Joint Civil Society Response to the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime

Executive summary

We, the above signed organisations and main contributors to this submission, believe that enabling effective police investigations is important but that requests for personal data across borders must comply with human rights protections. The procedures proposed by the Cybercrime Convention Committee (T-CY) exacerbate the challenges of the Cybercrime Convention (CCC), and create the potential for serious interference with human rights.

Therefore, we encourage the Cybercrime Committee of the Council of Europe to consider the following recommendations. We believe that the Draft Protocol:

- Should not include new mechanisms for compelled subscriber information production without involvement of Parties on both sides;
- Should clarify the scope of Article 4 to exclude data from individuals' ongoing use of a service that allows precise conclusions concerning the private lives and daily habits of the individuals concerned. It should also clearly ensure that Article 4 should be applied to subscriber data as defined in CCC, excluding log-on information, dynamic IP addresses, and location data, as well as records of carrier-grade NAT (CGN) IP address and port number mappings;
- Should exclude dynamic IP addresses and log-on IP addresses as examples of subscriber information;
- Should exclude location data or any data that can reveal precise conclusions concerning the private lives and daily habits of a subscriber;
- Should require Parties to ensure that data disclosed pursuant to it will not, cross-referenced with other data, result in an unexpected level of intrusion on individuals' private lives;
- Should include a dual criminality requirement for the issuing of an order;

- Should require prior judicial authorisation by a court or an independent judicial authority to issue an order in all instances;
- Should reiterate the need for Parties to comply with Article 15 of the CCC, Conditions and Safeguards and with international human rights law;
- Should require member countries to first sign and ratify Convention 108+ for the protection of individuals with regard to the processing of personal data;
- Should make the notification to the requested Party, including the possibility to halt the direct disclosure of data, mandatory for all Parties;
- Should only impose a gag order after careful independent review by a court;
- Should impose a minimum factual basis necessary to access subscriber information only when the person investigated is suspected of planning, committing, or has planned or committed criminal acts;
- Should adopt security, encryption and authentication mechanisms for the delivery of requests and responses;
- Should ensure that the Parties' domestic laws do not impose undue restrictions on freedom of expression;
- Should ensure that the requesting Parties publish, at a minimum, aggregate information on the specific number of cross-border orders approved and rejected, a disaggregation of the orders by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each;
- Should provide service providers all the information needed to review each order and the possibility to oppose as appropriate.

I. Introduction

The Electronic Frontier Foundation (EFF), European Digital Rights (EDRi), IT-Pol Denmark, Electronic Privacy Information Center (EPIC) are pleased to submit the following comments to the Council of Europe and States Parties involved in the negotiation of the Second Additional Protocol to the Budapest Convention on Cybercrime (CCC).

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 online. 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.

EDRi is an association of 42 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.

IT-Pol Denmark is a Danish digital rights organisation that works to promote privacy and freedom in the information society. We promote privacy for citizens and transparency and openness for government. Our work focuses on the interplay of technology, law and politics.

EPIC is a leading privacy and freedom of information organization in the United States, established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.

This submission is composed of four main sections including:

- General shortcomings in terms of safeguards and due process requirements of the provisional Second Additional Protocol, covering both Article 4 and 5.
- Comments specific to Article 4 and the procedure for direct disclosure of subscriber information mechanism in line with international human rights law.
- Comments specific to Article 5 and the rules for giving effect to orders from another Party for expedited production of data
- Conclusion and recommendations

II. General remarks

2.1 New mechanisms for compelled subscriber information production without involvement of both Parties involved should not be included in the Draft Protocol

First, as we have said in our previous submission[1], we oppose "voluntary disclosures" and "direct cooperation" mechanisms. Indeed, we doubt whether such drastic expansions of cross-border data access powers are truly necessary. Direct disclosure mechanisms allow law enforcement authorities (LEAs) to bypass Mutual Legal Assistance Treaties (MLATs) by requesting and obtaining electronic data directly from service providers. Such mechanisms entail that private companies are the last line of defense of users' rights against abuses. This gives LEAs an easy avenue to access personal data without having to go through the relevant formal processes, which they might consider as "red tape", but represent in fact essential requirements of the rule of law in cross-border contexts. The risk of permitting unsupervised cross-border access to personal data that may be incompatible to Parties' legal systems, notably data protection laws, and to international legal standards is also heightened by the large number of signatories of the Budapest Convention. Improving the existing system of mutual legal assistance among countries should be the priority of the Parties to the Convention[2].

Second, we believe that enforcement of jurisdiction by a state or state agency on the territory of another state cannot happen without the knowledge and agreement of the targeted State. The mechanism introduced in Article 5 provides a better framework for the protection of fundamental rights because of the significant role given to legal authorities. Their participation provides a critical human rights vetting mechanism to help navigate disparities in legal safeguards and application of human rights standards that inevitably arise between Parties.

Third, the Draft Second Additional Protocol should clarify the scope of Article 4 to exclude data from individuals' ongoing use of a service that allows precise conclusions concerning the private lives and daily habits of the individuals concerned. It should also clearly ensure that Article 4 should be applied

1 Joint Civil Society Response to Discussion Guide on a 2nd Additional Protocol to the Budapest Convention on Cybercrime, 28 June 2018 https://edri.org/files/consultations/globalcoalition-civilsocietyresponse_coe-t-cy_20180628.pdf

2 Significant improvements are possible as evidenced by the "MLAT Reform" program of the U.S. Department of Justice that reduced the amount of pending cases by a third and therefore, increased the overall efficiency of Mutual Legal Assistance (MLA) requests processing mechanisms.

to subscriber data as defined in the CCC, excluding logon information, dynamic IP addresses, records of carrier-grade NAT (CGN) IP address, port number mappings, and location data.

Fourth, the Draft Second Additional Protocol should ensure that an order whose asserted purpose is the "identification of a subscriber", but which clearly involves or requires the disclosure or processing of data that is traffic and/or content data, should not be treated as merely a request for subscriber information.

Finally, our following recommendations refer to the substance of Article 4 in case it continues to be a part of the Second Additional Protocol, but should not be taken as support for the adoption of this new mechanism.

2.2 IP addresses are neither inherently subscriber information nor inherently traffic data

Parties have struggled to reach a solid common understanding of what types of data do or do not fall within the Cybercrime Convention's existing defined category of "subscriber information". While the CCC has clearly defined subscriber information, there hasn't been a solid common understanding of what types of data do or do not fall within the category of "subscriber information" when it comes to technical means.

In other words, Article 18.3 of the CCC defines subscriber information[3] but this definition hasn't been implemented in a clear or consistent way across various Parties' domestic laws, as observed in the T-CY report on obtaining subscriber information[4].The European Parliament's Committee on Civil Liberties, Justice and Home Affairs also noted conflicts among Parties' laws on this point, including that:

> "The mentioned definition of subscriber information and its explanation is not fully clear as, on the one hand, it explicitly excludes "other than traffic data or content data", but, on the other hand, there is no agreement among the Parties to the Convention on the demarcation between subscriber information and traffic data."[5]

The CCC definition of subscriber information contemplates revealing a subscriber's IP address as an "access number", in circumstances in which the address does not constitute "traffic data" or "content data". Although this high level rule is clear, the technical subtleties of when an IP constitutes traffic data and when it constitutes subscriber information has not been discussed widely nor explained to Parties in detail.

---

3 Article 18.3 defines subscriber information as "Any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
a. the type of communication service used, the technical provisions taken thereto and the period of service;
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."

4 Rules on obtaining subscriber information, Report adopted by the T-CY at its 12th Plenary, 3 December 2014 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1

5 Birgit Sippel and Nuno Melo, 2nd Working Document (B) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) - Scope of application and relation with other instruments Committee on Civil Liberties, Justice and Home Affairs, 6 February 2019 http://www.europarl.europa.eu/doceo/document/LIBE-DT-634730_EN.pdf?redirect

Yet IP addresses, in another context, are expressly mentioned as a form of "traffic data" as defined in Article 1 (d) of the CCC. The Explanatory Report of the CCC states that "categories of traffic data" under the Convention include "origin", which "refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services".[6]

Indeed, Article 1 (d) of the CCC defines "traffic data" as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the *chain of communication*, indicating the *communication's origin*, destination, route, time, date, size, duration, or type of underlying service." (emphasis added)

> *2.2.1 IP address requests are only requests for subscriber information when they are directed only to internet access service providers and records of carrier-grade NAT (CGN) IP address and port number mappings are traffic data*

The distinction between IP addresses as subscriber information and IP addresses as traffic data is crucial, but easy to miss. One can easily go astray by attempting to categorically assign IP addresses themselves to either category of data, independent of context and circumstances. An identifier cannot be exclusively defined as either "subscriber information" or "traffic data" in every situation. Specifically, an IP address as such is not traffic data, but the fact that an IP address reveals "the origin of a communication" renders it traffic data.

As a result, **internet access service providers (IAS providers), such as telecommunications providers, are the only service providers that disclose IP addresses as subscriber information** because they are the sole service providers to assign those IP addresses. Other service providers, such as internet browsers, social media services or email service providers, are able to attribute a certain IP address to a person because they are in the "chain of communication" and empirically observe that the IP address in question is the at the origin of one or more specific communications using their services. In this context, the IP address and other information recorded are traffic data.

When an IAS provider discloses the IP address that it has *persistently* assigned to a specific individual, this represents a disclosure of subscriber data. But when any other type of service provider, as defined in the CCC[7], reveals how the subscriber has used his or her IP address to communicate with other Internet users or services, this represents a disclosure of traffic data. Similarly, when a particular person uses a particular e-mail address, it is considered subscriber information if revealed by the e-mail provider, whereas in the case where this particular e-mail address was among those used to contact another e-mail address, it is then traffic data. **When considering IP addresses, their characterisation as either subscriber information or traffic data depends on the context and circumstances in which information about them is revealed.**[8] Hence, law enforcement agencies can make many different requests which seek IP addresses. Some of these requests seek subscriber information, while others seek traffic data.

Further, some requests that notionally seek subscriber information cannot be answered by some providers because they do not retain the relevant information, or because obtaining an answer would require them to examine traffic data. This may be the case, for example, when internet access providers use carrier-grade NAT (CGN), in which a single IP address is used simultaneously by

6 Explanatory Report of the CCC, paragraph 30.
7 Article 1 (c), CCC
8 In other words, "what is an individual's e-mail address?" is a question that produces subscriber information, while "what e-mail addresses have e-mailed a specific person?" is a question that produces traffic data.

numerous subscribers at the same moment, and any individual's relationship to this address are completely ephemeral.

The level of sensitivity of revealing IP addresses differs in every different sort of context. An IP address revealed by an ISP will almost certainly not reveal information about the subscriber's whereabouts over time, but an IP address revealed by an application provider, from its logs, is likely to do so. The difference in intrusiveness is no more surprising than the fact that a customer's name turned over by a supermarket reveals a different sort of information than a customer's name turned over by a cancer clinic.

The Protocol's Draft Explanatory Report explains that subscriber data "does not allow precise conclusions concerning the private lives and daily habits of individuals concerned." Therefore, the Report concludes that accessing such data has a lower degree of intrusiveness on fundamental rights compared to the case when other categories of data are accessed. As we have discussed above, **ensuring that this is the case in practice depends on successfully excluding access to the more intrusive and revealing data (in other words, that which "allows precise conclusions concerning the private lives and daily habits of the individuals concerned") from Article 4.**

2.2.2 The Draft Protocol should exclude dynamic IP addresses as an example of subscriber information

In previous submissions to the T-CY[9], we repeatedly highlighted the problem of extending the definition of subscriber information to dynamic IP addresses, which can be highly revealing, and harm free expression and privacy online.

The T-CY paper on static and dynamic IP addresses[10] notes a trend among several courts at national and European levels to treat requests to ISPs for dynamically assigned IP addresses as traffic data, not subscriber information, based on several analyses of the providers' practices or the providers' representations of the data protection implications of answering these requests. These courts viewed statically assigned IP addresses as more akin to telephone numbers or other kinds of identifiers that the CCC's definition of subscriber information (or corresponding definitions in national law, as appropriate) was originally intended to include, and dynamic IP addresses as less compatible with that definition.

Since this trend is already reflected in several Parties' law and also in jurisprudence at supranational levels, **the Draft Protocol should avoid creating an implication that requires or assumes that dynamic IP addresses constitute subscriber information rather than traffic data.**

---

9 Prof. Douwe Korff, Key Points Re The Cybercrime Convention Committee (T-CY) Report: Criminal justice access to electronic evidence in the cloud:Recommendations for consideration by the T-CY, 16 September 2016, https://edri.org/files/surveillance/korff_note_coereport_leaaccesstocloud%20data_final.pdf
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", 8 September, 2017, https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf
Joint Civil Society Response to Discussion Guide on a 2nd Additional Protocol to the Budapest Convention on Cybercrime, 28 June 2018, https://edri.org/files/consultations/globalcoalition-civilsocietyresponse_coe-t-cy_20180628.pdf

10 Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments", T-CY (2018)26, 25 October 2018, https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/16808ea472

2.2.3 The Draft Protocol should exclude log-on IP address as an example of subscriber information

The Draft Explanatory Report offers as an example (in paragraph 4 on disclosure of subscriber information) "the log-on IP addresses used at a specific time" for subscriber information that might appropriately be disclosed pursuant to this provision. Yet in many circumstances, this history will reveal sensitive information about an individual user's whereabouts—precisely the kind of information that the definition was meant to exclude. For example, the fact that the same particular log-on IP addresses were used by two different persons on the same night to access an information service (such as Google, Facebook, or Twitter) might, for example, reveal that they spent the night in the same place (whether or not a particular investigator immediately knows where that place is). Examining patterns in this data over time would allow an inference about changes, as when people started (or stopped) dating or living together. Similarly, log-on IP addresses directly reveal one's presence at a specific business, residence, place of worship, etc., and collecting them over time will correspondingly show patterns and habits in one's whereabouts.

The Draft Second Additional Protocol provides a reservation in Article 4, paragraph 9.b, recognizing that some Parties currently do protect this information—as well as "the IP address used at the time when an account was created [and] the most recent log-on IP address"—as traffic data. For the reasons we described in an earlier section, the Draft Protocol should ensure that "the log-on IP addresses used at a specific time" are excluded by all Parties. **There is an evolving understanding that IP addresses can be invasive of privacy and data protection rights and require a higher level of scrutiny. We believe that the Draft Protocol should be wary of creating an incentive for Parties to change their treatment of this personal information in a way that reduces protections.**

2.2.4 The Ministerio Fiscal case supports the relevance of protecting location data for fundamental rights

The Court of Justice of the European Union (CJEU) ruling on the Ministerio Fiscal case[11] states that any interference with fundamental rights should be proportionate to the seriousness of the investigated crime. Access to subscriber data to prevent, investigate, detect and prosecute criminal offences generally is only compatible with Articles 7 and 8 of the Charter of Fundamental Rights when that data does not allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned.[12] Since the Convention does not introduce a limitation on the scope of offences covered by its provisions, the procedures could be used for all criminal offences—including petty crimes[13]—and permit unjustified and disproportionate access to sensitive, personal data.

This case arose in response to a law enforcement request for access to telecommunications carrier subscriber information. The Court understood that the data at issue could not reveal people's activities, whereabouts, etc.:

> [T]he request at issue in the main proceedings [...] seeks access to only the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses. By contrast, those data do not concern, as confirmed by both the Spanish Government and the Public Prosecutor's

11 CJEU judgment on Ministerio Fiscal, C-207/16, 2 October 2018 http://curia.europa.eu/juris/liste.jsf?num=C-207/16

12 Ministerio Fiscal case, para. 60

13 Petty crimes include for example simple theft, fraud, assault according to §§223, 242, 263 of the German Criminal Code [Strafgesetzbuch] or Art. 222-11. 311-3, 313-1 of the French Criminal Code [Code pénal]

Office during the hearing, the communications carried out with the stolen mobile telephone or its location.[14]

In this context, the Court viewed the interference with fundamental rights as falling short of a "serious" interference.[15] The analysis in this case does not expressly control how to assess the sensitivity of a data request to a provider in the contrary situation where law enforcement does possess additional databases, or where the information turned over in a particular context does afford an analysis that, in practice, would "allow precise conclusions concerning the private lives and daily habits" of the persons concerned to be drawn. The Ministerio Fiscal case analysed a very particular scenario in which the Court assumed and emphasised that law enforcement did not possess additional information capable of revealing subscribers' whereabouts. In our view, the Court's concern with proportionality and strong emphasis on the kinds of inferences that could not be drawn lead to a conclusion that the use of carrier information in other circumstances often can represent a serious interference with fundamental rights in practice.

If, in fact, Article 18 of the Convention is to guarantee that - as the Draft Explanatory Report asserts - subscriber information "does not allow precise conclusions concerning the private lives and daily habits of individuals concerned," **the draft Protocol must more concretely define and limit the scope of subscriber information. One important means of doing so is to expressly exclude data derived from an individual's ongoing use of a service provider's service.**

In general, developing policies and procedures related to the disclosure of personal information must remain attentive to technical details that affect whether the data in question can, in fact, "allow precise conclusions concerning the private lives and daily habits of individuals concerned." Whether specific data allows precise conclusions about an individual's private life may change over time, in response to the volume of data collected, as well as the availability of other databases or surveillance methods with which particular data can be cross-referenced.

The Draft Second Additional Protocol should require Parties to ensure that data disclosed pursuant to it will not, cross-referenced with other data, result in an unexpected level of intrusion on individuals' private lives. The Draft Second Additional Protocol should clarify the scope of Article 4 to exclude data from individuals' ongoing use of a service that allows precise conclusions concerning the private lives and daily habits of the individuals concerned.

2.3 The Draft Second Additional Protocol increases the stakes regarding the conditions and safeguards in cross-border data requests

As we noted above, the distinction between subscriber information and traffic and content data has not been drawn clearly or consistently by Parties in national law and has not been fixed in the Draft Protocol. There is a very significant lack of harmonisz~~z~~ation in national laws on both the definition of subscriber information and the procedures that law enforcement can use to obtain it. This discrepancy has a practical effect on the fundamental rights of individuals since requests will flow between Parties with extremely different substantive rules.

As a result, existing conditions and safeguards for access to subscriber information under domestic laws vary considerably among Parties to the Cybercrime Convention. Against this backdrop, the creation of a new mechanism to rapidly compel the disclosure of subscriber information between

14 Ministerio Fiscal case, para. 59
15 Ministerio Fiscal case, para. 60

Parties is fraught with pitfalls. We propose in the following section the essential requirements of the rule of law to be put in place in cross-border contexts.

2.3.1 Dual criminality and compliance with international human rights law

The potential for Articles 4 and 5 to chill or otherwise negatively affect free expression is exacerbated by the absence of a dual criminality requirement. This principle, whereby the offence prosecuted in one State must also constitute a crime in the State in which the data is being requested, is crucial in international judicial cooperation. It provides legal certainty for individuals and service providers and prevents politically motivated or otherwise unjust prosecutions. Regular refusals to execute European Arrest Warrants in the EU show the divergences between States in terms of freedom of expression protections and their application.[16] That's why Article 25, paragraph 5 of the CCC gives a Party the possibility to make the mutual assistance conditional upon the existence of dual criminality, except if the offence is a criminal offence under its law[17]. Given the level of interference in human rights foreseen that results from the procedures introduced by the draft Protocol, **we recommend that dual criminality should be clearly referenced as a condition for issuing an order by the requesting Party and that the offence for which the order is issued should be punished similarly in both Parties.**

2.3.2 Due process and legal safeguards before disclosing the identity of an anonymous online speaker

Due process and legal safeguards before disclosing the identity of an anonymous online speaker are necessary to protect free expression and privacy. These protections are vital, because fear of reprisal might chill critical discussions of public matters of importance. It will also chill their freedom to form their thoughts and opinions in private, free from intrusive oversight by governmental entities.

Any online subscriber who does not want his or her speech connected to their permanent identity has an interest in anonymity. Online speakers may be concerned about political or economic retribution, harassment, or even threats to their lives; or they may use anonymity as part of their personal expression or self-development. The value of anonymity to free expression is broadly recognised. Librarians believe library patrons should have the right to read anonymously—an essential prerequisite for intellectual freedom and privacy. Publishers have fought to preserve the anonymity of their customers on the grounds that being known as a reader of controversial works can create a chilling effect. Anonymity allows journalists' sources to come forward and speak without fear of retaliation.

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). The European Court of Human Rights held that the right to private life encompasses an individual's interest in having her identity protected with respect to her online activity and that individuals maintain a reasonable expectation that their otherwise anonymous online activity will remain anonymous, even where the individual takes no steps to shield her IP address from third parties[18]. Compelling an ISP to identify its customer was held to be

16 See the case of Josep Miquel Arenas Beltrán, known as Valtònyc, who was the subject of a European Arrest Warrant issued by Spain because he was found guilty of insulting the monarchy and glorifying terrorism. But Belgium, the country in which he fled, refused the extradition request. https://www.bbc.com/news/world-europe-45550944

17 The fact that the offence is not place within the same category of offence, or does not have the same terminology as in the requesting Party does not allow the use of absence of dual criminality as a refusal ground.

18 Benedik v Slovenia, 62357/14, 24 April 2018 (ECtHR 4th Section), para 119.

"manifestly inappropriate" in the context of the Benedik v Slovenia case, as the mechanism relied upon offered "virtually no protection from arbitrary interference" with the right to privacy[19].

Every individual must have confidence that the service providers that host their discussions will protect their privacy and expression online. Service providers occupy a key position in online communications. Service providers often know the identity of the person who creates a website or posts material on a platform. To protect individuals' rights to anonymous expression, the draft Protocol should incentivise service providers to respect the due process rights of online speakers before identifying them. Compelled disclosure must only occur once a legally defined offence has been committed. And even in those cases, all the rights of an online speaker must be considered before identifying that individual in response to a request to do so.

In conclusion, if the national law of the requesting Party lacks those conditions and safeguards, compelling companies to identify anonymous subscriber activity online becomes highly controversial. This is why we believe that Article 4, paragraph 2 should reiterate the need for Parties to comply with Article 15 of the CCC, Conditions and Safeguards. **Each Party shall therefore ensure that the establishment, implementation and application of the powers and procedures provided for in Article 4 and Article 5 are subject to conditions and safeguards provided for under its domestic law.**

2.3.3 Prior judicial authorisation

The draft Second Additional Protocol provides broad discretion to Parties to adopt national legislation to empower any "competent authorities" to issue orders under Article 4, paragraph 1, and Article 5, paragraph 1. The approach in these provisions is the same described in paragraph 138 of the Explanatory Report of the CCC in which competent authorities are "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 (...)". This will likely encompass any "competent authority" of any Party to the Cybercrime Convention, from judges and prosecutors to any provincial or state law enforcement officers (para. 138, Explanatory report of the CCC) to produce a legal order that is valid under that Party's law in order to compel service providers to disclose that data.

The only limitation to this provision is found in paragraph 2.b of Article 4, which gives discretion to certain Parties to require "at the time of signature or when depositing its instrument of ratification" that the order must be issued by, or under the supervision of, a prosecutor, or other judicial authority, or otherwise be issued under independent supervision." **This requirement involving the authorisation of an independent judicial authority should be mandatory, not optional.**

Prosecutors in several Parties (Art. 4, para. 2.b) do not always satisfy the independence criteria, as they are likely exposed to direct or indirect instructions from the Ministries and thus to political influence.[20] The Court of Justice of the European Union held that an authority competent to issue European Arrest Warrants should be "independent"—that is to say not exposed to the risk of being subject, directly or indirectly, to directions or instructions in a specific case from the executive, such as a Minister for Justice.

19 Idem, para 129.

20 This was confirmed by the CJEU in its judgment on the joined Cases C-508/18OG (Public Prosecutor's office of Lübeck) and C-82/19PPU PI (Public Prosecutor's office of Zwickau) and in Case C-509/18PF (Prosecutor General of Lithuania)
https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-05/cp190068en.pdf

In addition, according to the Tele2 judgment of the European Court of Justice: "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." This conclusion was also shared by the ECtHR in the Benedik v Slovenia case[21], concluding that prior judicial authorisation is needed for accessing subscriber information as well as content.

In 2014 the Supreme Court of Canada 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 a court order. 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 ISP to voluntarily disclose their subscriber data.[22]

The Second Additional Protocol should therefore require prior judicial authorisation, by a court or independent judicial authority, before an order can be issued by the requesting Party under the Protocol which can expose the identity of a subscriber. We believe that an independent prior judicial authorisation guarantees that all affected human rights are duly taken into consideration before a subscriber identity is disclosed.

2.3.4 Defence access to evidence-gathering tools

In many legal systems, broadly described as "inquisitorial", law enforcement authorities and investigative judges are responsible for conducting an investigation aimed at establishing the "truth". As such, there are obligations on these authorities to use investigatory powers to gather all relevant evidence, both incriminatory and exculpatory, and not just evidence which establishes guilt. Traditional mutual legal assistance systems do not recognise the possibility for defence practitioners to request cross-border electronic data. It is rare for countries to give an explicit right to the defence to make use of cross-border evidence gathering tool. This is one of the key threats to a fair criminal justice process, hindering the ability of the accused to prepare a defence, delaying proceedings and making it impossible to ensure procedural equality between the parties.

The Draft Second Additional Protocol should ensure that the powers to the defence to demand evidence gathering are on equal terms with prosecutors, and obligations on States or service providers receiving such requests to process them with the same urgency as requests received from competent authorities.

2.3.5 Costs reimbursement

No rules for harmonising the reimbursement of the costs induced by the production and transfer of data by service providers is foreseen in the Draft Protocol. In practice, some Parties will propose the reimbursement of these costs according to their domestic laws while some others will not. We see the reimbursement of costs as an accountability measure and deterrence against misuse such as

21 Benedik v Slovenia, 62357/14, 24 April 2018 (ECtHR 4th Section), http://www.bailii.org/eu/cases/ECHR/2018/363.html

22 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.pd

unnecessary data requests. If a fee applies to each order issued or if the costs induced from the data production were covered by the requesting Party, it would create an incentive for its authority to more clearly define the volume of personal data needed and issue orders with moderation and proportionality.

III. Direct disclosure and lack of safeguards (Article 4)

3.1 Lack of factual basis for accessing subscriber data

According to paragraph 8 of the Draft Explanatory Report on Article 4, para. 1, orders may only be issued for information that is "needed" for an investigation or proceeding. The explanation goes further by referring to the principles of necessity and proportionality for European countries, derived from the European Convention on Human Rights (ECHR), the ECtHR jurisprudence and other national legislation. For Parties which are not part of the Council of Europe, the draft Protocol foresees the application of the Parties' own law, notably the principle of relevance (the data sought should be relevant to the investigation or prosecution). **The draft Protocol should impose a minimum factual basis to access subscriber information only when the person investigated is suspected of planning, committing, or has planned or committed criminal acts.**[23]

Such requirements should be explicit, as the possibility of access to any person's data, even if they are not suspected of a criminal offence, carries an important risk of abuse. Examples of Parties making intrusive or inappropriate requests are numerous, such as requests for information on journalists' phone calls to investigate the source of a leak of confidential information. Further examples were spelled out by the German Ministry of Justice, based on the EU's e-evidence proposal, notably the hypothetical case in which users of a video platform that posted messages sympathetic to climate protesters suspected of criminal conspiracy could see their data accessed, including their real names, despite their content constituting protected free expressions[24]. In the UK, a local authority was revealed to have wrongly used its powers to access communications data to check up on school applications to ensure that parents were living in the school catchment area, despite access to such personal data being restricted to the prevention and investigation of crimes[25].

3.2 Additional information accompanying the order addressed to the service provider

In Article 4, paragraph 4, a requirement should be added that any order issued to a service provider should include: (1) background information about the legal process pursuant to which it is being made; and (2) information about the service provider's possibility to refuse the order and to obtain legal assistance in furtherance of its refusal to execute the order.

3.3 Simultaneous notification to the requested Party

In general, we believe that extending the jurisdiction of a State or State agency to the territory of another State should not happen without the knowledge and agreement of the targeted State, as

23 ECHR judgment on Zakharov v. Russia, 47143/06, 4 December 2015 http://hudoc.echr.coe.int/eng?i=001-159324

24 Alexander Fanta, Germany fears new EU law could endanger climate activists and journalists, 08 July 2019 https://netzpolitik.org/2019/germany-fears-new-eu-law-could-endanger-climate-activists-and-journalists/ https://cdn.netzpolitik.org/wp-upload/2019/07/Hintergrundpapier-e-Evidence-cl.pdf.pdf

25 Tom Whitehead, Hundreds of innocent people wrongly spied on by police, 13 July 2012 https://www.telegraph.co.uk/news/uknews/law-and-order/9398419/Hundreds-of-innocent-people-wrongly-spied-on-by-police.html

foreseen in Article 4, paragraph 5.a. **A notification to the requested authorities, including the possibility to halt the direct disclosure of data, should be mandatory.**

The Draft Explanatory Report itself concedes that the "ability of a Party to be notified and consulted provides an additional safeguard" (para. 21). Yet, the procedure implies the scenario where requested Parties have no knowledge of orders being enforced on their territory and therefore, are unable to refuse orders which risk infringing human rights. This is particularly questionable since criminal laws diverge extensively between Parties to the Convention, including laws establishing immunities and privileges for journalists and lawyers. Notification and agreement of the requested Party ensures that orders comply with the legality, necessity, and proportionality principles, and it helps prevent bulk data requests from being executed.

In a case where a Party has not required notification, individuals can only rely on service providers to defend their rights (para. 7). **Privately held companies should not be the last line of defence against human rights violations in democratic societies.** What is more, 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. Furthermore, according to paragraph 11 of the Draft Explanatory Report, "each Party must ensure that service providers can lawfully comply with orders foreseen by this article in a manner that provides legal certainty so that service providers do not incur legal liability for the sole fact of having complied in good faith with an order issued". This gives great incentives to service providers to comply with an order without conducting a proper review and therefore, increases the risk of data being disclosed based on an unlawful request.

Furthermore, paragraph 5.b. introduces another optional consultation model, in which the service provider itself may consult the authorities of the requested Party. However, the Draft Explanatory Report explains in paragraph 19 that this consultation cannot be required for all orders by the requested Party – but only in "identified circumstances". These specific circumstances are not spelled out and we assume they refer potentially to the type of crime investigated or prosecuted, the type of penalty envisaged or the existence of immunities and privileges enjoyed by certain professions. **We believe that service providers do not receive sufficient information to make this kind of judgment based on the order and that restricting the possibility to consult requested authorities may enable abuses and further put the burden of protecting human rights on service providers.**

Consequently, a procedure without mandatory notification is highly problematic as it provides very few procedural safeguards, robust legal protections and oversight mechanisms. **Notification to the competent authorities of the requested Party should therefore always be mandatory.**

3.4 Legal basis for disclosure of subscriber information by the service provider

Article 4, paragraph 2 requires each Party to adopt legislative measures or other measures as may be necessary to allow service providers on its territory to disclose subscriber information to authorities in the requesting State. The Draft Explanatory Report states that this may range from removing legal obstacles for service providers to respond to an order to providing an affirmative basis obliging service providers to respond. Furthermore, each Party must ensure that service providers can respond to authorities in "good faith" without incurring a legal liability.

In some States, notably Member States of the European Union, the legislative measures foreseen by Article 4(2) may conflict with States' existing data protection laws. In the European Union, disclosure of subscriber information 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 established in Member States' national law must constitute a measure that is necessary and proportionate in a democratic society to safeguard objectives of public interest. **We consider it highly unlikely that a blanket provision that simply removes obstacles in data protection laws for voluntary disclosure of subscriber information by private service providers can comply with these fundamental rights requirements.**

Disclosure implies that personal data is transferred from the service provider to a controller in another State which may conflict with third-country provisions in States' data protection law. **In the European Union, disclosure of subscriber information to authorities in a requesting State outside the European Union or European Economic Area would have to comply with the provisions in Chapter V of the GDPR.**

3.5 Notification to the individual whose data is being sought

Paragraph 4 specifies that the requesting Party can instruct the service provider to keep the order confidential and refrain from notifying the subscriber whose data is being sought— also called a "gag order". Although, under certain specific conditions, it might be necessary to maintain the confidentiality of a production order in the early stages of an investigation, it is highly problematic to leave the decision solely in the hands of the requesting authority. The subscriber may have valid objections under relevant law and human rights principles, but—without notification—is unable to present their objections, and exercise its right to an effective remedy.

Indeed, any such gag order should only be imposed after careful independent review by an independent judicial authority. For example, in 2017, a Los Angeles federal court ruled that Adobe could not be indefinitely gagged about a search warrant ordering it to turn over the contents of a customer account[26]. Gag orders prevent service providers from notifying users that some authorities are requesting their data and from being transparent about surveillance in general. In the case where a production order results in a criminal proceeding, a person who is targeted by an order should be notified as soon as possible in the criminal proceedings in order to adequately exercise his or her right to a fair trial. It is especially important in cases where criminal proceedings move forward into a trial, as the defence should also be able to collect evidence, according to the principle of equality of arms. **The Protocol should provide specific requirements for the timely notification of the subscriber from the requesting Party, the requested Party, or the service provider.**

States' 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 State, 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 State'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). **A request for non-notification by the requesting State cannot override obligations in data protection laws in the requested State.**

3.6 Transparency Requirements

26 Andrew Crocker, Adobe Puts an End to Indefinite Gag Order, 24 April 2017 https://www.eff.org/deeplinks/2017/04/adobe-puts-end-indefinite-gag-order

Each requesting Party should publish, at a minimum, aggregate information about the number of cross-border orders approved and rejected, a disaggregation of the orders by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by those orders. **Those requesting Parties should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting access to their data. Service providers should be allowed to do the same.**

In case the simultaneous notification is maintained as optional, **the Protocol should require more scrutiny by requested Parties that don't use the notification mechanism under Article 4, paragraph 5.a and b. so that they ensure that the mechanism is being used consistently with their domestic legal system, constitutional requirements and international human rights obligations.**

3.7 Security and authenticity

Systems and mechanisms intended to allow law enforcement access to personal data have been actively abused for malicious hacking and espionage. The Draft Explanatory Report appropriately recognises the fact that new cross-border order mechanisms can create new privacy and information security risks where orders are fraudulent or not properly authenticated, or where responsive data is delivered over an insecure channel and intercepted by third parties.

However, the Draft's response to these concerns remains entirely permissive in Article 4 paragraph 6 and Article 5 paragraph 5, indicating that a Party may adopt security or authentication mechanisms for the delivery of requests and responses. Instead, **the Protocol should adopt security, encryption and authentication mechanisms for the delivery of requests and responses.** If they are optional and especially if they are agreed upon bilaterally and on a case-by-case basis, the likeliest outcome will be the frequent use of unencrypted and unauthenticated channels. This would allow, for example, a malicious actor to impersonate a public authority in another State in order to improperly access a target's personal data with a counterfeit request.

This risk is substantially greater in the environment foreseen by the Second Additional Protocol because a large number of private-sector companies will be responsible for individually authenticating and answering requests from foreign entities, including those with which they have never dealt before and those with whom they might deal with extremely infrequently. A local police authority in one Party may for example request data from a small local IAS provider in another Party; these entities will not only not have an established relationship but they may literally never have heard of one another before. The IAS provider in this case should not be put in the position of having to informally verify the request without technical guidance from its own government, nor should it be encouraged or incentivised to answer what appears to be a random request with no verification.

In order to enable service providers in the private sector to verify that the request is valid, the Secretariat of the Council of Europe should maintain a public registry of all authorities that can issue requests for disclosure of subscriber information in accordance with Article 4. The public registry should contain information that allows service providers to authenticate the electronic contact details of the issuing authority, such as fingerprints of electronic signatures. At a minimum, the public registry should contain a complete list of access numbers (e.g. fax numbers and email addresses) for responses to requests for disclosure of subscriber information under Article 4.

The Protocol should expressly require Parties to define, declare, and keep up-to-date the rules and technical mechanisms to be used for the secure sending and reception of orders and replies under the Protocol. Alternatively, the Protocol could create a formal process through which Parties' technical

representatives can identify best practices in this regard which will then be published by the Council of Europe T-CY Secretariat.

IV. Giving effect to orders from another Party for expedited production of data (Article 5)

4.1 The service provider's ability to oppose an order

Article 5, paragraph 3.b. suggests that the supporting information to an order, including "the domestic legal grounds that empower the authority to issue an order" and "the legal provisions" for the offence being investigated, should be kept secret from the service provider unless the requested Party gives its consent. **We believe service providers should always have the possibility to challenge orders that request data.** Therefore, service providers, at a minimum, must be able to receive all the information needed to review each order. This is even more critical if the subscriber does not get notice, leaving the service provider as the only entity able to raise objections. This does not mean service providers should be the sole arbiter of the legality of a given order (see Part II "Simultaneous notification to the requested Party" above).

While the Draft Explanatory Report notes that sometimes the "facts and statement regarding the relevance of the information or data" must be kept secret, this should be, at most, a rare exception, and only when ordered by a judicial authority.

V. Conclusion

The Second Additional Protocol further creates a two-tier system where some Parties put necessary safeguards in place, while others opt for the most intrusive methods because they believe they need the most "efficient and expedited" procedures. The draft Protocol gives the possibility for Parties to compel service providers to hand over personal data without strong safeguards, oversight and transparency mechanisms. This is particularly worrying with regard to Parties who are not members of the Council of Europe or parties to Convention 108+.

Indeed, there is not even the requirement that all Parties to the Cybercrime Convention must also be a party to the European Convention of Human Rights (ECHR) or, for non-European States, the International Covenant on Civil and Political Rights (ICCPR), including their enforcement mechanisms, or to the Convention 108+. The elaboration of a Second Additional Protocol should be an opportunity to avoid a race to the bottom regarding human rights safeguards and standards. **Signatories to the Convention that have not yet done so[27] should urgently consider signing and ratifying Convention 108+.**

We are also very concerned by the rule of law implications of the direct disclosure procedure introduced by Article 4 of the draft Protocol, as it is enabling scenarios in which only private companies will have the opportunity to oppose abusive and unlawful requests for data. This places an important burden on companies, which do not have the mandate nor the inherent interest or capacity to review each order received for human rights violations in the field of criminal law. This is exacerbated by Article 5, which would deny the service provider the information necessary to decide whether to object.

Rather than first seeking to create a system that enables law enforcement authorities to act without judicial authorisation of the Party where the data are stored, to request subscriber information, the Council of Europe should give priority to making mutual legal assistance more effective.

27 Currently Australia, Canada, Costa Rica, Chile, Dominican Republic, Ghana, Israel, Japan, USA, Peru, Paraguay, South Africa, Sri Lanka, Panama, Philippines and Tonga haven't even signed Convention 108 yet. Furthermore, 20 Parties have not yet signed Convention 108+, of which the signature and ratification process is still ongoing.