Joint Civil Society Response to the provisional draft text on "Joint investigation teams and joint investigations", "Expedited disclosure of stored computer data in an emergency" and "Requests for domain name registration information" of the Cybercrime Convention Committee (T-CY)

SUBMITTED BY

Electronic Frontier Foundation (EFF)
European Digital Rights (EDRi),
IT-Pol Denmark
Al Sur
Article 19
Derechos Digitales
Homo Digitalis

DECEMBER 15, 2020

INTRODUCTION

The Electronic Frontier Foundation (EFF), the European Digital Rights (EDRi), IT-Pol Denmark, Al Sur, Article 19, Derechos Digitales, and Homo Digitalis welcome this opportunity to engage with the Council of Europe and State Parties involved in drafting the Second Additional Protocol to the Convention on Cybercrime.

We have serious concerns that the Protocol Drafting Plenary (PDP) has not yet disclosed their ongoing work on conditions and safeguards for data protection and privacy, even though the Cybercrime Convention Committee has extended the negotiations of the Draft Protocol until December 2020. Any effort to enable effective police investigations must go hand in hand with respecting critical human rights and data protection safeguards, including transparency, public oversight, and effective remedies. There are many signatories of the Budapest Convention, and some Parties' domestic legal frameworks may not be consistent with Article 15 of the CCC, and with their international human rights obligations. Some Parties' domestic legal frameworks may also impose undue restrictions on freedom of expression, which has the potential to result in arbitrary or unlawful direct cross-border disclosure of subscriber data.[1] The absence of a dual criminality provision can negatively affect subscribers' freedom of expression rights. Disproportionate or unnecessary disclosures of subscribers' data can be abused. Subscriber identification powers can be used to identify political opponents and to silence dissent. Before Parties can access and sign this Draft Protocol, Parties' domestic legal framework should demonstrate compliance with Article 15 and their international human rights obligations.

We reiterate our previous recommendations, calling for signatories to the Budapest Convention to first sign Convention 108+ for the Protection of Individuals about Automatic Processing of Personal Data. This Convention provides for comprehensive and detailed data protection safeguards in the use and transfer of personal data.

This submission provides recommendations on three provisions of the Draft Text of the Second Additional Protocol: Joint investigation teams and joint investigations, requests for domain name registration information, and expedited disclosure of stored computer data in an emergency. **We thank the Cybercrime Committee of the Council of Europe for considering the following recommendations. We believe that the Draft Protocol should:**

- Prohibit Parties from reaching secret agreements regarding the terms for accessing personal information, electronic evidence, or other evidence in Joint Investigations;
- Guarantee the separation and independence between the authorities authorising joint investigations and authorities undertaking them;
- Prohibit the practice of "forum shopping" in joint investigations and joint investigation teams;
- Limit the repurposing of information or evidence obtained in joint investigations;
- Introduce strong public oversight mechanisms to supervise the conduct of joint

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32 (2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

investigations;
- Ensure that access rules for domain name registration data do not bypass mutual legal assistance;
- Introduce a notification to and demand the authorisation of the competent authorities of the requested Party for the execution of a request seeking domain name registration information;
- Not weaken domestic legal protections against voluntary disclosure of domain registration data that are essential to the respect of fundamental rights;
- Include among minimum requirements that a request must meet the provision of enough information for service providers or authorities in the requested State to reject manifestly abusive requests;
- Guarantee the right to access effective remedies through the obligation to notify the targeted and other affected individuals when their data is accessed unless it would risk jeopardising ongoing investigations;
- Include accountability and public oversight mechanisms to supervise the expedited disclosure of stored computer data in an emergency.

1 JOINT INVESTIGATION TEAMS AND JOINT INVESTIGATIONS

As we have previously said, joint investigations are acceptable if they respect democratic processes, the rule of law, and human rights principles.[2] At all costs, the Draft Protocol should ensure that joint investigations do not open a floodgate of unsupervised cross-border access to electronic evidence (including content, metadata, personal data, and subscriber data) by "forum shopping". In other words, the Draft Protocol should prohibit participating authorities from conducting joint cross-border investigations (e.g. through computer network exploitation) that would not be permitted by the laws of the Party in which the investigation occurs. Doing so would invite domestic authorities to rely on foreign counterparts to do what they are legally prevented from doing themselves, bypassing one Party's domestic legal framework.

Therefore, we recommend to:

1.1 Prohibit Parties from reaching secret agreements regarding the terms for accessing personal information, electronic evidence, or other evidence in Joint Investigations:

Paragraphs 1, 2 and 6 of the Draft Protocol authorise competent authorities of two or more Parties to enter private agreements to set the terms of joint investigation teams (JITs). Such terms include when those teams may provide, limit, or withhold access to information (which may include personal information), potential evidence, or evidence. Accessing electronic evidence or potential evidence interferes with the right to privacy, and such terms must be publicly accessible. Such interference must comply with the Principle of Legality, which prescribes that any limitation to human rights must be "publicly accessible, clear, precise,

[2] Global Civil Society Submission to the Council of Europe, Comments and suggestions on the Terms of Reference for drafting a Second Optional Protocol to the Cybercrime Convention, HTTPS://EDRI.ORG/FILES/SURVEILLANCE/CYBERCRIME_2NDPROTOCOL_GLOBALSUBMISSION_E-EVIDENCE_20170908.PDF

comprehensive and non-discriminatory."[3] In scope, the Legality Principle covers "access to information held extraterritorially or information sharing with other States."[4]

1.2 Guarantee the separation and independence between the authorities authoritising joint investigations and authorities undertaking them:

Parties' competent authorities, which set the terms for their JITs, should be separate and independent from the Parties' participatory authorities which undertake the investigations. Unfortunately, the broad definition of "competent authorities" might improperly be interpreted as including law enforcement authorities, and authorising them to set the terms of their own JITs. We understand that the definition of "competent authorities" comes from Paragraph 138 of the 2001 Explanatory Report of the Budapest Convention, which defines competent authorities as any "judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of procedural measures for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings."[5] To avoid potential abuse of power, we recommend the Parties' competent authority setting up the joint investigation's governance structure to be independent from the participating authorities. Entanglement of competent authorities and participating authorities in setting the rules for Joint Investigations is even more problematic if the "competent authorities" are law enforcement agencies. Participating authorities should be acting independently of the competent authorities setting the terms of the joint investigations and according to due process of law.[6] This reflects the core requirement of international human rights law that access of personal information, evidence or potential evidence by public officials must not only be necessary and proportionate but also be attended by independently monitored strict safeguards against abuse.[7] In Klass, "The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure." This is because the executive branch of the government is incapable of providing the necessary degree of independence and objectivity to prevent the abuse.

1.3 Prohibit the practice of "forum shopping" in joint investigations and joint investigation teams:

The Draft Protocol should be limited to investigative measures that are authorised under the domestic laws of all participating Parties and, in particular, the domestic law applicable to the territory where the investigation is carried out. This is necessary to prevent forum shopping activities that could undermine fundamental rights protections under domestic law and international human rights law.

---

[3] U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018); U.N. General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/RES/72/180 (19 December 2017). Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

[4] Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

[5] Explanatory Report to the Convention on Cybercrime, HTTPS://RM.COE.INT/16800CCE5B

[6] See Weber & Savaria v. Germany, no. 54934, 29 June 2006,

[7] Weber and Savaria v. Germany, cited above at para 95, in which the Court identified various "minimum safeguards that should be set out in statute law in order to avoid 'abuses of power'" (para. 95).

Under Paragraph 4, if investigative measures need to be taken on the territory of one of the participating Parties, participating authorities of that Party may issue a request to their own authorities to carry out such measures. If the domestic authorities determine that they can take the investigative measure under their domestic law, a request for mutual assistance by other participating Parties may not be needed. With this wording, the Draft Explanatory Report seems to allow "forum shopping" activities that are likely to undermine fundamental rights protection under the laws of the territory where the investigation is carried out, which is very concerning. Domestic laws governing potentially very intrusive investigative measures such as computer network exploitation ("computer hacking") and (online) agent provocateurs are likely to differ considerably, resulting in certain measures being strictly prohibited in certain Parties and permitted in others.

We are particularly concerned by cybercrime investigations that indiscriminately target all users of an online service with intrusive measures. An example is the recent infiltration of the EncroChat communications service by a joint investigation team of Dutch and French law enforcement authorities. The joint investigation team appears to have gained access to communications contents for all EncroChat users, including a large number of users outside France and the Netherlands, through bulk equipment interference (planting trojans on devices of all users). This could potentially include persons whose communication is protected by immunities and privileges under the domestic laws of the State where they reside. Domestic laws permitting intrusive and indiscriminate investigative measures on the scale of the EncroChat investigation are likely to be the exception among the Parties to the Cybercrime Convention. It would be highly detrimental to fundamental rights if joint investigation teams are used in a way that undermines such limitations in domestic laws of participating Parties or other States where persons affected by the investigation have their place of residence.

Cross-border operations of joint investigation teams should not be used to circumvent limitations and prohibitions of certain investigative measures in domestic law (of the territory where the investigation is carried out).

As a result, we strongly recommend to amend Article 3 so that JITs are only allowed to carry out investigations on their own territories and only if authorised by the domestic laws of all participating Parties. This will provide a legal framework for cross-border mutual assistance in cases where other Parties have a greater expertise in certain investigations without undermining the legal protections and other safeguards provided by the laws of either participating Party.

1.4 Limit the repurposing of information or evidence in paragraph 5:

We believe the limitations, as laid down in paragraph 5b, to the use of information obtained for other criminal offenses than those for which the joint investigation agreement was concluded should be strengthened and only authorise such information repurposing in emergency cases, such as a situation in which there is a significant and imminent risk to the life or safety of any natural person (as stated in paragraph 5.c.). The consent of cooperating Parties is an insufficient safeguard as in practice, they will have little interest in protecting the data protection, defence and procedural rights of the person concerned. Thus, we propose the following amendments to Paragraph 5:

"Use of information or evidence provided by the participating authorities of one

Party to participating authorities of other Parties concerned may be refused or restricted in the manner set. Parties may only use the information or evidence provided:

a. for the purposes for which the agreement has been entered into;

b. if fundamental legal principles of the receiving Party require disclosure of the information or evidence to protect the rights of an accused person in criminal proceedings. In that case, authorities in the receiving Party shall notify the authorities that provided the information or evidence without undue delay; or

c. to prevent a situation in which there is a significant and imminent threat involving the life or safety of a natural person. In that case, the participating authorities that received the information or evidence shall notify the participating authorities that provided the information or evidence without undue delay, unless mutually determined otherwise.

1.5 Introduce strong public oversight mechanisms:

To ensure accountability in joint investigations, the Draft Protocol should require that joint investigations be subject to independent oversight mechanisms, carried out by each participating Party. Oversight bodies should have the authority to access all relevant information about Parties' joint investigations and joint team activities. Such access should include, when appropriate, confidential information to allow independent assessment of whether the participating Parties are making legitimate use of their lawful capabilities. Such mechanisms are also useful to evaluate whether the participating Parties have complied with their transparency obligations. Each Party should also publish periodic reports about the lawfulness of those actions, including the extent to which they comply with these principles.[8]

2 REQUESTS FOR DOMAIN NAME REGISTRATION INFORMATION

[8] See Public Oversight, Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis, (May 2014), http://necessaryandproportionate.org/global-legal-analysis; Valentina Hernandez, Juan Carlos Lara, Katitza Rodriguez, Interamerican Legal Analysis, Derechos Digitales and Electronic Frontier Foundation, https://necessaryandproportionate.org/americas-legal-analysis; Privacy International, Guide to International Law and Surveillance 2.0, February 2019. HTTPS://PRIVACYINTERNATIONAL.ORG/SITES/DEFAULT/FILES/2019-04/GUIDE%20TO%20INTERNATIONAL%20LAW%20AND%20SURVEILLANCE%202.0.PDF.

We are aware that Parties' investigative and prosecuting authorities increasingly protest about the current situation where many domain name registrars and registries exclude personal data of individuals from WHOIS records by default, in part due to data protection obligations such as the GDPR.[9] The access to such non-public WHOIS data is thus not direct and affects the Parties authorities' ability to easily obtain access to WHOIS data.[10]

Domain name registration information is personal data in several Parties' domestic data protection laws and should be collected and used only for a specific purpose by the controller—to provide domain name services to the registrant and facilitate billing for this service.

Such data should not be made available in connection with content hosted at a domain, absent an order by the competent authority (which should be an independent judicial authority[11]), and pursuant to privacy-protective conditions and safeguards. Content hosted on websites under a certain domain level is often posted by someone other than the registrant. This is why the domain name system should not become a point of control for governments to regulate users' online speech and activity. The content of a website can reveal a great number of sensitive and private information, such as political and religious beliefs and sexual orientations. Granting States sweeping powers to obtain the identity of domain name registrants without proper safeguards and independent judicial oversight would create a drastic chilling effect on speech because of the fear of reprisal and censorship .

We therefore provide the following recommendations to ensure access to domain name registration information complies with all relevant data protection and other human rights safeguards:

2.1 Access rules for domain name registration data should not bypass mutual legal assistance:

The first paragraph commands Parties to adopt laws that will empower their competent authorities to issue direct requests to domain name service providers in the territory of another Party, with the aim to disclose their users' domain name registration data, for specific criminal investigations and proceedings. Such direct requests would bypass the mutual legal assistance process. This provision would cover domain name providers such as GTLDs and country-code level domain names. According to the explanatory report, such data requests may be issued, and the information may be obtained, via a remote cross-border access tool, such as an interface, portal, or other technical tool.

Instead of taking the opportunity to create a consistent and privacy-protective method for cross-border subscriber and domain name registration (DNR) data access, the Draft Protocol seeks to encode the lowest common denominator of access. Similarly to our position on the 4th provision on direct disclosure of subscriber information, which authorises direct disclosure of subscriber data without going through the mutual legal assistance process, we oppose direct

[9] EFF, Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation, https://www.eff.org/files/2018/01/26/submission_to_icann_on_whois.pdf

[10] For example: HTTPS://DATA.CONSILIUM.EUROPA.EU/DOC/DOCUMENT/ST-13443-2018-INIT/EN/PDF

[11] See our previous submission, paragraph 2.3.3 HTTPS://EDRI.ORG/FILES/TCY_DRAFT_2ND_ADDITIONAL_PROTOCOL_CIVIL_SOCIETY_SUBMISSION_20191107.PDF

access of domain name registration information without specific conditions and safeguards, since it threatens the privacy, data protection, and possibly anonymity of the domain name registrant. To make matters worse, there is the lack of assessment of the Parties' domestic legal frameworks as to compliance with international human rights Treaties and their data protection obligations.

Thus, we recommend that a domain name registrant's data should only be disclosed in response to a request, subject to appropriate conditions and safeguards for data protection and privacy. These include independent judicial authorisation, legal and factual elements demonstrating that the subscriber data is relevant to the criminal investigation, the respect of the principles of necessity and proportionality, public transparency reporting and oversight mechanism, mandatory notification to the targeted individual at the earliest opportunity to ensure access to remedies, a fixed list of information that a request must contain so providers can challenge and reject disproportionate or unnecessary demands (see 2.3 below).

2.2 A notification to and the authorisation of the competent authorities of the requested Party should be mandatory:

As outlined in our previous submissions, we believe that extending the jurisdiction of a Party to the territory of another Party should not happen without the knowledge and agreement of the requested Party. Accordingly, if a request is sent directly to private service providers (domain name registrars or registries) in another State, there must be mandatory notification to the authorities of the requested Party in order to ensure that authorities in the requested Party can halt the disclosure of personal data if the conditions under its domestic law are not satisfied or if there are other valid grounds to oppose the disclosure. Private service providers cannot be expected to safeguard fundamental rights by refusing voluntary disclosure on a discretionary basis. Most service providers lack the capacity and often have no interest to carry out comprehensive human rights impact assessments of each order received and are likely to disclose data without proper review—despite the possibility that the transfer breaches domestic data protection and privacy laws. **For more details, we invite the T-CY drafting group and the plenary to consult our previous submission on the provision of direct disclosure of subscriber information.**[12]

2.3 Domestic limits on voluntary disclosure of domain registration data should not be swept away by the draft Protocol as they are essential to the respect of fundamental rights:

Paragraph 2 of the Draft Protocol requires Parties to adopt legislation to authorise domain name providers to disclose domain name registrants' data in response to a direct request by another Party – basically removing domestic barriers to data disclosure to foreign authorities. The data transfer by the domain name service providers remains voluntary and subject to reasonable conditions provided by domestic law as explained by paragraph 2 of the Draft Explanatory Report. This paragraph does not require Parties to enact legislation obligating these entities to respond to a request from an authority of another Party. Rather, it requires Parties to remove

[12] EFF, EDRI et al, Joint Civil Society Response to the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime, 2019, HTTPS://WWW.EFF.ORG/FILES/2019/11/18/20191107_CIVILSOCIETYSUBMISSION_T-CYDRAFTSECONDADDITIONALPROTOCOL.PDF

any existing domestic measures that may prohibit or limit voluntary disclosure of this personal data.

However, existing domestic limitations are there to advance and protect fundamental rights against abuse. For Parties of the European Union, the legislative measures required by paragraphs 1 and 2 may conflict with existing domestic data protection laws. In the European Union, disclosure of personal data, including subscriber data, to public authorities, whether voluntary or obligatory, is an act of processing personal data that requires a legal basis under GDPR Article 6 (1). A legal basis for voluntary disclosure must be necessary and proportionate in a democratic society. Therefore, these fundamental rights requirements cannot be reconciled with the Draft Protocol's undermining of domestic data protection laws on voluntary disclosure of domain registration data.[13] Under the current Draft, personal data would be transferred from the service provider to a controller in another Party, which may conflict with third-country provisions in Parties' data protection laws. In the European Union, disclosure of personal data to a requesting Party outside the European Union or European Economic Area would also have to comply with the provisions in Chapter V of the GDPR and the European Essential Guarantees.[14]

2.4 Minimum requirements that a request must meet should also include the provision of enough information for service providers or authorities in the requested State to reject manifestly abusive requests:

Paragraph 3 establishes the information that requests should give to domain name service providers, while paragraph 4, in turn, provides that "information disclosed in response to a request under paragraph 1 shall be subject to appropriate safeguards pursuant to Articles 15 and [data protection laws]."

We support the safeguards in paragraph 3 and 4 as an effort to mitigate the risks of direct disclosure of domain name registration data. Domain name registrant's data should only be disclosed upon a request that meets these safeguards, at the very least. Such safeguards should be expressly included in the draft protocol and align with Articles 15 of the Budapest Convention, international human rights treaties, and Convention 108+. For guidance, critical safeguards rooted in international human rights law are identified in the Necessary and Proportionate Principles on the Application of Human Rights, its global and inter-american legal analysis, and Privacy International guide to international law, as well as in the recent case law of the European Court of Human Rights concerning the Protection of Personal Data.[15]

---

[13] "The EDPS would also like to reiterate that the fundamental right to the protection of personal data cannot in any case be 'waived' by the individual concerned(…). The data controller remains fully bound by the personal data rules and principles even (…) when consent to the processing had been given by the data subject." HTTPS://EDPS.EUROPA.EU/SITES/EDP/FILES/PUBLICATION/20-06-16_OPINION_DATA_STRATEGY_EN.PDF

[14] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), HTTPS://EC.EUROPA.EU/JUSTICE/ARTICLE-29/DOCUMENTATION/OPINION-RECOMMENDATION/FILES/2016/WP237_EN.PDF

[15] Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis, (May 2014), http://necessaryandproportionate.org/global-legal-analysis; Privacy International, Guide to International Law and Surveillance 2.0, February 2019. HTTPS://PRIVACYINTERNATIONAL.ORG/SITES/DEFAULT/FILES/2019-04/GUIDE%20TO%20INTERNATIONAL%20LAW%20AND%20SURVEILLANCE%202.0.PDF; Katitza Rodriguez, Valentina Hernandez, Juan Carlos Lara, Interamerican Legal Analysis, Derechos Digitales and Electronic Frontier Foundation, https://necessaryandproportionate.org/americas-legal-analysis;

Domain name service providers should also be able to reject requests that are manifestly unnecessary and disproportionate or in clear conflict with the domestic law where the Domain Service Providers' is subject to, and to notify the target.[16] **This is why paragraph 3 should be expanded to include all the necessary information for a service provider and the Requested Party's authorities to identify and protect against manifestly abusive demands,** such as requests for data of a large group of individuals that would amount to a fishing expedition.

2.5 The right to access effective remedies should be guaranteed by the requirement to notify the targeted and other affected individual of the DNR data access request:

As made clear by the Report of the U.N. High Commissioner for Human Rights on the right to privacy in the digital age:

> "A State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State party, even if not situated within its territory. (…) Equally, where a State exercises regulatory jurisdiction over a third party that controls a person's information (for example, a cloud service provider), that State also has to extend human rights protections to those whose privacy would be affected by accessing or using that information."[17]

Likewise, according to the Human Rights Committee, U.N., States should: "ensure that (…) affected persons have proper access to effective remedies in cases of abuse."[18]As explained in the "Right to Privacy in the Digital Age" Report of the U.N. High Commissioner for Human Rights, effective remedies share certain characteristics:

> "First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice … and standing (to challenge such measures) thus become critical issues in determining access to effective remedy. … Second, effective remedies will involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an independent oversight body … governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society. Third, for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation."[19]

Paragraph 3, point d foresees that the Requesting State can submit a request for non-disclosure of the request for information to the registrant or other third parties.

---

[16] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014), HTTPS://WWW.OHCHR.ORG/EN/HRBODIES/HRC/REGULARSESSIONS/SESSION27/DOCUMENTS/A.HRC.27.37_EN.PDF

[17] Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018), pag. 11.

[18] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (2014), pag. 40.

[19] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (2014), pag. 13.

Furthermore, Parties' data protection laws may require notification to data subjects if their personal data are processed for a purpose other than the one for which the personal data were collected or if the personal data are disclosed to a third party. Even if service providers have a proper legal basis for disclosing the information to authorities in the requesting Party, there may still be a requirement to notify the data subject unless the right to information for the data subject has been restricted by the requested Party's domestic law. In the European Union this would have to be in accordance with GDPR Article 23 which, inter alia, requires specific provisions with safeguards for the data subject. **In any case, a request for non-notification by the Requesting Party cannot override obligations in data protection laws in the requested Party.**

3 EXPEDITED DISCLOSURE OF STORED COMPUTER DATA IN AN EMERGENCY

To minimise the risks associated with expeditious disclosure of stored computer data in an emergency, the Protocol should include accountability and public oversight mechanisms. These should include penalties for blatant or systemic misuse of emergency powers by a Party. Statistical and qualitative reporting on the volume of expedited disclosures should be annually published by both requesting and responding Parties. Service providers should also be required to publish Transparency reports. While this requirement should apply to all cross border requests, it is particularly vital for emergency requests given their potential for over-reach.

Finally, as to paragraph 4 authorisation of oral emergency requests, they should immediately be followed by a written request for accountability purposes.

4 CONCLUSION

.
As we have emphasised in our previous submissions, the Second Additional Protocol risks creating a two-tier system where some Parties put necessary safeguards in place to protect against government overreach, while others opt for the most intrusive methods because they believe they need the most "efficient and expedited" procedures. The system of voluntary disclosure for subscriber and WHOIS data places an enormous burden on companies to become quasi-judicial authorities, a role for which they do not have a legal mandate nor the inherent interest or capacity to review each order received for human rights violations in the field of criminal law. The direct disclosure mechanisms for subscriber and WHOIS data disproportionately incentivises service providers to always disclose the requested information to the extent permitted by applicable data protection laws. This is particularly worrying with regard to Parties who are not members of the Council of Europe or parties to Convention 108+.

5 ABOUT US

EFF is an international civil society non-governmental organisation with over 30,000 supporters in 99 countries throughout the world. EFF is dedicated to the protection of individuals' privacy and free expression in the digital age. EFF engages in strategic litigation and

works in a range of global and national policy venues to promote and protect human rights, foster innovation, and empower consumers: https://www.eff.org/

EDRi is an association of 44 civil and human rights organisations from across Europe. EDRi defends rights and freedoms in the digital environment and engages with policymakers across Europe to inform policies regulating the digital sphere: https://edri.org/

IT-Pol Denmark is a Danish digital rights organisation that works to promote privacy and freedom in the information society. IT-Pol works to promote privacy for citizens and transparency and openness for government. The work of IT-Pol focuses on the interplay of technology, law and politics: https://www.itpol.dk/presentation-of-it-pol

“Al Sur" is a consortium of eleven organisations which operate in the civil society and academia in Latin America, working together towards strengthening human rights in the region’s digital environment. More info of its members and work: https://www.alsur.lat/en

ARTICLE 19 is an independent human rights organisation that works around the world to protect and promote the right to freedom of expression and the right to freedom of information. ARTICLE 19 monitors threats to freedom of expression in different regions of the world, as well as national and global trends and develops long-term strategies to address them and advocates for the implementation of the highest standards of freedom of expression, nationally and globally: https://www.article19.org/

Derecho Digitales is an independent non-profit organisation based in Chile, established in 2005, working across Latin America to defend and promote the exercise of human rights in the digital environment, in particular related to freedom of expression, privacy and access to knowledge and information: https://www.derechosdigitales.org/

Homo Digitalis is the only digital rights civil society organisation in Greece. Our goal is the protection of human rights and freedoms in the digital age. We strive to influence legislators & policy makers on a national level, and to raise awareness amongst the people of Greece regarding digital rights issues. Moreover, when digital rights are jeopardised by public or private actors, we carry out investigations, conduct studies and proceed to legal actions: https://www.homodigitalis.gr/en