28 June 2018

Joint Civil Society Response to Discussion Guide on a 2nd Additional Protocol to the Budapest Convention on Cybercrime

T-CY (2018)16

The Electronic Frontier Foundation (EFF), European Digital Rights (EDRi), Association for Civil Rights (ADC), Derechos Digitales, Elektronisk Forpost Norge (EFN), IPANDETEC, Karisma Foundation, OpenMedia, Panoptykon Foundation, R3D: Red en Defensa de los Derechos Digitales, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), SonTusDatos (Artículo 12, A.C.) and TEDIC welcome this opportunity to engage with the Council of

Europe and State Parties involved in the elaboration of an additional Second Protocol to the Convention on Cybercrime (also known as the Budapest Convention).

EFF is an international civil society non-governmental organization with more than 39,000 members in 99 countries throughout the world. EFF is dedicated to the protection of individuals' online civil rights, privacy, and freedom of expression. EFF engages in strategic litigation in the United States, and works in a range of international and national policy venues to promote and protect human rights, foster innovation, and empower consumers.

European Digital Rights (EDRi) is an association of civil and human rights organisations from across Europe. We defend rights and freedoms in the digital environment.

Association for Civil Rights (ADC) is a civil society organization created in 1995, based in Buenos Aires (Argentina). ADC contributes to strengthening the legal and institutional culture that guarantees fundamental rights of individuals, based on respect for the Argentinian Constitution and democratic values. ADC promotes civil and social rights in Argentina and other Latin American countries.

Artículo 12 is a non-profit organization that defends the fundamental rights to privacy and data protection of all people in Mexico, but also throughout Latin America, in particular the rights of Internet and other information and communication technology users in the digital realm. It takes its name from Article 12 of the Universal Declaration of Human Rights of the United Nations, which guarantees the protection of privacy. SonTusDatos is the online data protection program of Artículo 12.

Derechos Digitales - América Latina is an independent non-governmental organisation, founded in 2005, with main offices in Santiago de Chile, dedicated to the defence and promotion of fundamental rights in the digital environment in Latin America.

Electronic Frontier Norway (EFN) is a cross-profession and cross-political organization furthering human rights in the digital world. Privacy, freedom of expression and equal access to information as essential liberties have been well established in the analogue realm. EFN fights for their equal importance in the digital realm.

IPANDETEC: We are a non-profit organization that promotes the use and regulation of ICT and the defense of Human Rights in the digital age, through analysis, advocacy, research, and legislative monitoring of Internet public policies in Central America.

Karisma Foundation seeks to respond to the opportunities and threats that arise in the context of 'technology for development' for the exercise of human rights. It approaches its work from perspectives that promote freedom of expression and gender and social equities. It approaches activism from multiple angles—both legal and technology, in coalitions with local, regional and international partners.

OpenMedia is a community-driven organization that works to keep the Internet open, affordable, and surveillance-free. We operate as a civic engagement platform to educate, engage, and empower Internet users to advance digital rights around the world.

Panoptykon Foundation was founded in 2009 to protect freedom and human rights in the context of electronic surveillance, used for commercial or security reasons. Our mission is to keep surveillance policies and practices under social control. We believe that surveillance measures should only be allowed when necessary to pursue legitimate goals determined by the society, not those in power. We monitor legislative process in Poland and at the EU level, take legal interventions (including strategic litigation), work with the media, and engage in cultural and educational activity.

R3D: Red en Defensa de los Derechos Digitales is a Mexican non-profit dedicated to defend and promote human rights in the digital environment. Since 2014, we develop and apply research, advocacy, communications, and strategic litigation strategies to ensure the exercise of rights such as freedom of expression, privacy, non discrimination, access to information technologies, access to knowledge, and free culture.

The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is a legal clinic based at the Centre for Law, Technology & Society (CLTS) at the University of Ottawa, Faculty of Law. Its core mandate is to advocate in the public interest on matters that arise at the intersection of law and technology.

TEDIC: A not-for profit organization from Paraguay that works on civic, open technology for social change and defends digital rights.

We respectfully submit the following comments organized according to the structure set out in the Discussion Guide issued in support of this consultation:

1. Background

We are civil society organisations from different parts of the world that defend, promote, and protect human rights and fundamental freedoms online.

We are part of a broader coalition of public interest organisations which is ready to closely follow the negotiations regarding the addition of a Second Protocol to the Budapest Convention.[1] We would like to reiterate that transparency and opportunities for input are needed continuously throughout the developing of the process. This ensures that civil society can listen to Member

[1] Nearly 100 Public Interest Organizations Urge Council of Europe to Ensure High Transparency Standards for Cybercrime Negotiations", April 3, 2018, https://www.eff.org/deeplinks/2018/03/nearly-100-public-interest-organizations-urge-council-europe-ensure-high

States, and provide targeted advice to the specific discussions taking place on an ongoing basis. Our opinions can build upon the richness of the discussion among States and experts, a discussion that civil society will miss if we are not invited to participate throughout the process. States and civil society need to fully engage with each other to achieve meaningful and mutually beneficial transparency and accountability in governance.

Our response will be open to endorsement by other NGOs until 5 July, before the 19th Plenary of the Council of Europe's Cybercrime Convention Committee (T-CY).

Supporting Documentation:

- Global Civil Society Submission to the Council of Europe, "Comments and Suggestions on the Terms of Reference for Drafting the Second Optional Protocol to the Cybercrime Convention", September 8, 2017. https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf

- Letter to Secretary-General Jagland regarding Cybercrime Negotiations, and Transparency, April 3, 2018. https://edri.org/files/letter-cybercrimenegotiations-and-transparency_20180403_EN.pdf

- International Principles on the Application of Human Rights to Communications Surveillance (Necessary & Proportionate principles), https://necessaryandproportionate.org/principles

2. Objective of our response

The elaboration of an additional Protocol can be an opportunity to avoid a race to the bottom regarding human rights safeguards and standards. Avoiding a race to the bottom can start by ensuring inclusive and transparent participation of civil society, and by ensuring our concerns, recommendations and suggestions are duly taken into account.

3. Issues for discussion

3.1. Context: Rationale for the Protocol – Recap and recent developments

a Question: What are the implications of these developments for work on the Protocol?

▸ Setting the scene

Thorough criminal investigations are of utmost importance. We acknowledge the need for law enforcement authorities to investigate crimes. Some of the conversations about cross-border access to data are driven by the fact that Mutual Legal Assistance Treaties (MLATs) are often slow and inefficient, and that big U.S.-based service providers in particular do not provide all the information certain law enforcement authorities may need. However, it is important to recall that:

- We live in a golden age of surveillance. Technology is giving new opportunities to law enforcement and intelligence agencies to access more information about people's lives than ever before.[2] That means that the level of interference with human rights and fundamental freedoms is unprecedented. For example, metadata has been proven to be more useful and more revealing than the content of our communications—regardless of whether data is encrypted or not. Yet metadata is often treated as less private and accorded lower levels of protection against state intrusion than content.

- It is important to learn from experience and adopt policy decisions based on evidence and anchored in a strong human rights framework. For example, the imposition of telecommunications data retention as a law enforcement tool led to the existence of an EU instrument that was declared illegal by the Court of Justice of the European Union,[3] and a variety of national laws that are not compliant with case law of the European Court of Human Rights and the Court of Justice of the European Union.[4]

- Mutual Legal Assistance Treaties (MLATs) are a long-established system for dealing with cross-border access to data requests. MLATs are often misrepresented as being categorically unsuitable for dealing with electronic evidence. The reality is that the challenges raised by the MLAT system are procedural, not substantive in nature. Significant improvements to MLAT procedures are possible, and indeed some have already been made—as evidenced by the recent major improvements in the efficiency of U.S. Department of Justice MLAT processing mechanisms. Thanks to the "MLAT Reform" program,[5] the U.S. DoJ recently reduced the amount of pending cases by a third. MLATs are not perfect, and we acknowledge the need to improve them. In fact, we urge all Parties to the Budapest Convention to consider MLAT reform first before looking at whether further cooperation mechanisms are necessary. We welcome the T-CY's efforts to focus on MLAT reform, and would welcome any opportunity to meaningfully discuss with the Council of Europe, State Members, and Observers on how to fix some of their problems.

▸ Relevant international developments

---

[2] Article 29 Data Protection Working Party, Statement of the WP29 on Encryption and their Impact on the Protection of Individuals with Regard to the Processing of their Personal Data in the EU", April 11, 2018, http://www.dataprotection.ro/servlet/ViewDocument?id=1476; See also: "Shining a Light on the Encryption Debate: A Canadian Field Guide", May 2018, *The Citizen Lab & CIPPIC*, https://cippic.ca/uploads/20180514-shining_a_light.pdf, pp 84-89.

[3] Kirsten Fiedler, "European Court Overturns EU Mass Surveillance Law" April 8, 2014, *EDRi.org*, https://edri.org/european-court-overturns-eu-mass-surveillance-law/.

[4] Privacy International, "A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws Since the CJEU's Tele-2/Watson Judgment", September 2017, *Privacy International*, https://www.privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf; Jesper Lund, IT-Pol, "EU Member States Fight to Retain Data Retention in Place Despite CJEU Rulings", May 2, 2018, *EDRi.org*, https://edri.org/eu-member-states-fight-to-retain-data-retention-in-place-despite-cjeu-rulings/.

[5] United States, Department of Justice, "FY 2019 Budget Request: Other Key Increases", https://www.justice.gov/file/1033596/download.

The implications of the developments identified in the Discussion Guide for work on the Protocol are manifold, including the following:

- These developments risk bypassing MLATs altogether. Recognising inefficiencies of MLATs should not translate into MLATs being bypassed. Both the U.S. CLOUD Act and the European Commission proposals on e-evidence propose short-cuts for law enforcement taking out several basic human rights safeguards, and shifting the burden to service providers (which do not have the same human rights obligations that States do). This has major implications for human rights and fundamental freedoms online, including due process and defence rights.

- Developments in the United States of America and the European Union risk lowering the standards at a global level. These new proposals ignore critical privacy obligations in order to facilitate easy access when facing data requests from foreign governments.[6]

- The proposed EU approach put emphasis on the representation of service providers without taking due account of the State of the nationality of the data subject or where the data subject resides. This can have implications for defence rights, human rights protection, and unintended consequences in other countries. For example, if the European Union asks service providers to set a representative in the European Union to specifically respond to, and potentially be liable for, production orders from competent authorities, the EU is at the same time inviting other (non-EU) countries to do the same against providers established in the European Union that offer services elsewhere (e.g. India or China). This is important because not all Parties to the Budapest Convention and potential signatories to the forthcoming Second Protocol share the same level of human rights protection and enforcement mechanisms.

- These developments cover the access to data, not its use or transfer. In view of several Parties not part of Convention 108 or the Council of Europe, this creates significant concerns in terms of their procedural laws, data protection, and privacy legal frameworks. The U.S., for example, does not have a comprehensive data protection framework. We advise the T-CY to ensure that any and all signatories of the Cybercrime Convention and its forthcoming additional Protocol also sign, ratify, and properly implement Convention 108+ of the Council of Europe.

Supporting Documentation:

- Katitza Rodriguez, "A Tale of Two Poorly Designed Cross-Border Access Regimes", April 25, 2018, *Electronic Frontier Foundation*, https://www.eff.org/deeplinks/2018/04/tale-two-poorly-designed-cross-border-data-access-regimes

[6] Katitza Rodriguez, "A Tale of Two Poorly Designed Cross-Border Access Regimes", April 25, 2018, EFF.org, https://www.eff.org/deeplinks/2018/04/tale-two-poorly-designed-cross-border-data-access-regimes

- Kirsten Fiedler, "European Court Overturns EU Mass Surveillance Law" April 8, 2014, *EDRi.org*, https://edri.org/european-court-overturns-eu-mass-surveillance-law/

- Privacy International, "A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws Since the CJEU's Tele-2/Watson Judgment", September 2017, *Privacy International*, https://www.privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf

- Jesper Lund, IT-Pol, "EU Member States Fight to Retain Data Retention in Place Despite CJEU Rulings", May 2, 2018, *European Digital Rights*, https://edri.org/eu-member-states-fight-to-retain-data-retention-in-place-despite-cjeu-rulings/

- Article 29 Data Protection Working Party, Statement of the WP29 on Encryption and their Impact on the Protection of Individuals with Regard to the Processing of their Personal Data in the EU", April 11, 2018, http://www.dataprotection.ro/servlet/ViewDocument?id=1476

- Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", May 2018, *The Citizen Lab & CIPPIC*, https://cippic.ca/uploads/20180514-shining_a_light.pdf

- United States, Department of Justice, "FY 2019 Budget Request: Other Key Increases", https://www.justice.gov/file/1033596/download

3.2. Provisions for more efficient mutual legal assistance

b Question: Would civil society, data protection, or industry organisations have any comments on such proposals?

▸ In general

Absolutely. Civil society is willing to provide comments on proposals to render MLATs more efficient. For that, it would be helpful if we could participate in expert conversations, and provide feedback to the T-CY in writing in every step of the process.

Prioritising MLAT reform is the right policy option and the logical thing to do, since it is a long-established, tried and tested mechanism. We should be cognisant of the fact that existing conditions and legal safeguards, for example with regard to the necessity and proportionality of data retention rulings, are being wilfully ignored in the EU. We should also urge you to consider the efficiency and implementation of the current European Investigation Order Directive in the European Union, including its impact on fundamental rights in practice; and the complementary

nature of the EU and national frameworks in relation to the forthcoming Second Protocol to the Cybercrime Convention.

In addition, practical measures can ease the difficulties identified by law enforcement authorities. These can include setting up a global and secure online portal; better training for law enforcement authorities on human rights safeguards and how to use MLATs; simplifying and standardising forms; establishing single points of contact, etc.

Particularly with regards to the items identified in the Discussion Guide:

▸ Emergency mutual legal assistance

Emergency MLA procedures are a worthwhile inquiry for this body to pursue. They would provide a mechanism for countries to access the data in foreign countries necessary to prevent an emerging life-threatening situation, but also provide an opportunity to create strong privacy protections for this process.

If this body creates emergency MLA procedures, it is necessary to create a narrow definition of an emergency situation so they are not used as a work-around to the standard MLA process. Existing EU law and interpretations of the EU Data Protection authorities[7] on "vital interests" could form a basis for this, as could the U.S. doctrine of "exigent circumstances." An emergency situation typically requires an imminent threat of death or serious bodily harm to an identifiable person or group. This standard allows some flexibility, but should be used with extreme caution, and only when it is not possible to obtain a probable cause warrant signed off by a judge before the prevention of an imminent threat of death or serious harm. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation since the potential evidence can be obtained using a data preservation order (Article 17, Budapest Convention), nor should the loss of evidence be grounds to receive information under emergency MLA procedures in the first place.

Emergency MLA procedures should only be used for questions or life or death or, at the very least, to prevent validly established and immediate serious harm to identifiable people or groups, and should also not be used for the investigation of financial or property crimes.

For a country to request information under emergency MLA procedures, a Party to the Convention should not only demonstrate the existence of the emergency situation but should only access information that they would otherwise be able to receive during the normal MLA process if the emergency was not present. The country should demonstrate four factors:

[7] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article of Directive 95/46/EC, 844/14/EN, WP217, adopted April 9, 2014, http://www.dataprotection.ro/servlet/ViewDocument?id=1086.

- There are reasonable grounds to believe an immediate risk of danger to human life or serious bodily harm to an identifiable person or group;
- Access to information stored in another country is necessary to prevent that serious harm;
- There is not time, with due diligence, to use the standard MLA process;
- There are grounds to believe that the requesting Party would be able to access the information through the standard MLA process.

Emergency mechanisms raise serious potential for abuse in transborder contexts. The basis for an emergency MLA must be established in sworn statements, and there must be accountability mechanisms for misuse of these procedures. These accountability mechanisms could include penalties for blatant or systemic misuse of emergency powers by a Party to the Convention.

An auditing process should also be in place. After receiving information from an internet service provider through an emergency MLA procedure, the Parties should then submit an MLA request through standard procedures to ensure that grounds existed for access to that information. In the case where a country is denied access to that information under a standard MLA request, all information received during the emergency MLA procedures should be deleted once the danger has passed and cannot be used for future investigatory or prosecution purposes. To further ensure emergency procedures are not being abused, the requesting state should leave a paper trail to facilitate this audit process.

Statistical and qualitative reporting on the volume of emergency requests should be published by both requesting and responding Parties on an annual basis. While this should be the case for all manner of MLA procedures, it is particularly vital for emergency mechanisms given their potential for over-reach.

▸ Language of requests
▸ Audio/video hearings

These can be practical solutions to ease some difficulties identified in MLA processes. We reserve these points to other stakeholders with expertise on these issues, as these two items would fall outside our scope of work.

▸ Joint investigation teams.

Joint investigation teams can render investigations more effective. However, these are only acceptable provided they respect basic principles of international law. As already stated, in practice, this means that the way in which joint intelligence task forces work (such as the NSA-GCHQ joint bases) should not be replicated on the law enforcement level.[8] Legal safeguards should be implemented to protect against risks of a joint task force, such as when one country

[8] Global Civil Society Submission to the Council of Europe, "Comments and Suggestions on the Terms of Reference for Drafting the Secodn Optional Protocol to the Cybercrime Convention", September 8, 2017, https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf.

attempts to bypass domestic safeguards. Additional oversight could include joint due diligence, obligations of clear logging and monitoring and public reporting, in order to ensure that accountability.

Supporting Documentation:

- Global Civil Society Submission to the Council of Europe, "Comments and Suggestions on the Terms of Reference for Drafting the Second Optional Protocol to the Cybercrime Convention", September 8, 2017, https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf

- Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article of Directive 95/46/EC, 844/14/EN, WP217, adopted April 9, 2014, http://www.dataprotection.ro/servlet/ViewDocument?id=1086

3.3. Direct cooperation with providers across jurisdictions

c Questions: Can current practices by US providers be generalised in a Protocol?

i. With regard to subscriber information?

▸ Voluntary disclosure [of subscriber information] by service providers

We acknowledge that direct cooperation between Parties and service providers outside those Parties' respective territories can—in appropriate circumstances—have benefits to all involved. However, the current practices by U.S. providers cannot be generalised for inclusion in a Protocol.

As noted in the Discussion Guide, U.S. providers are governed in their scope of voluntary cooperation by the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2702. Section 2702 permits providers to voluntarily disclose non-content data to persons other than "to any governmental entity." *Id*. Due to the way "governmental entity" is defined in section 2711, only U.S. federal, state, and local entities are considered governmental; foreign states are not.

Because ECPA was drafted more than 30 years ago, it may be that the drafters simply did not anticipate foreign government requests to US based providers, who at the time generally provided local service to local users. Indeed, the current functioning of ECPA results in providers being permitted to voluntarily turn over non-content data to certain non-U.S. government entities but being prohibited to do so to U.S. government entities.

But beyond the uneven application of U.S. law that allows non-U.S. law enforcement to request non-content data outside of the MLAT process, generalising U.S. providers' practice would be inconsistent with the domestic frameworks of several Parties. For instance, in 2014 the Supreme

Court of Canada has ruled that it is a violation of Section 8 of the Canadian *Charter of Rights and Freedoms* for a Canadian provider to disclose subscriber data to any entity without prior judicial authorisation. *See R. v. Spencer*, 2014 SCC 43, [2014] S.C.R. 212.

In its decision, Canada's highest court recognised the importance of online anonymity to maintaining the constitutionally protected right to privacy in the digital era. The decision specifically held that individuals can reasonably expect that the state will not seek to identify their otherwise anonymous online activity by asking their Internet Service Provider to voluntarily disclose their subscriber data. Further, Canadian law enforcement cannot ask ISPs to voluntarily identify customers associated with anonymous online activity. Also, Canada's federal data protection statute, PIPEDA, was held to prevent ISPs from voluntarily identifying customers associated with anonymous online activity. The typical identification scenario at issue in *Spencer*—disclosing the name and address of a customer whose IP address is associated with known anonymous online activity—is now only effectively permitted where a production order is issued by a court or in emergency situations.

This decision is in line with a growing trend around the world recognising the greater sensitivity demanded by online anonymity. In his seminal report on encryption and anonymity, David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, highlighted the importance that online anonymity plays in furthering free expression in digital contexts (A/HRC/29/32, paras 47 et seq). More recently, the Fourth Section of the European Court of Human Rights held that the human right to private life encompasses an individual's interest in having her identity with respect to her online activity protected (*Benedik v Slovenia*, App No 62357/14, April 24, 2018 (ECtHR 4th Section), para 119) and that individuals maintained a reasonable expectation that their otherwise anonymous online activity will remain anonymous, even where the individual takes no steps to shield her/his IP address from third parties. Compelling an ISP to identify its customer was held to be "manifestly inappropriate" in this context, as the mechanism relied upon offered "virtually no protection from arbitrary interference" with the right to privacy (para 129). The ECtHR stopped short of being clearer about requiring a court order in all contexts where subscriber data is obtained, but *Benedik v Slovenia* further cements a growing recognition of the important anonymity interests inherent in subscriber data. We further note that in doing so, the ECtHR specifically considered the Budapest Convention and emphasised that, pursuant to Article 15 thereof, data access under the Convention must be "appropriate" in view of the nature of the procedure or power concerned (paras. 126 - 129).

Because current law regarding the ability of providers to voluntarily provide subscriber and non-content data varies widely, and current US practice is less rights-protective than some Parties' law, we urge that no legal provisions in the Protocol be adopted to generalise US practice.

ii. For disclosure of other data in emergency situations?
See our response to 3.2.

Supporting Documentation:

- David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/29/32, May 22, 2015, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

- *Benedik v Slovenia*, App No 62357/14, April 24, 2018 (ECtHR 4th Section) http://www.bailii.org/eu/cases/ECHR/2018/363.html

- *R v Spencer*, 2014 SCC 43, [2014] S.C.R. 212, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

- Tamir Israel, "Subscriber Data in Canada: Backgrounder", March 3, 2017, *CIPPIC*, https://cippic.ca/uploads/20170303-Subscriber_data_in_Canada-Backgrounder.pdf

- Tamir Israel & Christopher Parsons, "Digital Anonymity & Subscriber Identification Revisited… Yet Again", October 6, 2016, *The Citizen Lab / CIPPIC*, https://citizenlab.org/wp-content/uploads/2016/10/20161005-CNSCI-RevisitingAnonymityYetAgain.pdf

d Question: What rules/regulations or other factors prevent providers from voluntarily disclosing subscriber information to criminal justice authorities from other jurisdictions?
See our responses to 3.3 c i.

e Questions: Connecting factors: in what circumstances may service providers be subject to a domestic production order?
Extraterritorial jurisdiction has been traditionally defined by domestic law. The various approaches to jurisdiction among Parties have different bases, as recognised by the three "connecting factors" listed in the Discussion Guide, namely:

i. "Real and substantial connection" to a Party;
ii. Offering a service in the territory of a Party;
iii. Or otherwise "established" in the Party.

Those various approaches resist reconciliation into a single global rule.

The question of under which circumstances a private entity may be subject to a domestic order has ramifications far beyond access to cloud data, e.g., copyright, trade law, tort law, labor and environmental law, etc. We urge that this body refrain from entering the briar patch that is the topic of cross-border jurisdiction in the limited context of the Cybercrime Convention Committee.

f Questions regarding data protection and other safeguards for voluntary disclosure:

i. Which data protection and other safeguards apply:

- **Legal framework of country of service provider?**

The principle of purpose limitation (GDPR article 5 1, b) must be respected as detailed in Article 5 of Convention 108. This states that data can only be stored for specified and legitimate purposes "and not used in a way incompatible with these purposes." The Convention's explanatory memorandum explains that "it should not be allowed to store data for undefined purposes."

It is clear that voluntary processing of data for law enforcement purposes is not compatible with the original data collection.

As a result, specific national law is needed for access to data, whose provisions would need to be in force and to comply fully with Articles 8 and 10 of the European Convention on Human Rights.

Such specific national law is a restriction on the right to privacy and freedom of expression and therefore needs to be "necessary in a democratic society" (Articles 8 and 10 of the ECHR) and, simultaneously, not sufficiently necessary to require a disclosure *obligation*.

Only in the most extreme cases should the data subject not be informed of the processing of the data.

- **Legal framework of country of requesting criminal justice authority?**

The requesting Party would obviously have to show a demonstrable nexus to the data being collected. The requesting Party must have an obligation to demonstrate that nexus at the request of the country of the service provider and the country where the data is stored. It would need to have domestic laws in place which would permit the disclosure and use of the data for the purposes in question as well as robust rules on informing the data subject that the data has been used in this way.

- **Legal framework of country where data is stored?**

As per the rules on the legal framework of the service provider.

- **Legal framework of country of data subject?**

All data subjects should be assured that they will be informed of their data being accessed at the earliest possible moment.

- **What if several countries are involved?**

We reserve comment on this point.

ii. On the part of the service provider as the data controller under European legal frameworks:

- **What conditions precisely have to be met to permit disclosure and which are the applicable provisions of the GDPR or Convention 108?**

Under the GDPR a specific legal basis would be needed for processing the data for an entirely different purpose from the one for which it was collected (in line with the basic principle of purpose limitation). Article 6 of the GDPR provides five specific and one general grounds for data processing, none of which would, without specific legislation, be appropriate in this context. We believe that Convention 108 should be understood in the same sense.

- **What would be considered a sufficient legal basis under the GDPR or Convention 108?**

A specific legal instrument would be needed to permit this. However, there is a logical contradiction between a disclosure that would be both "voluntary" and also "necessary in a democratic society," in line with Articles 8 and 10 of the European Convention on Human Rights.

As explained by the Article 29 Working Party Opinion 06/2014 and eloquently by the Court of Justice of the EU in its Opinion 01/15,[9] restrictions need to be provided for by law and, crucially, in paragraph 139, "*the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned.*" This concept is absolutely fundamental.

- **What constitutes a "legitimate interest" (Article 6.1.(f) GDPR) of a service provider in this context?**

Legitimate interest is not an appropriate legal basis for "voluntary" disclosure of data to the authorities of a foreign government. It does not appear to us to permit another interpretation. As explained in the WP29 Opinion 06/2014,[10] a specific legal basis is needed for processing personal data and "[F]urther, the legal obligation itself must be sufficiently clear as to the processing of personal data it requires."

---

[9] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article of Directive 95/46/EC, 844/14/EN, WP217, adopted April 9, 2014, http://www.dataprotection.ro/servlet/ViewDocument?id=1086; Opinion 01/15, Re Draft Agreement Between Canada and the European Union - Transfer of Passenger Name Record data from the European Union to Canada, July 26, 2017 (CJEU Grand Chamber).

[10] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article of Directive 95/46/EC, 844/14/EN, WP217, adopted April 9, 2014, http://www.dataprotection.ro/servlet/ViewDocument?id=1086

- **What are requirements for disclosure/transfers of subscriber information to “third countries”?**

This question appears to be fully addressed by the other questions in this section.

- **Would the derogations of Article 49 GDPR – such as Article 49.1 (f) – apply if data is required in a specific criminal investigation?**

A criminal investigation would normally apply to crimes that have already been committed. The above mentioned Article 29 Working Party makes it clear that this wording needs to be understood very narrowly. A vital interest that would be "essential for the life of the data subject or that of another natural person" appears to be a highly unusual circumstance that should not be provided for in an instrument such as the one that is currently under negotiation.

- **What is the meaning of Article 48 GDPR?**

Countries should not be permitted (this was nicknamed the "anti-FISA" provision by the Financial Times) to grant themselves the right to unilaterally gain access to data in other countries without a clear, robust legal framework.

iii. In the requesting country (that is, in the country of destination of data):

- **What conditions precisely have to be met to permit transfer to this country and which are the applicable provisions of the GDPR or Convention 108?**

Data cannot voluntarily be disclosed to the law enforcement authorities of foreign countries under the GDPR and Convention 108.

iv. What data protection and other safeguards must be met for the voluntary disclosure of data in other jurisdictions?

A specific legal instrument would be needed to permit this. However, there is a logical contradiction between a disclosure that would be both "voluntary", and also "necessary in a democratic society," in line with Articles 8 and 10 of the European Convention on Human Rights.

▸ Preservation of data by service providers

Brief review of current practices.

▸ Mandatory Preservation Orders for Stored and Traffic Data

We believe it's important to address the topic on mandatory preservation orders since those provisions have been included in the EU proposals on e-evidence.[11]

While the Budapest Convention itself foresees targeted preservation orders in Articles 16 (stored data), 17 (traffic data), 29 (expedited), and 30 (expedited disclosure of preserved traffic data) to be issued and assessed on a case-by-case basis, many States Parties have failed to implement those provisions. Facilitating compliance with these obligations amongst existing State Parties should be addressed prior to the adoption of any new mechanism for facilitating transborder preservation.

We would like to further caution that while the Budapest Convention envisions a distinction between orders forcing service providers to preserve data they have already collected and orders aimed at forcing service providers to intercept and record data in real time, there are not enough safeguards to prevent the misuse of proactive or 'ongoing' preservation orders, which could end up undermining this distinction.

In the U.S., for example, courts have determined that the preservation power cannot proactively compel service providers to preserve data such as email or text messages that are not yet in their possession or control at the time the order is issued or received.[12] Proactive preservation forces service providers to record data they would never have otherwise retained, effectively bypassing legal protections in place for real-time electronic interceptions. As the US Department of Justice (DOJ) notes in its manual on seizing electronic evidence, preservation orders:

> "...should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the electronic surveillance statutes..."[13]

While we generally warn against the inclusion of any additional mechanisms for preservation in the Second Protocol, if any such addition were to be made it must be clear that it may only be used to compel preservation of data already under the non-ephemeral possession or control of the service provider at the time the preservation order in question is issued, that it be limited in time, and that it comply with human rights law principles.

Supporting Documentation:

- Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article of Directive 95/46/EC, 844/14/EN, WP217, adopted April 9, 2014, http://www.dataprotection.ro/servlet/ViewDocument?id=1086

---

[11] Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 Final, April 17, 2018, Explanatory Report, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.
[12] *US v Warshak*, (2010), 631 F.3d 266, (US 6th Circuit), https://caselaw.findlaw.com/us-6th-circuit/1548071.html.
[13] United States, Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", *Office of Legal Education Executive Office for United States Attorneys*, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf, p 140.

- Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 Final, April 17, 2018, Explanatory Report, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN

- *US v Warshak*, (2010), 631 F.3d 266, (US 6th Circuit), https://caselaw.findlaw.com/us-6th-circuit/1548071.html

- United States, Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", *Office of Legal Education Executive Office for United States Attorneys, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

g Question: Can current practices by US-providers be generalised in a Protocol?

▸ Voluntary preservation of data by service providers

Despite a consistent general 'case by case' approach to assessing requests from foreign law enforcement to voluntarily preserve data, current U.S. provider practices are highly varied in their application.[14] For example, Google will preserve indefinitely upon receipt of a signed letter, while Facebook will preserve only 90 days and only pending receipt of formal legal process. At the same time, under U.S. law, specifically the Electronic Communication Privacy Act (ECPA) Section 2703(f), U.S. authorities cannot request voluntary preservation of data from US providers at all.

Given the wide variance in how U.S. providers currently treat foreign data preservation requests, and the U.S. law prohibition on voluntary preservation, we do not believe that U.S. practice can be generalised by the forthcoming Protocol.

h Questions: Could such a mandatory regime be envisaged for non-EU countries?

▸ Mandatory production orders

- Brief overview of European Commission proposals for a European Production and Preservation Order and how this would work within the European Union.

In principle, we would discourage extending the proposed EU regime to non-EU countries as it would be a premature decision. The European Parliament and the Council of the European Union

[14] Council of Europe, Cybercrime Convention Committee (T-CY), "Criminal Justice Access to Data in the Cloud: Cooperation with 'foreign' service providers", T-CY (2016)2, May 3, 2016, https://rm.coe.int/168064b77d , p 17.

still need to express their views, which may mean that the final version may well be significantly different from the European Commission's initial proposal.

On 17 April 2018, the European Commission published two proposals on cross-border access to data:

1. A Regulation on cross-border access to and preservation of electronic data held by service providers, thereby respectively proposing the creation of a European Production Order and a European Preservation Order.[15]
2. A Directive to require service providers to appoint a legal representative within the European Union.[16]

The European Union recently created a European Investigation Order Directive (the EIO), which includes provisions on access to electronic data. The EIO replaces "most of the existing laws in a key area of judicial cooperation – the transfer of evidence between Member States [excluding Denmark and Ireland] in criminal cases – by a single new instrument which will make cross-border investigations faster and more efficient".[17]

EU Member States had until 22 May 2017 to transpose this instrument. At the time of writing, there are still some countries that have not transposed it.[18] In addition, at the time of writing, the European Commission still has not made an assessment of the use, efficiency and implementation of the EIO, including its impact on fundamental rights in practice and how the safeguards are being respected (or not) in practice. In addition, according to the Commission's proposal, the measures proposed "should not supersede European Investigation Orders" (Recital 61). However, if the draft proposals were adopted as they are, law enforcement would have short-cuts with lower safeguards than current MLATs or the EIO.

Therefore, we consider the presentation of these new instruments to be premature. Data protection authorities and civil society organisations have expressed concerns about these proposals prior to their publication and continue to shape their positions and recommendations now that they have been made public.

---

[15] Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 Final, April 27, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

[16] Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 Final, April 17, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN.

[17] Emilio De Capitani & Steve Peers, "The European Investigation Order: A New Approach to Mutual Recognition in Criminal Matters", May 23, 2014, *EU Law Analysis*, https://eulawanalysis.blogspot.be/2014/05/the-european-investigation-order-new.html.

[18] European Judicial Network, Status of the Implementation of Directive 2014/41/EU, Regarding European Investigation Order in Criminal Matters, last accessed on June 20, 2018 https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120.

We urge the T-CY to be cautious about the European Commission's proposals, as these are not EU law yet, and they are likely to be heavily amended prior to becoming so. We encourage the T-CY to look at other jurisdictions that have higher standards in place to use these discussions as an opportunity to raise human rights standards and avoid a race to the bottom. In particular, we recommend looking at the Canadian system.

Supporting Documentation:

- Council of Europe, Cybercrime Convention Committee (T-CY), "Criminal Justice Access to Data in the Cloud: Cooperation with 'foreign' service providers", T-CY (2016)2, May 3, 2016, https://rm.coe.int/168064b77d

- Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 Final, April 27, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN

- Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 Final, April 17, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN

- Emilio De Capitani & Steve Peers, "The European Investigation Order: A New Approach to Mutual Recognition in Criminal Matters", May 23, 2014, *EU Law Analysis*, https://eulawanalysis.blogspot.be/2014/05/the-european-investigation-order-new.html

- Directive 2014/41/EU, Regarding European Investigation Order in Criminal Matters, June 20, 2018, https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120

i. For what type of data? Subscriber information only?

We strongly discourage the T-CY to consider extending the still highly fluid EU proposal to any type of data. Instead, we encourage the T-CY to follow the Canadian model (recently relied upon by the ECtHR in *Benedik v Slovenia*, App No 62357/14, April 24, 2018 (ECtHR 4th Section)), whereby prior judicial authorisation is needed for subscriber information as well as content. See our response to question 3.3. c for a more complete discussion of subscriber information.

ii. What limitations and connecting factors?

The Commission's proposals need to be understood within an EU framework where there is certain harmonisation of the judicial system, including certain harmonisation of offences, procedural laws, data protection, and privacy legal frameworks. That means that in case the T-CY considers

the European Commission's approach, it should pay particular attention to the safeguards in which these proposals are made. As a starting point:

- Signatories to the Cybercrime Convention should urgently consider signing and ratifying Convention 108+;
- There should be more work put into bridging the disconnection between domestic laws and human rights law, including case law from the ECtHR and CJEU. Many of the necessary and proportionate principles are based on good case law.[19]

It is wise to ask about the European Commission's proposals (in particular the draft Regulation) limitations as we have identified several preliminary points of concern and would like to bring them to your attention for your discussions:

- We question the need for this proposal, not alone for the concerns it raises, but also in view of parallel negotiations on similar topics at the T-CY.

- It covers service providers of all sizes, with very different data architectures and collection practices, and subject to different regulations (Article 2.3), without duly accounting for these differences.

- It contains too many incentives for service providers to over comply, to the detriment of due process and human rights protections. For instance:

    - Providers are exempt from liability if, by complying in "good faith" with European production orders, they do not fulfil their data protection obligations (recital 46);

    - Providers can be held liable if they do not comply, facing sanctions (see, for instance, Articles 13 and 14.10);

    - Providers are given 10 days to produce the data "unless the issuing authority indicates reasons for earlier disclosure" or they need to provide the data within 6 hours in an emergency (Article 9). This element is particularly worrisome from a due process perspective, in contrast with the 120-day legal deadline under the EIO;[20]

    - Providers will only be reimbursed if Member States decide to have reimbursement cost rules (Article 12), which has been heavily criticised by smaller companies.[21]

[19] International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles"), https://necessaryandproportionate.org/.
[20] European Commission, “Cross-border Access to Electronic Evidence: Improving Cross-Border Access to Electronic Evidence”, accessed June 27, 2018, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.
[21] EuroISPA, “E-Evidence Proposal: EuroISPA Criticises the Privatisation of Law Enforcement”, April 17, 2018, *EuroISPA*, http://www.euroispa.org/e-evidence-proposal-euroispa-criticises-privatisation-law-enforcement/.

- It creates a new categorisation of data that can lead to legal uncertainty (vis-à-vis the categorisation under the Budapest Convention and definitions and categorisation of established case law by the ECtHR and the CJEU) and lead to significant human rights interference. For example, the European Commission defines 'subscriber information' in a very broad way, and it assumes that metadata deserves less protection than other types of data under certain circumstances (Articles 2, 4 and 6). However, it is established knowledge that metadata can be even more revealing than content data.

- According to ECtHR and CJEU case law, prior judicial authorisation is essential. For example, according to the Tele 2 CJEU judgment, "*it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80)*."[22] Nevertheless, the EU proposals do not meet this requirement, as orders to produce certain types of data can be done with just the approval of a Prosecutor (Article 4) — which is not an "independent administrative body" as we understand it. This is contrary to the ECtHR case law in *Benedik v Slovenia*, App No 62357/14, April 24, 2018 (ECtHR 4th Section). This concern goes in line with the recent U.S. Supreme Court Carpenter case, where the Court established that a court-issued warrant is needed for mobile location data based on probable cause.[23]

- It lacks dual criminality requirements (as do most MLATs) and goes beyond the U.S. CLOUD Act by not restricting the proposal to serious crimes. In fact, under the proposal, competent authorities can order the production of subscriber data or access data for "all criminal offences" (Article 5.3); and authorities can order the production of data that falls under the definition of "transactional or content data" for crimes of a maximum penalty of at least 3 years, or for *any* crimes "committed by means of an information system," even where such crimes fall below the 3-year threshold (Article 5.4). In practice, this proposal could be used for almost all criminal offences of the criminal codes of EU Member States, regardless of whether a crime is not criminalised or not punished in the same way in another country.

---

[22] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och Telestyrelsen, December 21, 2016 (CJEU Grand Chamber), para 120, emphasis added.

[23] Andrew Crocker & Jennifer Lynch, "Victory! Supreme Court Says Fourth Amendment Applies to Cell Phone Tracking", June 22, 2018, *Electronic Frontiers Foundation*, https://www.eff.org/deeplinks/2018/06/victory-supreme-court-says-fourth-amendment-applies-cell-phone-tracking; *United States v Carpenter*, (2018) 585 US __ (Supreme Court of the United States).

- The provision on user notification and confidentiality (Article 11) is very vague, and doesn't contain enough safeguards against abuse. For example, service providers would not receive the underlying orders, but only certificates with very little information (see the Annex to the Regulation). This means, for example, that service providers will not be notified of the exact crime that that is being investigated , or the grounds by which the requesting State has determined the underlying order is necessary and proportionate.[24] In addition, there is no mechanism for service providers to challenge gag orders or any requirement for the authorities to provide a reasoned opinion as to why confidentiality is necessary.

- The fundamental rights safeguards are rather artificial and need more work. For example, service providers can only bring objections to the authority if, "based on the sole information contained in the [certificate], it is apparent that it manifestly violates the Charter or that it is manifestly abusive" (Article 14.4 and 14.5, emphasis added). However, the provider would not have enough elements to consider whether it is appropriate to raise a "manifest" violation of the Charter of Fundamental Rights with the competent authority (see Annex to the Regulation).

- The enforcement authority will only know about whether something is happening in their country if the service provider fails to comply with an order and if the issuing authority decides to "transfer [the order with the certificate] to the competent authority in the enforcing State" (Article 14.1). In addition, the enforcing state's grounds for opposition are very narrowly restricted. On the other hand, the enforcement authority would be linked to where the service provider is established (Article 2.13) — sometimes without having any interest or connection to that country. Who would protect concerned users? This affects basic principles of international law, such as sovereignty, legal predictability, or respect of human rights.

- The exercise of the rights to remedy and defence are considerably limited — especially if the production order is made secret (see Articles 11 and 17). In addition, collateral data access from third parties and notification and remedies to these parties are not considered because this regime is only focused on criminal investigation measures.

- The process for resolving conflicts of laws needs considerable work as it is not very clear and it is limited to national security or defence or to the protection of the fundamental rights of the individuals concerned (Article 15.1).

This is a preliminary, non-exhaustive list of concerns. Yet, based on this preliminary assessment, we warn against using this draft regime as a model for the Council of Europe conversations. These

[24] Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 Final, April 17, 2018, Explanatory Report, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN, para 38: "The Certificates should contain the same mandatory information as the Orders, except for the grounds for the necessity and proportionality of the measure or further details about the case to avoid jeopardising the investigations."

concerns are not only intra-EU, as foreign States will be affected by them and reciprocity will play a big part of the EU's intention to enter into bilateral deals.[25] We look forward to providing further input to the Council of Europe, Parties involved, and other relevant stakeholders.

iii. Role of competent authorities in requested country?
This is a crucial point. In line with the Global Civil Society Submission of August 2017,[26] we reiterate that a direct cooperation mechanism cannot happen without the knowledge and agreement of the other State involved.

Otherwise, this will conflict with the sovereignty of the targeted country and with the fundamental requirement of predictability of the law: people that are citizens or residents of a particular state may be assumed to know the laws of that state that apply to them (and those laws must indeed be "foreseeable" in their application, even if, if needs be, with the help of a [domestic] lawyer), but they cannot be expected to know all laws of all States. National laws still differ considerably in their substance (and in accompanying guarantees). Even on matters that all or most states agree should be regulated, one cannot simply allow all States to enforce all of their laws to anyone anywhere. For example, there are different exceptions and exemptions under copyright law; different standards on freedom of expression (e.g. Holocaust denial; claims about Polish people in WWII); incitement to hatred or violence; "promotion" of homosexuality; verbally or otherwise [though non-violently] threatening the integrity of the state, etc). If States could all enforce their laws in respect of anyone's actions anywhere, fundamental principles of States in which the actions took place (or from which they took place) could be undermined.

iv. Enforcement in case of non-compliance with order?
The EU proposals on e-evidence fail to duly involve other countries, e.g. the country of nationality or residence of the data subject whose rights to privacy and data protection, right to defence, among others, are affected.

v. Safeguards and data protection requirements?
See our comments above, and in section I.4.

Supporting Documentation:

- Statement of the Working Party 29 on e-evidence
  http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610177

- EDRi's response to the European Commission's consultation on "e-evidence"
  https://edri.org/files/consultations/e-evidence_edriresponse_20171027.pdf
  https://edri.org/files/consultations/annexconsultatione-evidence_20171026.pdf

[25] Anamarija Tomicic, "Wiretapping & Data Access by Foreign Courts? Why Not!", June 13, 2018, *European Digital Rights*, https://edri.org/wiretapping-data-access-by-foreign-courts-why-not/.
[26] Global Civil Society Submission to the Council of Europe, "Comments and Suggestions on the Terms of Reference for Drafting the Second Optional Protocol to the Cybercrime Convention", September 8, 2017, https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf.

- “EU ‘e-evidence’ proposals turn service providers into judicial authorities”, April 17, 2018, *European Digital Rights*, https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/

- Anamarija Tomicic, “Wiretapping & Data Access by Foreign Courts? Why Not!”, June 13, 2018, *European Digital Rights*, https://edri.org/wiretapping-data-access-by-foreign-courts-why-not/

- Katitza Rodriguez, "A Tale of Two Poorly Designed Cross-Border Access Regimes", April 25, 2018, *Electronic Frontier Foundation*, https://www.eff.org/deeplinks/2018/04/tale-two-poorly-designed-cross-border-data-access-regimes

- Global Civil Society Submission to the Council of Europe, "Comments and Suggestions on the Terms of Reference for Drafting the Second Optional Protocol to the Cybercrime Convention", September 8, 2017, https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf

- International Principles on the Application of Human Rights to Communications Surveillance ("Necessary and Proportionate Principles") https://necessaryandproportionate.org/

- European Commission, “Cross-border Access to Electronic Evidence: Improving Cross-Border Access to Electronic Evidence”, accessed June 27, 2018, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

- EuroISPA, “E-Evidence Proposal: EuroISPA Criticises the Privatisation of Law Enforcement”, April 17, 2018, *EuroISPA*, http://www.euroispa.org/e-evidence-proposal-euroispa-criticises-privatisation-law-enforcement/

- Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och Telestyrelsen, December 21, 2016 (CJEU Grand Chamber)

- Andrew Crocker & Jennifer Lynch, “Victory! Supreme Court Says Fourth Amendment Applies to Cell Phone Tracking”, June 22, 2018, *Electronic Frontiers Foundation*, https://www.eff.org/deeplinks/2018/06/victory-supreme-court-says-fourth-amendment-applies-cell-phone-tracking

- *United States v Carpenter*, (2018) 585 US __ (Supreme Court of the United States), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

- Katitza Rodriguez, "The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom", April 9, 2018, *Electronic Frontiers Foundation*, https://www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom

- *Benedik v Slovenia*, App No 62357/14, April 24, 2018 (ECtHR 4th Section), http://www.bailii.org/eu/cases/ECHR/2018/363.html

3.4 Lawful access to data in the cloud

Brief discussion of the problem of loss of (knowledge of) location situations and the feasibility of mutual legal assistance.

As an initial matter, the problem of loss of knowledge of location can be solved by using preservation requests. As we understand the problem, some providers purport to be unable to determine the location of cloud-stored data, which in turn makes determining where to direct a mutual assistance request impossible. However, it appears that once a provider has complied with a preservation request, the location of the *preserved* data is knowable and therefore the proper jurisdiction to direct a mutual assistance request is knowable.

We note in this regard that Parties to the Budapest Convention must already enact measures to expeditiously preserve and disclose a sufficient amount of traffic data to enable a requesting Party to identify the service provider, and the path through which a communication was transmitted (Article 17 1.b, Article 30).

▸ Understanding jurisdiction: Connecting factors

i Question: What may be relevant factors to determine jurisdiction to enforce (location of data or equipment in the territory of a State, and/or access by a person in the territory of a State who has "possession or control" of data)?

We recommend the T-CY consider the nationality or residence of the data subject concerned by the production orders or requests as a relevant factor.

In any case, this question cannot be answered properly because the answer will depend on the model proposed and the jurisdiction rules underlined by domestic law. Therefore, this should be left to domestic law. Ultimately, the T-CY should consider the severe risks to declaring universal jurisdiction on the basis that a suspect, a victim or a crime has been committed in a territory.

j Question: What is "transborder"?

The Explanatory Report to the Budapest Convention indicates that 'transborder' is defined in a contextual manner. In the context of Article 32, it refers to situations where one Party "unilaterally accesses computer data stored in another Party without seeking mutual assistance" (para 293). It is not clear there is any justification to disturb this definition. We further note that the Convention is

intended to facilitate transborder access to data within signatory Parties, and should not be artificially extended to data that is located outside of said Parties.

▸ Article 32 Budapest Convention

k Question: Is further clarification needed on the scope of Article 32?

We believe this question is unclear, and could not be answered at this stage.
See our responses to questions 3.4, 3.4 j, and 3.4 l.

▸ Options

The Guidance Note on Article 32 provides an example of "transborder" access: "A suspected drug trafficker is lawfully arrested while his/her mailbox - possibly with evidence of a crime - is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b."[27]

l Question: What other scenarios could be envisaged?

- Scenarios?
- Risks?
- Conditions and safeguards?

l.1 Transborder Access to Stored Computer Data with lawful and voluntary consent

Article 32b of the Budapest Convention currently permits transborder access to remote content stored in a foreign jurisdiction on the basis of its 'publicly available' character or of 'lawful and voluntary' consent, as defined in the requesting jurisdictions. The justification for this appears to be a presumed shared understanding of what constitutes 'consent' amongst Parties.[28]

However, some jurisdictions require more than consent before the rights of an individual can be viewed as "waived." This becomes an increasingly complicated endeavour where one party controls access to the data of a third party (e.g. where an individual controls access to a shared account or has control over data, images, or social media activity of an online contact). Further, many jurisdictions are still debating what meaningful consent may look like in situations of shared

[27] Council of Europe, Cybercrime Convention Committee (T-CY), "T-CY Guidance Note #3: Transborder Access to Data (Article 32)", December 3, 2014, T-CY(2013)7 E, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a.
[28] Council of Europe, Cybercrime Convention Committee (T-CY), "T-CY Guidance Note #3: Transborder Access to Data (Article 32)", December 3, 2014, T-CY(2013)7 E, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a, section 3.4.

control or access to information. Because this area of law has not been answered in several countries' domestic law, it should not be discussed in this setting at this time.

Additionally, while some countries allow criminal suspects to consent to data disclosure for reduced prison sentences, this could be viewed as "forced consent" in other jurisdictions and potentially as prosecutorial coercion.

It is important that transborder access to stored computer data does not become real-time interception. Law enforcement officials can take proactive steps when they seize a suspect's computer or device so that it will not receive ongoing communications. In this regard, we note that under the current policy of the U.S. Customs and Border Protection agency, when border officers search travellers' electronic devices, they may only examine information resident upon the devices, and may not access information stored remotely. To ensure compliance with this rule, border officers must ensure that network connectivity is disabled, for example, by placing the device in airplane mode.[29] This is a key security practice that could prevent an accomplice from remotely wiping a device that is still network-connected. In other words, law enforcement upon seizure of a mobile device should immediately terminate its network access to ensure the integrity of the data.

I.2 Transborder Access to Stored Computer Data Where Publicly Available

Article 32a currently permits transborder access to presumptively publicly available or 'open source' information stored in other jurisdictions. This term appears to include information that is available to the general public for purchase, seemingly inclusive of private profiles held by data brokers and other repositories of personal information available for purchase by the general public (see T-CY Guidance Note #3: "It is commonly understood that law enforcement officials may access any data that the public may access, and for this purpose subscribe to or register for services available to the public"). However, cross-jurisdictional differences in data protection rules have created a landscape where such services are frequently populated with deeply private personal information obtained from social media sites and other private companies in ways that are not necessarily consistent with the privacy expectations and protections of the requesting jurisdiction.[30] In light of these complexities, we would not recommend any expansion of the current regime encoded in Article 32b, and would by contrast recommend the addition of added safeguards or limitations.

I.3 Article 32 Interpretation of 'On The Applicable Law'

[29] United States, Customs and Border Protection, "Border Search of Electronic Devices", CBP Directive No. 3340-049A, January 4, 2018, https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf, Section 5.1.2.

[30] For an overview of such challenges see: Christopher Parasons, Lex Gill, Tamir Israel, Bill Robinson & Ronald Deibert, "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters)", December 2017, The Citizen Lab / CIPPIC, https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf, pp 49-54; Lex Gill, Tamir Israel & Christopher Parsons, "Government's Defence of Proposed CSE Act Falls Short", January 29, 2018, CIPPIC / The Citizen Lab, https://cippic.ca/uploads/201801-CSE_Act_Defences_Fall_Short.pdf.

T-CY Guidance Note # 3, section 3.5 "on the applicable law" also wrongly presumes that the Parties to the Convention "form a community of trust, and that rule of law and human rights principles are respected in line with Article 15 of the Budapest Convention." Unfortunately, Article 15 provides only a general statement on the protection on human rights and the rule of law without specifying the necessary safeguards to limit the power it grants to law enforcement agencies. Furthermore, whereas other Articles of the Convention do establish thresholds, these are not mandatory, and do not preclude Parties from adopting less protective mechanisms. This has created problems for implementation since conditions and safeguards are not as detailed as we can find in the European Court of Human Rights (ECtHR) jurisprudence, other international human rights instruments, and court cases.

Countries' laws have adopted the lowest possible standard of protection against many of the invasive powers established in the Budapest Convention. One example is data retention mandates. While the Budapest Convention itself foresees expedited preservation orders for traffic data in a case-by-case basis (Article 17, and 30), many Council of Europe Members and Non-Members involved in the negotiations of the forthcoming Protocol have gone further and adopted questionable data retention regimes. More than half of the EU Member States,[31] Australia, Colombia, Mexico, and Peru, to name a few, have adopted sweeping and untargeted data retention regimes. On two separate occasions, the Court of Justice of the European Union (CJEU) has invalidated comparable data retention regimes for being inconsistent with the rights to data protection and private life as protected in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[32] Most recently, the CJEU held in its Tele2/Watson ruling that even pressing objectives such as the need to fight serious crime "cannot in itself justify ... the general and indiscriminate retention of all traffic and location data" (para 103). This is particularly so given that data retention regimes such as those adopted by Australia and other Parties apply to all persons, including those for whom there is no evidence capable of suggesting the remotest of links to serious crime (para 105). Under the envisioned transborder data access regime, EU member states will regularly access data that was retained in a manner that is inconsistent with these constitutional precepts.[33]

Cross border information access can also implicate human rights in other cross-border contexts, notably in the fields of immigration and refugee decision-making processes, which involve significant cross-border data access. For example, an agreement between the European Union and Canada was found to be incompatible with EU law by the CJEU.[34] The Canadian border services used data acquired by it in order to assess the risk that EU air travellers posed to public

[31] http://stopdataretention.eu/.
[32] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland v Ireland, April 8, 2014 (CJEU Grand Chamber) and Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och Telestyrelsen, December 21, 2016 (CJEU Grand Chamber).
[33] Privacy International, "A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws Since the CJEU's Tele-2/Watson Judgment", September 2017, *Privacy International*, https://www.privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf.
[34] Access Now, "In Win for Privacy, European Court Rejects EU-Canada 'PNR' Agreement", July 26, 2017, *Access Now*, https://www.accessnow.org/win-privacy-european-court-rejects-eu-canada-pnr-agreement/.

safety in Canada in a systematic and automated manner, and with a "significant" margin of error.[35] In order to be consistent with Articles 7 & 8 of the European Charter of Fundamental Rights, the CJEU held that automated risk assessment mechanisms of this type must have safeguards in place to ensure their accuracy and reliability in terms of identifying those participating in serious transnational crime, to ensure they are applied in a non-discriminatory manner, and to ensure that final decisions affecting individuals are based "solely and decisively" on individualized human-based assessment.[36] However, Canadian border services increasingly rely on automated assessment tools of this nature leading to scenarios where high volumes of individuals that pose no threat to security are "subjected to recurring attention from CBSA and its law enforcement and intelligence partners, including in other jurisdictions, simply because they fit within the parameters of a scenario.[37] United States Immigration and Customs Enforcement uses similar databases and automated risk assessment mechanisms to guide decisions related to detention, interrogation, arrest or denial of entry in the immigration and refugee context.[38] One such risk assessment tool was described by the US Department of Homeland Security Office of the Inspector General as "not effective in determining which aliens to release or under what conditions. Such databases are often populated with data obtained through law enforcement" investigations.

Bypassing the careful vetting mechanisms that are currently a central feature of the MLAT regime can also lead to serious human rights liabilities for Parties. For example, the lack of common understanding regarding the rule of law and human rights principles has led Canadian and European states to violate their own human rights obligations in their attempts to assist US counter-terrorism activities. A number of European states have been implicated in the rendition of various individuals by the US Central Intelligence Agency, in violation of the European Convention on Human Rights.[39] A similarly fundamental disagreement over the scope of human rights obligations combined with lax information-sharing practices between the Royal Canadian Mounted Police (RCMP) and the U.S. Federal Bureau of Investigation (FBI) also contributed to the mistaken rendition and torture of Maher Arar, in violation of Canada's human rights obligations.[40] We note in

[35] Opinion 1/15, Re Draft Agreement Between Canada and the European Union - Transfer of Passenger Name Record data from the European Union to Canada, July 26, 2017 (CJEU Grand Chamber) paras 169-170.
[36] Opinion 1/15, Re Draft Agreement Between Canada and the European Union - Transfer of Passenger Name Record data from the European Union to Canada, July 26, 2017 (CJEU Grand Chamber) paras 172-174.
[37] Privacy Commissioner of Canada, Canada Border Services Agency - Scenario Based Targeting of Travelers, Final Report 2017, September 21, 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_cbsa_2017/.
[38] Daniel Oberhaus, "ICE Modified its 'Risk Assessment' Software so it Automatically Recommends Detention", June 26, 2018, *VICE/Motherboard*, https://motherboard.vice.com/en_us/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention; Justin Ling, "Revealed: Canada Uses Massive US Anti-Terrorist Database at Borders", June 21, 2018, *The Guardian*, https://amp.theguardian.com/world/2018/jun/21/canada-us-tuscan-anti-terrorist-database-at-borders.
[39] Brian Chang, "How the European Convention on Human Rights Limits Cooperation with the Trump Administration", January 25, 2018, Just Security, https://www.justsecurity.org/36751/european-convention-human-rights-limit-cooperation-trumps-administration/ ; BBC News, “Lithuania and Romania Complicit in CIA Torture — European Court,” May 31, 2018, *BBC News*, https://www.bbc.com/news/world-europe-44313905; BBC News, “Trump Signs Order to Keep Guantanamo Bay Prison Open”, *BBC News*, January 31, 2018, https://www.bbc.com/news/world-us-canada-42883443.
[40] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar: Factual Background, Volume I, Government of Canada, 2006, http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-eng.pdf; CBC News, “Ottawa Reaches $10M Settlement with Arar”, January 26, 2007, *CBC News*, http://www.cbc.ca/news/canada/ottawa-reaches-10m-settlement-with-arar-1.682875.

this respect that counter-terror increasingly involves mixed law enforcement and national security components, and information shared between law enforcement and other agencies contributes to counter-terror related decision-making.

Finally, disagreements over safeguards for journalists and civil society advocates in the context of law enforcement activities are also common amongst states involved in the negotiation of the proposed second Protocol. In Mexico, the United Nations and the Inter-American Commission on Human Rights Special Rapporteurs for Freedom of Expression noted that local policing agencies are often believed to have colluded with organized crime in situations that have resulted in violence to journalists.[41] Civil society advocates and journalists have also been targeted by aggressive spyware fishing campaigns suspected to have been carried out on behalf of Mexican government agencies under the guise of 'crime fighting.'[42] Finally, in Canada, a recent Commission of Inquiry documented a number of instances where law enforcement agencies directed surveillance powers at journalists reporting on police-related matters, leading to the systematic tracking of journalists and the use of law enforcement data access powers in ways that threaten to unmask journalist sources.[43]

All in all, it is difficult to state categorically that Parties to the Convention share an indisputable agreement on the scope of human rights at this stage. It is difficult if not impossible to anticipate how such disconnections might evolve in the future, yet the Convention does not include any mechanisms to address such disconnections. By seeking to provide various avenues of direct access to data stored in a Party, the second protocol bypasses domestic legal processes currently required by the existing MLAT regime, yet these processes provide a critical vetting mechanism for ensuring data requests from foreign states are not likely to contribute to egregious human rights abuses. The second Protocol proposals must offer explicit safeguards to counterbalance the countervailing risk that will result from them.

Supporting Documentation:

- Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland v Ireland*, April 8, 2014 (CJEU Grand Chamber)

- Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och Telestyrelsen*, December 21, 2016 (CJEU Grand Chamber)

---

[41] David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on his Mission to Mexico, June 12, 2018, A/HRC/38/35/Add.2 AEV, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Pages/ListReports.aspx, para 47.
[42] John Scott-Railton, Bill Marczak, Bahr Adul Razzak, Masashi Crete-Nishihata & Ron Deibert, "Reckless Exploit: Mexican Journalists, Lawyers and a Child Targeted with NSO Spyware", June 19, 2017, *The Citizen Lab*, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/; Ronald Deibert, "Mexico Wages Cyber Warfare Against Journalists, and their Minor Children", June 19, 2017, *The Citizen Lab*, https://deibert.citizenlab.ca/2017/06/mexico-nso/.
[43] Commission d'enquête sur la protection de la confidentialité des sources journalistiques, "Report Overview", (Québec: Gouvernement du Québec, 2017), https://www.cepcsj.gouv.qc.ca/fileadmin/documents_client/documents/CEPCSJ_Synthese-ANG_Accessible_2017-12-14.pdf; Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", May 2018, *The Citizen Lab & CIPPIC*, https://cippic.ca/uploads/20180514-shining_a_light.pdf.

- Privacy International, “A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws Since the CJEU’s Tele-2/Watson Judgment”, September 2017, *Privacy International*, https://www.privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf

- Opinion 1/15, Re Draft Agreement Between Canada and the European Union - Transfer of Passenger Name Record data from the European Union to Canada, July 26, 2017 (CJEU Grand Chamber)

- Privacy Commissioner of Canada, Canada Border Services Agency - Scenario Based Targeting of Travelers, Final Report 2017, September 21, 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_cbsa_2017/

- Access Now, "In Win for Privacy, European Court Rejects EU-Canada 'PNR' Agreement", July 26, 2017, *Access Now*, https://www.accessnow.org/win-privacy-european-court-rejects-eu-canada-pnr-agreement/

- Christopher Parasons, Lex Gill, Tamir Israel, Bill Robinson & Ronald Deibert, "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters)", December 2017, *The Citizen Lab / CIPPIC*, https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf

- Lex Gill, Tamir Israel & Christopher Parsons, "Government's Defence of Proposed CSE Act Falls Short", January 29, 2018, *CIPPIC / The Citizen Lab*, https://cippic.ca/uploads/201801-CSE_Act_Defences_Fall_Short.pdf

- Brian Chang, "How the European Convention on Human Rights LImits Cooperation with the Trump Administration", January 25, 2018, *Just Security*, https://www.justsecurity.org/36751/european-convention-human-rights-limit-cooperation-trumps-administration/

- Commisison of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar: Factual Background, Volume I, Government of Canada, 2006, http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-eng.pdf

- Daniel Oberhaus, "ICE Modified its 'Risk Assessment' Software so it Automatically Recommends Detention", June 26, 2018, *VICE: Motherboard*, https://motherboard.vice.com/en_us/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention

- Department of Homeland Security, Office of the Inspector General, US Immigration and Customs Enforcement's Alternatives to Detention (Revised), February 4, 2015, OIG-15-22, *United States Government,* https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-22_Feb15.pdf

- Justin Ling, "Revealed: Canada Uses Massive US Anti-Terrorist Database at Borders", June 21, 2018, *The Guardian*, https://amp.theguardian.com/world/2018/jun/21/canada-us-tuscan-anti-terrorist-database-at-borders

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Mexico, A/HRC/38/35/Add.2, AEV, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Pages/ListReports.aspx

- John Scott-Railton, Bill Marczak, Bahr Adul Razzak, Masashi Crete-Nishihata & Ron Deibert, "Reckless Exploit: Mexican Journalists, Lawyers and a Child Targeted with NSO Spyware", June 19, 2017, *The Citizen Lab*, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ https://deibert.citizenlab.ca/2017/06/mexico-nso/

- Commission d'enquête sur la protection de la confidentialité des sources journalistiques, "Report Overview", (Québec: Gouvernement du Québec, 2017), https://www.cepcsj.gouv.qc.ca/fileadmin/documents_client/documents/CEPCSJ_Synthese-ANG_Accessible_2017-12-14.pdf

- Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", May 2018, *The Citizen Lab & CIPPIC*, https://cippic.ca/uploads/20180514-shining_a_light.pdf

- David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on his Mission to Mexico, June 12, 2018, A/HRC/38/35/Add.2 AEV, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Pages/ListReports.aspx

- Stop Data Retention, http://stopdataretention.eu/

- United States, Customs and Border Protection, "Border Search of Electronic Devices", CBP Directive No: 3340-049A, January 4, 2018, https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf

A. Inclusion of Transparency Mechanisms:
Any system adopted for transborder access must include robust transparency and accountability mechanisms. At minimum, this must include annual statistical reporting, limitations on gag orders and, to the maximum extent possible without undermining investigations, individual notice obligations.

Including such transparency mechanisms will allow monitoring of transborder access mechanisms to assess their ongoing utility as well as to ensure they continue to operate in a manner that is respectful of privacy and other human rights.

Supporting Documentation:

- Christopher Parsons, The (In)Effectiveness of Voluntarily Produced Transpareny Reports" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798855

B. The Case for Dual Privacy Protection:
We believe that when law enforcement authorities seek cross-border data, they should satisfy the privacy standards of *both* the requesting nation and the responding nation. Such dual data privacy protection is the best way to ensure that the ever-growing movement of sensitive data across national frontiers does not reduce privacy protection and implicate other human rights obligations.

The starting point is the Necessary and Proportionate Principles regarding communications surveillance. According to Principle #12, which addresses safeguards for international cooperation:

> "where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is required."

Privacy rules and national legal systems are often complex. So in many cases it will be difficult to determine whether the standards of the requesting country or the responding country are more protective. For example, allowing European states to access US-hosted data on the basis of their own domestic legal standards could bypass critical U.S. protections for the protection of data such as email content.[44] Thus, to ensure the effectiveness of Principle #12, law enforcement should satisfy both standards.

Dual data privacy protection echoes the international norm of "dual criminality." Under this norm, a responding nation will not assist a requesting nation unless the crime being investigated is a crime not just in the requesting nation, but also in the responding nation. For example, if blasphemy or sodomy or abortion is a crime in the requesting nation but not the responding nation, then the responding nation will not assist the requesting nation to investigate or punish that crime. Extradition treaties often contain this dual criminality norm. So does the U.S. statute regarding when federal judges may grant search warrants to assist foreign police.

[44] Cynthia M Wong, "US Cross-Border Data Deal Could Open Surveillance Floodgates", September 18, 2017, *Human Rights Watch*, https://www.hrw.org/news/2017/09/18/us-cross-border-data-deal-could-open-surveillance-floodgates.

Just as a nation will not extradite or help investigate a suspect for conduct that is not prohibited under its own criminal laws, so a nation should not allow foreign police to seize data located in its jurisdiction when doing so violates its own privacy and data protection laws.

In the absence of a global consensus on privacy standards, dual privacy protection in cross-border access mechanisms is an important safeguard against forum shopping. Without such safeguards, Parties to the Budapest Convention will be free to strategically rely on the system put in place by the Second Additional Protocol in situations where their own domestic standards are lower than that of the data-hosting state, while relying on options such as the MLAT regime in contexts where the requesting state offers more permissive standards, and on direct voluntary cooperation where no explicit bar exists. Dual data privacy protection will also help ensure that as nations seek to harmonise their respective privacy standards, they do so on the basis of the highest privacy and data protection standards. Absent a dual privacy protection rule, nations may be tempted to harmonise at the lowest common denominator. In either scenario, the ultimate impact is a net global loss of privacy.

Given the exceptional nature of the transborder access mechanisms being considered, requiring parties to comply with both domestic and foreign privacy protections is not unreasonable. Creating a privacy respective cross-border data access mechanism of this nature will at the same time have the ancillary impact of reducing backlogs and response times in the existing MLAT regime, which will remain an available alternative to Parties. Most importantly, however, a dual privacy protection mechanism imposes an important safeguard for privacy and other human rights. Experience has shown that all States have a tendency to over-reach in their data access aspirations at some point or another. Creating a cross-border access mechanism that respects both applicable standards will not only address law enforcement needs by providing an additional formalised mechanism for access, but also operate as a critical check on excessive short term data access policies. In these, and other scenarios, allowing both requesting and host states a means of setting conditions for data access will ensure that cross-border access does not operate to reduce the level of privacy protection currently in place while providing a critical safeguard against anticipated human rights challenges that will all but inevitably arise.

Supporting Documentation:

- The International Principles on the Application of Human Rights to Communications Surveillance ("Necessary and Proportionate Principles") https://necessaryandproportionate.org/

- Cynthia M Wong, “US Cross-Border Data Deal Could Open Surveillance Floodgates”, September 18, 2017, Human Rights Watch, https://www.hrw.org/news/2017/09/18/us-cross-border-data-deal-could-open-surveillance-floodgates

SIGNATORIES

Electronic Frontier Foundation (EFF), 39,000 members in 99 countries (International)
European Digital Rights (EDRi), a coalition of 39 civil society organisations (Europe)
Association for Civil Rights (Argentina)
Derechos Digitales (América Latina)
Elektronisk Forpost Norge (Electronic Frontier Norway)
IPANDETEC (Central America)
Karisma Foundation (Colombia)
OpenMedia (Canada / International)
Panoptykon Foundation (Poland)
R3D: Red en Defensa de los Derechos Digitales (México)
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) (Canada)
SonTusDatos (Artículo 12, A.C.) (Mexico)
TEDIC NGO (Paraguay)