United States of America, Argentina, Costa Rica, and the Philippines.

At Access Now we care deeply about the right to privacy and advancing digital security for users. As a part of that process we have extensively covered various areas of international law and their application to the digital sphere. Central to this have been Mutual Legal Assistance Treaties (MLATs), which are key to the international framework that allows law enforcement in one country to get access to information stored in another country. Access Now has repeatedly called for improvements to the MLAT process in order to address its known inadequacies; the process is too slow for urgent law enforcement investigations and is often under-resourced and confusing.[2]

While the need for reform is dire, this must not come at the expense of the established democratic integrity of our legislative frameworks. Increasingly, we are seeing a rise in government's attempts to streamline cross border access to data by attempting to circumvent the established MLAT process. The frustration with the analog MLAT system is leading to an increase in direct cooperation between governments and industry, a process fraught with disregard for fundamental rights of users, transparency, accountability and redress. The MLAT process, however, ensures safeguards which must be present in any cross-border cooperation, regardless of whether the evidence is electronic or not, and therefore should be updated and maintained to ensure the integrity of our legal process; established protections must not conveniently disappear in the electronic ecosystem.

The overarching legal requirement for any EU or member state level solutions for access of the competent national authorities to data is laid down by the Court of Justice of the European Union. The Charter of Fundamental Rights of the European Union and the relevant jurisprudence must be respected either in the MLA reform or the direct cooperation approach.

We welcome the effort by the HOME and JUST Commission Services in facilitating a multistakeholder platform to discuss the current investigation into improving criminal justice in cyberspace. We welcome the effort made at transparency and the frequency of

[1] Access Now, https://www.accessnow.org/
[2] Access Now, https://www.accessnow.org/the-urgent-needs-for-mlat-reform/

consultation with civil society groups. This document is our reflection of the current state of play of cross-border access to information, and seeks to provide helpful commentary to the Commission's investigation.

In our feedback **we followed the structure and numbering of the Commission's report.**

1.1 Expert process

The approach taken by the Commission in consulting a number of stakeholders in this process has been thorough and inclusive. The Member State questionnaire on cross-border access to electronic evidence provides a detailed overview of national-level problems and approaches currently faced by law enforcement and paints the most suitable background for this investigation; that there is no common approach to obtain cross-border access to digital evidence. While the overview in the report is helpful, it would be immensely useful for academia and civil society to be able to access the individual responses to scrutinize the situation on national levels.[3]

1.2.1. Direct cooperation, in particular when the service provider is outside the domestic jurisdiction

There are two causes for concern regarding the state responses to this question. First, is the discrepancy with which member states view applicability of their requests in regards to the receiving company; the fact that 8 Member States already have agreements with foreign service providers seems to warrant its own investigation by the Commission, if only to review the compatibility of these agreements with EU legal standards, in particular with Article 48 of the Charter of Fundamental Rights of the European Union (the Charter).

Such an evaluation must be a part of a comprehensive human rights impact assessment which should precede any further steps of the Commission's investigation into this matter.

Second, the disparity between categories of data by the various member states is cause to worry regarding the compatibility of domestic regimes with the incoming General Data Protection Regulation[4], the Police Directive, and the current e-Privacy Directive and its new proposal. Regardless of the exact scope of application of the different legal regimes, Article 7 and 8 of Charter on the fundamental rights to privacy and data protection apply. Given the inconsistency of the terminology used by the member states it is extremely difficult to judge the effectiveness of existing cross-border legal cooperation.

Recital 2 of the Police Directive lays down that "[t]he principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data." Following from the obligations to respect fundamental rights, this principle should be taken into account for the definition of connecting factors.

[3] There is a pending freedom of information request for the national-level responses to the questionnaire, which was filed in December 2016 and remains unanswered to date; https://www.asktheeu.org/en/request/responses_to_the_questionnaire_o#outgoing-7890

[4] Regulation (EU) 2016/679, http://eur-lex.europa.eu/eli/reg/2016/679/oj

1.2.2. Mutual Legal Assistance (MLA) with third countries

Many of the problems highlighted by member states in this category are among known issues endemic to the current MLA set-up.[5] The issue of insecure and inadequate communications channels is appropriately highlighted by the Commission. Member States have national as well as EU-level obligations to respect individuals' rights to protection of personal data (Article 8 of the Charter) and confidentiality. Transmitting any category of data relevant to an investigation must be properly secured and should be adequately tracked; contrary to what the member state responses suggest.

1.2.3. Enforcement of jurisdiction in cyberspace

There are multiple issues for concern in this section, but none more so than the suggestion that if the existence of evidence, or its location is unclear, the member states proceed to file MLA requests on multiple fronts in a broad search for one which may potentially receive a response. While we respect the frustration that not knowing the location of potential evidence can cause to an investigation, the state response to this question needs to be in line with the criteria set out in the Necessary and Proportionate Principles which state that, "All agreements for the international transfer of Protected Information must include human rights safeguards. States should only initiate and maintain full cooperation relationships with States whose justice systems adequately protect human rights. States should ensure that any request for User Data complies with international law and policies and human rights."[6] The practical application of the safeguards outlined in the Principles can further be examined through the Access Now Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance.[7] See our comments for unknown locations also at section 2.3.3.

Summary

There are several relevant issues raised by the member states regarding the dysfunctionality of the existing MLA system and issues of current cross-border cooperation. However, as demonstrated above, there are several instances where the Commission should have increased cause for concern over the gaping disparity between existing national-level approaches. In line with the Commission's commitment to better regulation as well as the REFIT platform, a thorough human rights impact assessment must precede any further investigation into the matter of improving criminal justice in cyberspace.[8]

---

[5] Similar issues and more have been identified by our own study into Mutual Legal Assistance Treaties, including the failure to properly protect user information and privacy. More at: https://www.accessnow.org/the-urgent-needs-for-mlat-reform/

[6] 13 International Principles on the Application of Human Rights to Communications Surveillance; https://en.necessaryandproportionate.org/

[7] Access Now implementation guide of the Necessary and Proportionate Principles: https://necessaryandproportionate.org/files/2016/04/01/implementation_guide_international_principles_2015.pdf

[8] The Commission has repeatedly committed itself to improve legislation through evidence-based law making and thorough impact assessments of considered legislation; https://ec.europa.eu/info/law/law-making-process/better-regulation-why-and-how_en

2.1 Cooperation with service providers

In the progress report, the Commission correctly identifies a number of issues which stem from direct cooperation between a member country and a service provider, often located in a third party outside the EU legal framework. The identified issues of transparency, accountability, attribution, reliability and authenticity are key concerns for all stakeholders involved. As the Commission rightfully points out, there are severe obstacles when it comes to enforcement in remote jurisdictions -- an issue which is entirely unpatchable through an informal extrajudicial direct cooperation agreement between a government and industry.

The progress report makes it appear that the variance in percentage figures regarding complying with requests is a problem at the platform level. This ignores the fact that agencies across different states may be sending wrongful, improper requests, resulting in legally justified pushback from companies.[9]

These democratic deficiencies of direct cooperation cannot be overcome outside the framework of rule of law, and based on its own analysis, the Commission should therefore focus on creating a functional legal framework; updating and re-negotiating the MLAT infrastructure to better respond to the fast-paced needs of law enforcement; not attempting to circumvent it. Under MLATs, individuals retain the same rights and legal standards which they would in a purely domestic investigation. It is essential that for the sake of transparency, accountability and redress, there is a functional legal mechanism in place rather than an ad-hoc agreement with little traceability.

Problems with direct cooperation; UK - US case

Having identified the same issues as the Commission -- the fact that most tech companies are resident to the U.S., and under U.S. law cooperation with law enforcement in this matter is voluntary or prohibited depending on the type of data -- in July 2016, the U.S. government proposed a new piece of legislation which would empower the U.S. to reach an agreement with other governments, starting with the UK, to allow direct requests for users' data from any tech company within the U.S. It would also grant the U.S. government reciprocity to make direct requests to companies in the countries where agreements are reached. While this has been identified as a great opportunity "if done right", the current agreement fails to adequately safeguard individuals and their privacy.[10]

This proposed agreement would let a court — or, in some cases, a law enforcement official — in one country issue a legally binding order on a company in another country. This can significantly undermine legal protections and harm human rights. Law enforcement in the UK and elsewhere need to conduct valid investigations, and there should be appropriate tools to access data. But we cannot allow privacy safeguards to deteriorate, and, unfortunately, the proposed legislation does not guarantee that a partner country will

[9] Access Now Transparency Reporting Index, available at: https://www.accessnow.org/transparency-reporting-index/

[10] Analysis of the proposal by Jennifer Daskal, Associate Professor at American University Washington College of Law, https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity

respect human rights standards. Nor does it offer much-needed improvements for the existing MLAT system, rather, it circumvents the system entirely.[11]

In our analysis of the UK-US direct cooperation agreement, we have concluded there are four significant deficiencies in language and protections which would inherently translate to any similar agreements within other EU countries;

1. The vague nod to "adhere to applicable international human rights standards" sets a low standard and enables agreements with countries who have poor human rights records.
2. The inclusion of communications interception with immediate transmission (live wiretaps) has not been given the necessary heightened protections, as guaranteed under most national legislative frameworks.[12]
3. Direct cooperation which supersedes the established legislative framework will only broaden state level surveillance, which is increasingly causing concern throughout the EU.
4. This agreement does not address the issues endemic within the MLAT system, but rather places temporary fixes to the process.

When questioned by the Washington Post in February 2016, two members of the US administration admitted to this loose standard with matter-of-fact tone saying that "[British privacy protections] may not be word for word exactly what ours are, but they are equivalent in the sense of being robust protections." The official further clarified that it was not the intent of the agreement to establish a standard for legal process in the other country, stating that it would be undesirable for either party to start dictating a specific standard of protections.[13]

Summary

While direct cooperation with providers has been resorted to as a reaction to the malfunctioning MLAT system, it should not be adopted as a long term - or ideal - solution to the issue of cross-border access to e-evidence. The simplicity which comes from such simplified processes is the same simplicity which places human rights standards on the line, and displaces legal certainty for individuals.

[11] Access Now, https://www.accessnow.org/four-ways-new-proposal-bypassing-mlats-fails-human-rights/

[12] As demonstrated under the 'Initiative for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters.' Answers to the questionnaire on interception of telecommunications: http://www.statewatch.org/news/2011/may/eu-council-eio-quest-interception-14591-rev1-10.pdf

[13] Washington Post: The British want to come to America — with wiretap orders and search warrants, By Ellen Nakashima & Andrea Peterson, Published February 4, 2016; https://wpo.st/CKEe2

2.2 Mutual Legal Assistance and Mutual Recognition Proceedings

The Commission's assessment of the current issues with MLATs identifies three central issues. The requests take too long to be processed, the process is resource-heavy and complicated, and it lacks transparency. These issues have been repeatedly raised during MLAT reviews as well as having been voiced by civil society.[14] There is a clear need for the standardization of process between cooperating countries, as well as an increase in capacity and funding for the bodies processing the requests; both key issues which should be the focus of the Commission's MLAT reform process.

The European Investigation Order

This section of the report also focuses on the European Investigation Order (EIO), which will replace the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. The report concludes that the EIO "provides for deadlines, standardised forms, and a limited possibility to refuse the execution of requests." While the EIO is likely to streamline cooperation within the EU (still a hypothetical assertion at this time), as the Commission rightfully points out, it was not designed as an instrument to address the issues currently experienced under the MLATs.

In 2010, the Commission submitted comments to a draft of the EIO, stating that, "There is neither a proper impact assessment nor an explanatory memorandum that provides enough material to state that the draft Directive respects the Charter and the ECHR."[15] In this commentary, the Commission further asserted that the detailed statement which was provided in June 2010 is insufficient and misunderstands the provisions in the Charter and therefore "fails to identify and assess the more important fundamental rights potentially affected by this [EIO] proposal.[16] The absence of safeguards was also criticized by the European Data Protection Supervisor who noted the lack of any reference to data protection instruments in the EIO and said this "once again raise[s] the fundamental issue of the incomplete and inconsistent application of data protection principles in the field of judicial cooperation in criminal matters".[17] Based on this feedback, the wording of the respect for fundamental rights as well as the Charter was changed in the final version of the EIO, but no further satisfaction for the impact assessment, extension of safeguards or detailed direction was provided.

Based on the fact that there is no evidence of the functionality or efficiency of the EIO, nor its compatibility with EU standards for fundamental rights protections, it is an inaccurate expectation to say that the EIO will improve any of these problems with certainty - the Directive is meant to be fully transposed only in May 2017 with an evaluation to be carried

---

[14] Access Now, https://www.accessnow.org/the-urgent-needs-for-mlat-reform/
[15] JUST/B/1/AA-et D(2010) 6815;
http://ec.europa.eu/justice/news/intro/doc/comment_2010_08_24_en.pdf
[16] Refers to Council doc. 9288/10 ADD 2, Published in 23 June 2010
[17] European Data Protection Supervisor opinion on European Investigation Order, 18 October 2010, Para 28

out in May 2019.[18] There is a great danger to fundamental rights' standards if - as the report asserts - the EIO is to be used as a blueprint for cooperation with third countries/providers at this stage.

2.3 Enforcing jurisdiction in cyberspace

The issue of jurisdiction in cyberspace is a lively cause for debate among academics and policymakers alike. The two key arenas of debate (if somewhat Euro-centric); the Convention Committee of the Budapest Convention on Cybercrime (T-CY) plenary efforts mentioned in the report, as well as the Tallinn Manual 2nd ed., have provided little comfort or certainty on how to approach the issue.[19] The Commission's report points out that certain cases should not merit the involvement of a third country if the case does not pertain to an individual under their jurisdiction, which is a seemingly reasonable argument to make based on the evidence. However, no clear and uniform basis for jurisdiction has been established. Addressing this issue must not create legal uncertainty for individuals and their right to privacy, which the temporary national-level solutions have often done. Furthermore, as the Tallinn Manual 2.0 points out, "two or more States [may] often enjoy jurisdiction over the same person or object in respect to the same event."

2.3.3. The loss of location

This section focuses on one of the most contentious current issues of the digital sphere -- the issue of attribution.[20] While there seems to be a lot of buzz around attribution in terms of e-evidence and cyber crime, attribution as a problem applies to any type of investigation in the analog world as well, and the same protections for individuals must apply in both of those instances. Far too often, is the chase for perfect attribution a reason to steamroll individual's rights to privacy, freedom of expression, and presumption of innocence which is the cornerstone of the fundamental rights recognized in the Charter within the area of criminal justice. Attacking anonymization or encryption tools, a tactic witnessed increasingly often both within and outside of the EU, creates far more risks for individuals than it brings solutions.

While the issue of attribution is a serious obstacle for investigations, the solution must not pose a risk to anonymity, encryption or other digital security tools currently under use. According to a report from the United Nations special rapporteur on freedom of expression, David Kaye, encryption and anonymity on the internet are necessary for the advancement of human rights.[21] In his report, he asserts that privacy is a "gateway for freedom of opinion and expression," and therefore encryption and anonymity "deserve strong protection" because they "enable individuals to exercise their rights to freedom of opinion and

[18] DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL; http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN
[19] Lawfare Blog: The Tallinn Manual 2.0, Sovereignty 1.0, Andrew Keane Woods; https://www.lawfareblog.com/tallinn-manual-20-sovereignty-10
[20] See coverage by WIRED: https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/
[21] David Kaye, Report on encryption, anonymity and the human rights framework, Published May 2015 http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

expression in the digital age." Kaye specifically advises that states should not restrict encryption and anonymity through blanket prohibitions which fail the necessary and proportionate test.[22] He further advises against state use of measures which would weaken the security individuals may enjoy online, such as through backdoors, weak encryption standards and key escrows.

The loss of location in investigations, cannot be solved by arbitrarily de-anonymizing or de-stabilizing the internet's architecture. The report hints that several member states have taken to "alternative measures" which include "accessing an information system remotely." While, government hacking has been repeatedly cited as the new age solution to secure infrastructure and systems, there are still human rights standards which must be respected and safeguards which must be implemented for this investigation tools to fall within the lines of rule of law.[23]

It must be acknowledged, that all government hacking substantially interferes with human rights, including the right to privacy and freedom of expression. While in many ways this interference may be similar to more traditional government activity, the nature of hacking creates new threats to human rights that are greater in both scale and scope. Hacking 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. In addition, we reason that more information about the history and the extent of government hacking is necessary to determine the full ramifications of the activity. The Commission should consider these adverse impacts of member states current practices and take care not to expand, but rather limit, their breadth.[24]

3. Avenues for Further exploration

3.1. Practical Improvements

The Council's request for the streamlining of mutual recognition procedures fits in line with the general need to update the MLAT mechanism. The use of e-CODEX, and existing secure system for the exchange of legislative documents (and ease of cross-border legal procedures), is a good way to create this interoperability and streamline communication within Europe. However, both the e-CODEX as well as the EIO are not appropriate

[22] 13 International Principles on the Application of Human Rights to Communications Surveillance; https://en.necessaryandproportionate.org/
[23]Access Now, A Human Rights Response to Government Hacking; https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf
[24]Access Now, A Human Rights Response to Government Hacking; https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

mechanisms to address the issue of cooperation with third countries and companies with seats in foreign countries. Both of those tools were created for a much more limited use and should not be repurposed without adequate impact considerations and due safeguards.

As mentioned in our comments on section 2.2., several questions around the application of the EIO remain; its potential as an enabler of mass scale surveillance as well as broader human rights considerations - or lack thereof - have remained unaddressed by the Commission for several years.[25] It is therefore inappropriate, to begin considering repurposing an untested framework to a much broader scale, which, as suggested in the report, could include cooperation with third countries and possibly direct cooperation with service providers. The implications of this broad authority under the EIO could have detrimental impacts on individual's rights -- a concern which cannot be disregarded until a proper impact assessment on the application of the EIO to these broader uses is conducted. It is the Commission's responsibility and obligation to create evidence-based legislation, something which would be entirely absent in this broad repurposing of the EIO framework.

The remainder of this section is dedicated to very tangible policy improvements for law enforcement communication with service providers; all of which should be encouraged, although not in order to circumvent MLATs, but rather to supplement or improve them. The broader introduction of a direct point of contact, standardized and unified approaches as well as training for law enforcement are all very tangible ways in which to improve the functionality of the MLAT system as a whole while maintaining the legal certainty these treaties guarantee.

While companies whose data are subject to information requests can play a significant role by clarifying their own jurisdictional requirements and by taking clear positions on the standards they believe govern the transfer of data, Access Now has previously suggested that governments undergo a number of complementary means of fixing the MLAT problem;[26]

- Protect users through adequate human rights safeguards by requiring the requesting state to certify that it has adequate human rights protections in place, creating clear guidelines for handling emergency cases, and using a dual criminality standard;
- Reduce legal uncertainty and inconsistency by making clear which laws apply in which situations and applying higher standards for more sensitive information;
- Remove inefficiency and delays by improving resources, using electronic request forms, and designating a single agency as a point of contact;
- Create transparency through publicizing clear, easily accessible information covering the way in which online records are shared with foreign law enforcement and by providing notification of access;
- Establish accountability, remedies, authentication, and oversight;

[25] Statewatch Analysis, The proposed European Investigation Order: Assault on human rights and national sovereignty. By Steve Peers, Professor of Law, University of Essex. Published May 2010 http://www.statewatch.org/analyses/no-96-european-investigation-order.pdf
[26] https://www.accessnow.org/the-urgent-needs-for-mlat-reform/

- Provide accessibility for defendants by permitting governments to seek records on their behalf;
- Promote comprehensive geographical coverage; and
- Keep up with technological changes.

We encourage the Commission's focus on these improvements, and the integration of these suggestions into the MLAT update process rather than seek to circumvent them.

3.2. Middle- to long-term solutions

Given the clean-cut solutions proposed in the previous section on improving cooperation, the strategies explored in 3.2. seem both disproportionate and unnecessary. While the increase in funding is a lucrative reason to expand a program, these resources can be directed at executing the aforementioned improvements and streamlining the underfunded MLATs in general - thus improving an existing program rather than re-inventing the wheel. The Commission's proposal in this report to further pursue the idea of unmediated forms of cross-border access to electronic evidence - as defined in the report - is entirely unacceptable from a human rights perspective.

Conclusion

There are real problems with the current MLAT process. Bilateral agreements could help us address the inconsistency, inefficiency, and lack of support that law enforcement faces in current systems for data access. Better systems would reduce the incentive for data localization laws, encryption mandates, and overuse of national security authorities. However, if we don't do it right, these agreements could also do irreparable damage to global human rights. They could end up lowering legal standards, decreasing transparency, and blocking avenues for access to remedy. A better process could be created, and if properly targeted and robustly implemented, could help law enforcement get expedited access to important data in the most urgent criminal cases. However, such a framework must guarantee human rights protections. The simple fact that evidence is electronic does not do away with due process guaranteed under the Charter. It is essential that the Commission focuses its efforts on strengthening the MLAT process rather than creating alternate extrajudicial avenues with predetermined expiration dates.

There is a need to shift this investigation from a questionnaire-based inquiry to an evidence-based policy project; this requires the inclusion of robust human rights impact assessments and evaluations of current smaller frameworks - such as the EIO. Simply settling for the fact that there is no conclusive statistic to support whether a framework functions or not is no basis for furthering its scope and reach; it does not do justice to the human rights commitments the EU has signed up to.

We will be looking forward to the comprehensive options paper which is meant to be delivered by June 2017, as well as further meetings and opportunities to discuss this complex issue with all interested parties.

****

For more information, please contact:

Lucie Krahulcová
EU Policy Associate
lucie@accessnow.org

-or-

Fanny Hidvégi
European Policy Manager
fanny@accessnow.org