Privacy & Human Rights in Cross-Border Law Enforcement

Joint Civil Society Comment to the Parliamentary Assembly of the Council of Europe (PACE) on the Second Additional Protocol to the Cybercrime Convention (CETS 185)

Ver 2 – August 9, 2021

TABLE OF CONTENTS

TABLE OF RECOMMENDATIONS

Executive Summary

Derechos Digitales, the Electronic Frontier Foundation (EFF), European Digital Rights (EDRi), the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), Fundación Karisma and Association of Technology, Education, Development, Research and Communication (TEDIC) are pleased to provide these recommendations to the Parliamentary Assembly of the Council of Europe (PACE) to assist in its deliberation on the draft Second Additional Protocol to the Budapest Convention on Cybercrime.

The draft Protocol will reshape cross-border law enforcement data-gathering on a global scale. In particular, the draft Protocol's objectives are to facilitate cross-border investigations between countries with varying legal systems and standards for accessing people's personal information. Unfortunately, in seeking to meet this objective, the Protocol as drafted is flawed in several key respects that, unless amended, will have serious negative implications for human rights.

As elaborated below, the draft Protocol's flaws can be grouped into three categories. First, the law enforcement powers it recognizes are mostly mandatory to all signatories, whereas the majority of its human rights safeguards are optional. Second, the draft text contains defects that will have seemingly unintended harmful consequences for human rights. Third, the draft Protocol actively attempts to undermine settled law in regional and national legal systems of many anticipated signatories.

In an attempt to cater to would-be signatories with widely varying criminal justice systems, the draft Protocol's law enforcement powers are largely mandatory while most of its human rights safeguards are optional. As a result, the draft Protocol's safeguards frequently allow the lowest common denominator to prevail, leading to substantial erosion of privacy, data protection, freedom of expression and human rights. This inconsistent approach is most notable with respect to the core data protection safeguards established in Articles 14.2 - 14.15. These safeguards fall well short of established modern data protection principles. Yet even these basic safeguards are 'optional' under the Protocol in that they can be superseded by any informal secret agreement between Parties or, seemingly, between their policing agencies in joint investigative contexts. Many of the Protocol's other central safeguards are equally fully optional in nature, and have no effect at all unless they are invoked through

notification at the time of the Protocol's adoption (see Articles 19.3). By stark contrast, derogation from the Protocol's intrusive law enforcement powers requires an explicit reservation that can only be asserted at the time of the Protocol's adoption (Articles 19 and 20). The net impact of this one-sided approach is an untenable erosion of human rights.

Second, the hasty nature of the drafting process and its lack of stakeholder input is evident in clear defects in the Protocol's text. Article 7, for example, empowers law enforcement agencies to access subscriber data from service providers based in other Parties' territories. Parties may limit the scope of Article 7's application by removing disclosure of various "access numbers" (e.g. IP address, dynamic IP address, static IP address, phone number) from Article 7's scope. However, most regional and national human rights and national legislative frameworks limit disclosure of subscriber information on the basis of different considerations, such as the sensitivity of the disclosure, the absence of reasonable grounds or based on the disclosure's potential to identify the subscriber by disclosing the name or address associated with their account. There is no evident rationale for limiting Article 7 on the sole basis of which access number is being disclosed.

Similarly, the interaction between Articles 12 and 14 creates problems that we believe were not intended by the drafters. Article 14 allows Parties to bypass the numerous data protection safeguards encoded in Articles 14.2 – 14.15 by mutual agreement. Article 12 empowers frontline law enforcement authorities to enter into informal agreements to govern specific joint investigations on an ad hoc basis on behalf of Parties. The combined impact of these two Articles seems to be that frontline officials are able to bypass the draft Protocol's central data protection safeguards without any approval or input from a Party's government or any need to even publicly disclose an agreement is in place. If allowed to stand, this constitutes a major weakness in the draft Protocol's core data protection scheme and one that we believe is unintended.

Third, the Protocol as drafted actively undermines settled law in a number of ways that we find disturbing. The Protocol expressly mischaracterizes access to subscriber information. It suggests that access to subscriber data does not allow law enforcement to draw precise conclusions concerning the private lives and daily habits of individuals. This characterization reflects an outdated understanding of subscriber information and directly contradicts more recent findings in courts at the highest national and regional levels. Access to subscriber data will frequently reveal sensitive details regarding the daily lives of individuals—almost invariably so when the

individuals in question are protected by immunities and privileges. Unfettered access to subscriber data poses a dire threat to online anonymity and places whistleblowers, journalists, politicians, political dissidents, and others at risk.

The draft Protocol also impedes local data protection authorities in determining whether adequate safeguards are in place to permit transfers of personal data to foreign jurisdictions despite judicial confirmation of this role. Under Article 14, transfers may only be suspended if there is "substantial evidence" of "systematic or material breach", setting a far higher standard for suspending transfers than that adopted by legal regimes and courts particularly in the European Union. Under Article 14, the executive branch of Member States may also impose other, more restrictive preconditions for the suspension of transfers into any qualifying agreement it enters with another Party. The net result is that the draft Protocol permits the executive branch to unilaterally encumber independent regulators seeking to exercise their jurisdiction over data transfers.

Collectively, these and other elements of the draft Protocol will substantially erode global privacy, data protection and human rights in cross-border law enforcement contexts. The enclosed recommendations seek to ameliorate the worst elements of this proposal, strengthening human rights protections while leaving intact law enforcement powers that will improve the efficiency and speed of cross-border investigations.

To this effect, we make the following recommendations:

- The draft Protocol's treatment of subscriber information must be aligned with judicial findings by properly describing its sensitive nature and its capacity to reveal insights regarding individual's private lives (**Recommendation 1**).
- Safeguards adopted for subscriber data must also be commensurate with the sensitive insights into an individual's private life that can be revealed when subscriber data is disclosed. Articles 6 and 7 must be modified to provide adequate safeguards and as such we recommend that:
    - Article 8 of the draft Protocol provides the best vehicle for facilitating this form of access while still maintaining a substantial amount of flexibility for different approaches to criminal justice. It should become the sole vehicle for cross-border access to subscriber data for all Parties (**Recommendation 2**) or, if Article 7 is retained, the draft Protocol must at minimum be amended to allow for more nuanced reservations with respect to that

Article (**Recommendations 3-4**).

- If Article 7 is retained, additional safeguards must also ensure that Parties are notified or consulted when requests are issued to service providers in their territory and that sufficient information and context is provided to ensure the human rights implications of a request can be properly assessed (**Recommendations 5-6**). Independent judicial authorization should also be a required condition for cross-border subscriber disclosures or, at minimum, Parties must be able to impose that condition on requests directed to service providers in their territory (**Recommendations 7-8**).

- Article 12 of the draft Protocol creates a framework for international Joint Investigative Teams comprising various authorities from two or more Parties to the Protocol. It contemplates highly intrusive cross-border investigative techniques without adequately ensuring respect for core safeguards of the draft Protocol and for the laws and human rights standards of countries in which these techniques are implemented. We therefore recommend that:

  - Article 12 and its accompanying explanatory text must be amended to confirm that joint investigative teams will be limited in time and purpose, so that they are established for specific investigations of specific crimes and do not become open-ended investigative mandates (**Recommendation 10**).

  - Under Article 12, Joint Investigation Teams may operate under their own agreements. The draft Protocol must ensure that these agreements cannot bypass the core safeguards embedded in the Protocol, including the data protection provisions in Article 14 (**Recommendation 9**) and safeguards in Articles 6-10 of the draft Protocol (**Recommendation 13**).

  - Article 12 and its accompanying explanatory text must also be amended to confirm that investigative teams respect local laws and standards when operating in a Party's territory. This requires the involvement of a Party's government when investigative team agreements governing investigative teams are made so that frontline officers are not able to unilaterally bypass critical safeguards (**Recommendation 11**) and that investigative measures within a given territory be taken by that territory's authorities and, in all circumstances, in accordance with that territory's laws, as is the case in CETS 182 (**Recommendation 12**).

  - To avoid forum shopping, the explanatory text accompanying Article 12 must explain that, where an investigative technique can be properly taken by multiple participants in an investigative team, the most privacy and human rights-protective investigative path should be taken (**Recommendation 13**).

- Many of the draft Protocol's provisions allow Parties to impose confidentiality requirements, yet the draft Protocol does not provide any clear and adequate limits on when confidentiality can be imposed. Investigative secrecy can be necessary, but can also shield problematic practices that pose a threat to human rights. We recommend that the draft Protocol be amended to ensure that confidentiality is the exception, not the rule, only to be invoked where strictly necessary to achieve important public interest objectives and in a manner that respects the legitimate interests and fundamental rights of individuals (**Recommendations 14-15**).

- Article 14 imposes a number of specific safeguards with the intention of supplementing the more general and undefined safeguards which characterize human rights protection under the Budapest Cybercrime Convention. Unfortunately, in effect, Article 14 does more to undermine than to advance data protection. To mitigate this impact, we recommend that:

    - Article 14 must be amended so that the specific protections it imposes in Articles 14.2-14.15 cannot be abrogated by simple formal or informal agreement among Parties (**Recommendation 16**). We note that these safeguards are only triggered in situations where the law enforcement powers recognized by the draft Protocol are invoked, and as such we see no reason why a minimal level of data protection should not be established.

    - Article 14 must also be amended to clarify that independent regulators remain fully responsible for assessing the adequacy and sufficiency of data protection safeguards where personal information is being transferred between jurisdictions. This is particularly critical in light of the wide and inconsistent range of legal systems among anticipated signatories (**Recommendation 17**).

    - As the safeguards in Articles 14.2-14.15 fall short of what is required by modern data protection frameworks such as Convention 108/+, Parties must be permitted to supplement these safeguards with additional protections (**Recommendation 18**) and must be permitted to reserve the Protocol's most intrusive powers with respect to any other Party that has failed to ratify Convention 108+ (CETS 223)(**Recommendation 19**).

    - While the European Committee on Crime Problems (CDPC) must be involved in all revisions, consultations and reviews relating to the implementation and future evolution of the draft Protocol, there is no comparable requirement to involve the Consultative Committee on Convention 108 (T-PD), independent data protection authorities, or any privacy or human rights subject matter experts. This lack of a formal consultative role compounds flaws already evident in the current Protocol's drafting process, and must be remedied through a formal consultation obligation (**Recommendation 20**).

We thank you for taking the time to review our submission, and urge you to implement our recommendations.

Introduction

Derechos Digitales, the Electronic Frontier Foundation, European Digital Rights (EDRi), the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), Fundación Karisma and TEDIC are pleased with this opportunity to provide our input to the Parliamentary Assembly of the Council of Europe (PACE) to assist in its deliberation on the draft Second Additional Protocol to the Budapest Convention on Cybercrime.

The draft Protocol will establish a comprehensive system for cross-border law enforcement investigations. A range of intrusive practices will occur under its auspices, and the implications for privacy, data protection, free expression and fundamental human rights are significant.

Unfortunately, the draft Protocol does not currently include sufficient protections for fundamental rights.

We urge PACE to take our concerns and recommendations into account and ensure that cross-border law enforcement investigations embed an adequate level of respect needed for privacy, data protection, free expression and human rights.

Section 1. Subscriber Data & Online Anonymity

The draft Protocol must recognize that access to subscriber data under certain conditions can be highly intrusive and implicate fundamental rights.

Unfettered access to subscriber data can threaten whistleblowers, journalist sources, dissidents, political figures, and others while undermining core privileges and immunities. The draft Protocol seeks to diminish the sensitive nature of subscriber data, and resulting in a range of intrusive powers.

While our analysis below focuses predominantly on Article 7 of the Protocol, we note that Article 6 raises many of the same problems as those identified below as it implicates similar privacy and human rights interests and contains similarly sparse safeguards.

1.1. Do not mischaracterize the intrusiveness of subscriber data access.

Paragraph 92 of the Explanatory Memorandum to the draft Protocol indicates that subscriber data is highly valuable at early investigative stages. It also claims that subscriber data "does not allow precise conclusions concerning the private lives and daily habits of individuals…." This dismissive characterization ignores the intrusive potential of law enforcement identification capabilities and directly conflicts with judicial precedent, particularly when considering the Protocol's broad definition of subscriber information, which permits identification of anonymous online activity.

Frequently, when law enforcement agencies seek access to subscriber data, it is for the express purpose of identifying anonymous online activity. Common law enforcement data access scenarios remove anonymity and expose intimate details of individual's private lives by linking anonymous activity to those individuals. The Court of Justice of the European Union has held that public authority access to subscriber data may constitute a 'serious' interference with privacy where used to associate anonymous communications activity with particular subscribers, allowing precise conclusions to be drawn regarding the private lives of those subscribers.[1] The European Court of Human Rights has explicitly held that accessing some types of subscriber data for the purpose of identifying anonymous online activity can "reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle."[2] The United Nations Special Rapporteur on free expression and other national courts have reached similar conclusions, and the description adopted by the explanatory text is in direct contradiction with these.[3]

Article 7 and its accompanying Explanatory text also fail to recognize that subscriber data will almost invariably be sensitive when it concerns individuals protected by immunities and privileges.

We believe that it is inappropriate for a Council of Europe treaty to characterize subscriber data in

[1] Case C-207/16, *Ministerio Fiscal*, October 2, 2018 (CJEU, Grand Chamber), paras 60-61.

[2] *Benedik v Slovenia*, App No 62357/14 (ECtHR, 4th Section), paras 109-119: "109. Furthermore, the Court cannot ignore the particular context in which the subscriber information was sought in the present case. The sole purpose of obtaining the subscriber information was to identify a particular person behind the independently collected content revealing data he had been sharing. ... Information on such activities engages the privacy aspect the moment it is linked to or attributed to an identified or identifiable individual. Therefore what would appear to be peripheral information sought by the police, namely the name and address of a subscriber, must in situations such as the present one be treated as inextricably connected to the relevant pre-existing content revealing data. To hold otherwise would be to deny the necessary protection to information which might reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle."

[3] See, for example, *R v Spencer*, [2014] 2 SCR 212; United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, A/HRC/29/32, https://www.undocs.org/A/HRC/29/32.

a manner that contradicts the potential sensitivity of this data, as well as determinations of the European Court of Human Rights.

> **Recommendation 1: Align the draft explanatory text's description of subscriber data with binding judgements.**
>
> 92. Subscriber information is the most often sought information in criminal investigations relating to cybercrime and other types of crime for which electronic evidence is needed. It provides the identity of a particular subscriber to a service, his or her address, and similar information identified in Article 18.3 of the Convention. ~~It does not allow precise conclusions concerning the private lives and daily habits of individuals concerned, meaning that its disclosure may be of a lower degree of intrusiveness compared to the disclosure of other categories of data.~~

1.2. Article 8 should be the primary path to subscriber data.

Article 7 compels parties to provide direct cross-border access to subscriber data without requiring adequate safeguards. Parties may require independent judicial authorization for domestic production orders but, under Article 7, any laws that might impede local service providers from responding to a foreign non-judicial request must be removed.

As a result, the Protocol permits access to subscriber data under conditions that the ECtHR described as offering "virtually no protection from arbitrary interference", as under the law:

> … the police, having at their disposal information on a particular online activity, could have identified an author by merely asking the ISP provider to look up that information. Furthermore no independent supervision of the use of these police powers has been shown to have existed at the relevant time, despite the fact that those powers, as interpreted by the domestic courts, compelled the ISP to retrieve the stored connection data and enabled the police to associate a great deal of information concerning online activity with a particular individual without his or her consent.
>
> … the Court is of the view that the law on which the contested measure, that is the obtaining by the police of subscriber information associated with the dynamic IP address in question (see paragraph 7 above), was based and the way it was applied by the domestic courts lacked clarity and did not offer sufficient safeguards against arbitrary interference with Article 8 rights.[4]

Where national law prevents service providers from responding to subscriber data requests

[4] *Benedik v Slovenia*, App No 62357/14 (ECtHR, 4th Section), paras 7 and 129-133. Note that despite this finding, the court made no ruling on the proportionality of the law, finding instead that the specific law in question did not provide a lawful basis for the search in question, which was therefore not "in accordance with the law." Note additionally, however, that the provision at issue in App No 62357/24 required "grounds for suspecting" that access to the subscriber information in question is needed to uncover a criminal offence or its perpetrator (*Benedik*, para 36). Article 7 does not require that such grounds exist and expressly indicates that the basis for such grounds need not be itemized in the request (see discussion below).

without appropriate safeguards such as a court order and/or a reasonable grounds requirement, Article 7 requires these legal impediments to be removed.[5]

Article 7 also creates unjustifiable asymmetries in national law. In a survey of data access regimes conducted by the Council of Europe's Cybercrime Committee (i.e. the drafting committee for this Protocol, T-CY), many surveyed countries required prior judicial authorization before law enforcement could access some types of subscriber data.[6] Under Article 7, these states will need to establish a lawful basis for foreign access on a more permissive basis than what is granted to their own law enforcement agencies.[7] Similarly, many service providers (e.g. Internet Service Providers in Chile) require prior judicial authorization as a best practice when processing many types of national subscriber data requests and will be discouraged from doing so.[8] In part, this will be because Article 7 relies on "orders" that are binding as a matter of national law but only unenforceable due to their cross-border nature. Service providers will find it more difficult to deny requests that are, in effect, orders, even if these orders are not enforceable in a cross-border context.[9]

National law in many jurisdictions also imposes other critical safeguards that Article 7 fails to contemplate or categorically excludes. For example, some states prohibit their policing agencies based on expressive activities. Article 7 places no explicit restrictions on targeting activities which implicate fundamental rights including expressive activities in cross-border requests and requesting states are not required to explain why the request in question outbalances expressive interests when issuing a request for subscriber data.[10] Similarly, some states limit national policing agencies from requiring subscriber data access in the absence of reasonable grounds

[5] *R v Spencer*, [2014] 2 SCR 212; *Personal Information Protection and Electronic Documents Act*, SC 2001, c 5, paragraph 7(3)(c.1).

[6] https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/16808ea472.

[7] EM, para 100: "for Parties that have data protection requirements, this would include providing a clear basis for the processing of personal data."

[8] https://www.derechosdigitales.org/wp-content/uploads/QDTD-2021.pdf.

[9] See, for example, *Doe v Ashcroft*, (2004) 334 F.Supp.2d 471 (United States, SDNY), p 501, narrowed on other grounds, *Doe v Mukasey*, 549 F.3d 861 (2008): "Objectively viewed, it is improbable that an FBI summons invoking the authority of a certified 'investigation to protect against international terrorism or clandestine intelligence activities,' and phrased in tones sounding virtually as biblical commandment, would not be perceived with some apprehension by an ordinary person and therefore elicit passive obedience from a reasonable NSL recipient."

[10] As with aspects of the underlying Convention (CETS 185), Article 13 of the Protocol could be interpreted to require an explicit prohibition on the targeting of expressive activities and the need to balance competing expressive interests. However, it is largely left to national law to determine whether such safeguards are required under Article 13 or not (CETS 185, Explanatory Memorandum, paragraph 145). The absence of explicit safeguards for anonymous expressive activity is deeply problematic in light of the cross-border nature of the Protocol and the wide range of legal systems among anticipated signatories, who have no shared commitments to any "minimum safeguards arising pursuant to obligations...undertaken under applicable international human rights instruments" (CETS 185, Explanatory Memorandum, para 145). It is therefore incumbent on the Protocol to establish these critical safeguards explicitly.

establishing that the data sought will advance a criminal investigation.[11] Far from explicitly including a reasonable grounds requirement, Article 7 implicitly concludes instead that no such grounds are necessary in cross-border requests.[12]

Article 7 therefore erodes privacy standards even where appropriate protections already exist. We recommend that Article 7 be removed in its entirety from the text of the Protocol. This would permit Article 8 to form the primary basis by which subscriber data is accessed in cross-border contexts. While Article 8 could benefit from additional safeguards as well, it provides a more appropriate basis for access to subscriber data even as it currently stands in two key respects—it directly incorporates traditional grounds for refusal of a mutual assistance request and it relies on a Party's national legal authorization regime when processing requests, thereby avoiding the untenable asymmetries identified above.[13]

> **Recommendation 2: Do not mandate direct cooperation between service providers and foreign law enforcement for subscriber data requests.**
>
> Article 7 does not provide sufficient baseline safeguards for subscriber data consistent with international standards of human rights and best practices as encoded in many national legal regimes or adopted by service providers. Article 8 allows states to impose meaningful safeguards and is therefore a more appropriate basis for cross-border access to subscriber data. Article 7 should be removed in total from the Protocol.

In the alternative, if Article 7 remains in the Protocol, then paragraph 7.9 must be amended to provide greater flexibility in Parties' ability to limit the scope of Article 7. Paragraph 7.9 permits Parties to replace Article 7 with Article 8 as the primary mechanism for addressing cross-border access requests to some or all types of subscriber data. This provision is flawed in two respects.

First, Parties may only remove a subset of the various types of subscriber information that law enforcement frequently access during of an investigation. Specifically, under paragraph 7.9.b,

---

[11] *Benedik v Slovenia*, App No 62357/14 (ECtHR, 4th Section), paras 7, 36 and 129-133; Katitza Rodriguez, Veridiana Alimonti & Nathalie Fragoso, "The State of Communication Privacy Law in Brazil", August 2020, https://necessaryandproportionate.org/uploads/2020-brazil-en-faq.pdf, p 13; Tamir Israel, "Law Enforcement Access to Subscriber Data in Canada: Backgrounder", March 3, 2017, https://cippic.ca/uploads/20170303-Subscriber_data_in_Canada-Backgrounder.pdf.

[12] Contrast paragraph 7.4 with paragraphs 8.3.iv-v. While service providers and states may request additional information in some instances, it is clearly anticipated that reasonable grounds will not be the norm (see EM, para 104: "No statement of facts is required...").

[13] Paragraphs 8.8 and 8.1, respectively. Notably, as every request under Article is processed by the responding Party's authorities, requests can be systematically vetted for human rights considerations before a request is processed, as is standard for mutual assistance. By contrast, paragraph 110 of the Explanatory Memorandum to the draft Protocol suggests that invoking the traditional grounds for refusing mutual assistance codified in Cybercrime Convention (ETS 185) should only be invoked sparingly. Additionally, responding Parties must rely on their national legal framework to require disclosure of subscriber data. As a result, no asymmetries are created between processing of foreign and domestic requests.

Parties may only remove disclosure of "access numbers" from the scope of Article 7. Access numbers include various device identifiers such as telephone numbers and IP addresses and can include other numbers with more intrusive potential such as cell phone IMSI numbers. But Article 7 itself applies to a broader range of subscriber information including account identifiers—that is, any information that can establish "the subscriber's identity, postal or geographic address."[14] Parties cannot currently reserve access to account identifiers under paragraph 7.9.b.

As a result of this formulation, Article 7's reservation power does not allow Parties to reserve the most intrusive categories of subscriber information disclosure. The dire threat to anonymity arises most frequently when a service provider discloses the name of a customer already associated with anonymous online activity and related access numbers already known to police.[15] Allowing Parties to remove types of access numbers (e.g. all IP addresses, dynamic IP addresses, static IP addresses, or mobile telephone numbers) therefore fails to address some of the most problematic privacy threats posed by Article 7, as law enforcement will continue to be able to demand the name and address of Internet subscribers associated with access numbers.

> **Recommendation 3: Extend reservations to preserve online anonymity.**
>
> Article 7.9.b. if disclosure of certain types of [**subscriber information** ~~access numbers~~][**account identifiers or** access numbers] under this article would be inconsistent with the fundamental principles of its domestic legal system, reserve the right not to apply this article to such [**subscriber information** ~~numbers~~][**identifiers or numbers**].
>
> or
>
> Article 7.9.b. if disclosure of ~~certain types of access numbers~~ **subscriber information associated with certain types of access numbers** under this article would be inconsistent with the fundamental principles of its domestic legal system, reserve the right not to apply this article to such numbers.

Second, paragraph 7.9 may only be invoked by a signatory when adopting the Protocol. As a result, Parties will be unable to designate Article 8 as the sole means of accessing some or all types of subscriber data even if their legal systems recognize additional safeguards for subscriber information at some point in the future.

[14] Draft Protocol, paragraph 3.1; Convention on Cybercrime, CETS 185, Paragraph 18.3.b.

[15] See, for example: *Benedik v Slovenia*, App No 62357/14 (ECtHR, 4th Section), para 7 ("In response, on 10 August 2006 the ISP gave the police the name and address of the applicant's father, who was a subscriber to the Internet service relating to the respective IP address."); *R v Spencer*, [2014] 2 SCR 212.

In taking this approach, the drafting committee effectively freezes current state practices at a time when courts around the world and international human rights bodies are increasingly recognizing the sensitive nature of subscriber data disclosure. Moreover, paragraph 7.9.b may only be invoked if providing access to the access number in question is "inconsistent with the fundamental principles" of the Party. However, courts in many jurisdictions have not yet definitively resolved what safeguards are minimally required to meet fundamental constitutional requirements.

In addition, many states require judicial control and/or the presence of reasonable grounds before their policing agencies may access subscriber information as a best practice. But paragraph 7.9.b's scoping limitation does not allow for reservations invoked in order to align cross-border practices with national legal practice unless these practices are demonstrably premised on fundamental principles of the Party's legal system.

Finally, Article 7 does not allow for reservations based on circumstances rather than types of subscriber information. This limitation is especially problematic considering the manner in which Article 7 departs from core principles of mutual legal assistance. Specifically, paragraphs 25.4 and 27.4 of the Convention of Cybercrime recognize a Party's right to refuse a request for assistance in order to preserve sovereignty, security or essential interests such as fundamental human rights. This aligns with standard practice in mutual legal assistance. Article 7 deters systematic application of these principles by rendering its consultation and notification mechanisms optional (paragraphs 7.5.a and 7.5.b) and by further indicating that impediments to cooperation and refusals of requests should be "strictly limited".[16] Parties may also wish to employ reservations in other circumstances, such as where privileges and immunities are implicated. In light of this limitation, Parties should be able to reserve Article 7 from applying to other identified circumstances.

Imposing time and scope limits on Article 7's reservation mechanism effectively commits states to a particular level of protection despite the ongoing evolution of jurisprudence in relation to subscriber information. It also precludes reservations intended to align cross-border access with national practice and with widely accepted tenets of mutual legal assistance, posing a threat to the fulfillment of human rights. If Article 7 is retained, these time and scope limitations must be removed.

[16] Explanatory Memorandum, paragraphs 108-110.

Recommendation 4: Ensure parties can remove subscriber information from Article 7 in accordance with jurisprudential and legislative developments over time and to address disparities with national law or established principles of mutual legal assistance.

Article 7.9. At **any** ~~the~~ time**, upon notifying the Secretary General of the Council of Europe** ~~of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval~~, a Party may:

a. reserve the right not to apply this article; or

b. ~~if disclosure of certain types of access numbers under this article would be inconsistent with the fundamental principles of its domestic legal system,~~ reserve the right not to apply this article to **types of subscriber information** ~~such numbers~~ or other identified circumstances.

1.3. Provide more safeguards if Article 7 is retained.

If Article 7 remains, additional safeguards must be added to lessen its intrusive impact on fundamental rights.

Service providers are expected to comply with Article 7 requests, which the Protocol formulates as 'orders' that are binding at a national level but are not to be directly enforced due to their cross-border application.[17] Service providers will also be aware that refusal of a request will likely lead to an order compelling disclosure under Article 8, further deterring providers from refusing any particular requests.[18] Indeed, under Article 7, service providers are not even given enough information to properly assess or process a request in order to identify circumstances that are inconsistent with fundamental rights.

Paragraph 7.5 optionally allows Parties to impose simultaneous notification or consultation mechanisms for subscriber data requests (paragraphs 7.5.a and 7.5.b, respectively). If invoked, Parties will be able to assess requests and refuse those that are contrary to fundamental rights e.g. because of privileges and immunities guaranteed by national law.

Since notification or consultation of authorities in the requested Party is essential for upholding

[17] See discussion preceding Recommendation 2:, above and, in particular, paragraph 118 of the Explanatory Memorandum.

[18] Explanatory Memorandum, paras 118 and 131 ("For enforcement of the order via Article 8, this Protocol contemplates a simplified procedure of conversion of an order under[Article 7] to an order under Article 8 to facilitate the ability of the issuing Party to obtain subscriber information."). See also: *Doe v Ashcroft*, (2004) 334 F.Supp.2d 471 (United States, SDNY, p 501, narrowed on other grounds, *Doe v Mukasey*, 549 F.3d 861 (2008): "Objectively viewed, it is improbable that an FBI summons invoking the authority of a certified 'investigation to protect against international terrorism or clandestine intelligence activities,' and phrased in tones sounding virtually as biblical commandment, would not be perceived with some apprehension by an ordinary person and therefore elicit passive obedience from a reasonable NSL recipient."

fundamental rights, it should be mandatory in Article 7 instead of depending on a declaration by the Parties.

> **Recommendation 5: Introduce mandatory notification or consultation of authorities in the requested Party so that they can apply grounds for refusal, if necessary, and instruct the service provider not to disclose the subscriber information in such cases.**
>
> Article 7.5.b. Whether or not a Party requires notification under paragraph 5.a, it may require the service provider to consult the Party's authorities in identified circumstances prior to disclosure. **In cases where the requested Party does not require notification under paragraph 5.a, it must require consultation of the Party's authorities by the service provider.**
>
> 108. Under paragraph 5.b, a Party may also, under its domestic law, require a service provider that receives an order from another Party to consult with it in identified circumstances. ~~A Party may not require consultation for all orders, which would add an additional step that could cause significant delay, but only in more limited, identified circumstances. Consultation requirements should be limited to circumstances in which there is heightened potential for the need to impose a condition or to invoke a ground for refusal or a concern of potential prejudice to the transferring Party's criminal investigations or proceedings.~~ **If a Party does not require notification by the requesting Party, it must require consultation by the service provider. The purpose is to ensure that domestic authorities are always aware of production orders issued on its territory, so that conditions or grounds for refusal can be applied in the same way as for production orders issued through mutual legal assistance instruments (including Article 8 of the Additional Protocol).**
>
> ~~109. The notification and consultation procedures are entirely discretionary. A Party is not obligated to require either procedure.~~

Article 7 requests can be issued without specifying any factual context or explaining the relevance of the request. Specifically, no information is provided regarding factual background of the investigation or regarding any grounds establishing investigative relevance and necessity.[19]

In order for a Party to invoke grounds for refusal in order to avoid disclosures that are contrary to fundamental rights, Parties must have sufficient supporting information to assess the legality of requests. Specifically, the order should contain enough information with regards to the relevance and necessity of the subscriber data sought. While paragraph 7.5.d allows Parties to request additional information if a particular request is subject to an obligation to notify or consult, as per

[19] Explanatory Memorandum, paragraph 104: "No statement of facts is required, taking into account that this information is confidential inmost criminal investigations and may not be disclosed to a private party."

paragraphs 7.5.a or 7.5.b, if the underlying requests lack detailed baseline information regarding the background of the request, it will be difficult if not impossible to identify the types of circumstances that require more detailed information.

Article 7 must therefore be modified to ensure that requesting parties provide sufficient information to either the service provider or to requested Party's authorities through notification.

Recommendation 6: Subscriber data requests must be provide enough factual context and explanation of investigative relevance if subscriber data requests are to be properly assessed for their impact on fundamental rights.

Article 7.4. The order under paragraph 1 shall be accompanied by the following ~~**supplemental**~~ **supporting** information:

a. the domestic legal grounds that empower the authority to issue the order;

b. a reference to legal provisions and applicable penalties for the offence being investigated or prosecuted;

c. a summary of the facts related to the investigation or proceeding;

d. the relevance of the subscriber information or data to the investigation or proceeding;

e~~c~~. the contact information of the authority to which the service provider shall return the subscriber information, from which it can request further information, or to which it shall otherwise respond;

…

104. ~~No statement of facts is required, taking into account that this information is confidential in most criminal investigations and may not be disclosed to a private party.~~ **Requesting parties that wish to keep relevant facts confidential from private parties should rely on Article 8 or provide the information to the Requested Party's authorities through notification if a declaration for notification under paragraph 5.a has been made.**

Under paragraph 7.2.b, Parties may require judicial or prosecutorial supervision of qualifying foreign law enforcement requests. However, parties cannot require prior independent judicial approval of qualifying foreign requests. No justification is provided for why Parties are refused this option. Parties should be able to require independent judicial authorization for qualifying requests under Article 7.

It is also important that Article 7 does not mischaracterize prosecutors as independent judicial authorities. While prosecutorial supervision can provide a measure of restraint on police powers, it is inaccurate to characterize them as independent in any judicial sense.

> **Recommendation 7: Allow parties to require independent judicial authorization for qualifying requests for subscriber data.**
>
> Article 7.2.b. At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, a Party may – with respect to orders issued to service providers in its territory – make the following declaration: ~~"The order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision"~~ **"The order under Article 7, paragraph 1, must be issued by an independent judicial authority"**.

Invoking paragraph 7.2.b is also currently optional. The Protocol must establish independent judicial authorization as a minimum threshold for cross-border access to subscriber data. This is an intrusive power, and individual officers in policing forces across the world cannot be empowered to identify anonymous Internet conduct at their sole discretion and without any supervision at all.

Judicial authorisation would be commensurate with the frequently sensitive nature of subscriber data as well as with the greater threat to fundamental rights posed by cross-border investigative contexts. Paragraph 7.2.b should not remain optional.

> **Recommendation 8: Obligate independent supervision of cross-border subscriber data requests.**
>
> Article 7.2.b. **[**~~At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, a Party may – with respect to orders issued to service providers in its territory – make the following declaration: "The order~~ **Orders** under Article 7, paragraph 1, must be issued by~~, or under the supervision of, a prosecutor or other~~ **an independent** judicial authority~~, or otherwise be issued under independent supervision"~~. **]**

Section 2. Joint Investigative Teams

Article 12 allows law enforcement agencies to establish informal and ad hoc arrangements for intrusive cross-border investigative conduct. Supervision of this conduct is left largely to local policing forces.

Article 12 contemplates law enforcement use of highly intrusive investigative techniques in other jurisdictions, including potentially the use of offensive attacks such as disruption of communications networks.[20] The Article lacks sufficient safeguards to ensure these techniques do not violate the laws of the jurisdictions in which they are undertaken. Joint Investigative Teams will frequently comprise policing agencies from numerous countries with a wide array of investigative powers and standards.[21] There is no international consensus over what constitutes an intrusive power and what minimum safeguards are commensurate with the resulting privacy and other human rights interferences. Rather than attempting to provide such a basis, the Protocol effectively normalizes an approach where any policing agency's powers prevail, regardless of the consequences.

By failing to provide minimum standards or a meaningful replacement for the mutual legal assistance framework it would displace, Article 12 also encourages forum shopping. In a joint team comprising multiple policing forces, the incentive will be to rely on the agency with the most permissive investigative powers in each given instance. As Article 12 places no meaningful restrictions on data transfers between agencies and jurisdictions, the investigative team can jointly accumulate private data by the most intrusive means available. In a global investigation, if one policing agency is specifically empowered to carry out network infiltration and interception activities, it can be tasked with forced access on behalf of the collective investigative team. If another single policing agency on a team can access subscriber data in bulk or historical location data without judicial authorization, it can become the team's point of collection for any multi-jurisdictional service providers. Under Article 12, the products of this collective investigative effort can purportedly be shared with all participating agencies.[22]

Article 12 is also intended to operate between Protocol signatories who have no other existing arrangements in place for mutual assistance. Typically, the absence of a pre-existing arrangement signals a number of heightened human rights risk factors that can include a lack of familiarity with implicated legal systems due to infrequent interaction, or an inability to form agreements due to irreconcilable disagreements over core human rights standards. It is

[20] https://www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft. See also recent problematic proposals to Brazil's Criminal Law: https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/.

[21] https://www.eurojust.europa.eu/coordinated-action-cuts-access-vpn-service-used-ransomware-groups.

[22] This may well include deeply sensitive private communications, typically accorded the highest level of protection at law: https://www.eurojust.europa.eu/ar2020/7-casework-crime-type/72-encrochat-dismantling-encrypted-network-used-criminal-groups;

therefore especially concerning that the joint investigations Article 12 envisions that Parties can operate with even less safeguards than those typically in place where formal bilateral arrangements govern joint cross-border investigations. Far from attempting to address this anticipated disparity in human rights and privacy standards, Article 12 instead adopts far fewer safeguards than its European-focused counterpart encoded in Article 20 of ETS 182.

2.1. JIT Agreements Cannot Supplant the Protocol's Central Safeguards.

Article 12's framework is triggered by an agreement entered into by competent authorities (including frontline law enforcement officials) on behalf of the transferring and of the receiving signatory Parties participating in the joint investigative team.

The bulk of the Protocol's data protection safeguards are concentrated in Article 14. Yet paragraph 14.1.c permits Parties to ignore any or all of the specific protections encoded in Article 14 by mutual agreement.

The combined effect of Article 12 and paragraph 14.1.c is that frontline officers may ignore the core protective elements of the Protocol simply by agreeing to when establishing a joint investigative team. Given the ad-hoc nature of some joint investigative teams (including teams established on a case-by-case basis under paragraph 12.7), Article 12 therefore provides a lawful basis in treaty for wide-ranging use of intrusive cross-border powers with few meaningful safeguards. We find this particularly disturbing as paragraph 12.5 authorizes law enforcement agencies to bypass formalized MLAT arrangements already in place for specific investigative tasks.

Article 12 must be amended to ensure that mutual agreements described in paragraphs 12.1 and 12.7 cannot supersede the Protocol's central safeguards. We note that doing so will not prevent the formation of joint investigative teams that fail to respect the detailed data protections encoded in paragraphs 14.2–14.15. It simply means that investigative teams that do not respect paragraphs 14.2-14.15 will need to find lawful authorization for their joint evidence gathering and sharing initiatives outside of the auspices of Article 12.

> **Recommendation 9: Prevent joint investigation team agreements from bypassing the Protocol's core safeguards.**
>
> Article 12**.8 An agreement described in paragraphs 1 and 7 does not qualify as a mutual agreement or arrangement under sub-paragraphs 14.1.b or 14.1.c.**

2.2. Article 12 Cannot Authorize Open-Ended Joint Investigative Mandates.

Article 12 provides no obligation to limit the operation of joint investigative teams in scope, size or purpose.

While it is appropriate to provide some investigative teams with some measure of flexibility, Article 12 must place some limits. Otherwise it may be relied upon to establish investigative teams that are effectively permanent in mandate and limited by investigative subject matter rather than by the parameters of a specific crime.

The open-ended nature of the investigative mandate adopted by Article 12 is particularly concerning given the wide disparities in law enforcement regimes that are anticipated to join the Protocol. On the other hand, it is unclear why the parameter limitations adopted in ETS 182 for European investigative teams would impede investigative teams conducted under the auspices of the Protocol.

We therefore strongly recommend that Article 12 adopt the limiting parameters employed by Article 20 of ETS 182 so that investigative authority groups are clearly delimited in terms of both purpose and time.

> **Recommendation 10: Prevent open-ended JITs of unlimited mandate.**
>
> Article 12.1. By mutual agreement, the competent authorities of two or more Parties may establish and operate a joint investigation team in their territories to facilitate criminal investigations or proceedings, **for a specific purpose and a limited period, which may be extended by mutual consent. A joint investigation team may be established** ~~where enhanced coordination is deemed to be of particular utility~~**:**
>
> **a. where any Party's investigation into criminal offences require difficult and demanding investigations having links with other Parties; or**
>
> **b. where a number of Parties are conducting investigations into criminal offences in which the circumstance of the case necessitate co-ordinated, concerted action in the Parties involved**.
>
> The competent authorities shall be determined by the respective Parties concerned.

2.3. Respecting local laws & fundamental values.

Article 12 allows frontline law enforcement officers to unilaterally establish joint investigative

teams and to fully determine all parameters and safeguards that will guide investigative techniques and evidence transfers authorized by those teams. Oversight by a central authority is an essential minimum requirement to ensure mutual assistance mechanisms are aligned with respect for fundamental rights.

Agreements may also be informal. As a result, investigative teams can be established on an ad-hoc basis. Moreover, paragraph 12.5 permits investigative assistance mechanisms to bypass existing MLAT arrangements, which typically assign a 'Central Authority' to vet individual assistance requests and ensure these do not violate human rights and other vital considerations.[23] Unless such a requirement is added to a specific JIT agreement, this vetting will simply not occur.

Central Authorities must therefore at the least approve each agreement that forms the basis for a joint investigation team. Paragraph 12.3 currently allows Parties to require central authority concurrence in any agreement. This approach allows frontline agencies to establish the basic parameters of an investigative team, but compelling approval from the central authority. Currently, paragraph 12.3 is optional. We believe that at minimum, this concurrence requirement must be mandatory.

> **Recommendation 11: Require Central Authority approval of JIT agreements.**
>
> Article 12.3. A Party**'s** ~~may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval that its~~ central authority must be a signatory to or otherwise concur in the agreement establishing the team.

Additionally, we are concerned with the broad latitude that Article 12.5 provides to joint teams in terms of initiating cross-border investigative techniques and transferring the investigative outcomes of those techniques between countries.

First and foremost, Article 12 of the Protocol does not prevent members of an investigative team from interfering with the sovereignty and laws of other States involved in the investigative team. This is particularly concerning in light of the nature of digital evidence. Article 12 does nothing, for example, to prevent a member of an investigative team from forcefully intruding into network infrastructure of a service provider located where another member of the team operates, with

[23] Paragraph 27.1 of the Cybercrime Convention (CETS 185) requires the appointment of a central authority "responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution" if a central authority is not already appointed by a Party under an existing mutual assistance treaty. See also paragraph 3.2 of the draft Protocol.

insufficient safeguards in place to ensure the sovereignty and even the national laws of the country in question are not violated.[24]

Investigative steps taken in a jurisdiction represented by a member of the investigative team must be taken by that member and in accordance with that jurisdiction's national laws. This approach is in stark contrast to Article 20 of ETS 182,[25] which expressly ensures that local authorities lead on local investigative operations. No justification for this departure has been provided.

> **Recommendation 12: Ensure investigative steps respect territorial sovereignty and national laws.**
>
> Article 12.5. Where investigative measures need to be taken in the territory of one of the Parties concerned~~,~~ **those investigative measures:**
>
> **a.** **will be taken by** participating **competent** authorities from that Party**;**
>
> **b.** may ~~request their own authorities to take those measures~~ **be taken** without the other Parties having to submit a request for mutual assistance~~.~~**; and**
>
> **c.** **in all circumstances** ~~Those measures~~ shall be carried out ~~by that Party's authorities in its territory~~ under the conditions **and in accordance with the laws** that apply under domestic law in a national investigation.

2.4. Avoiding forum shopping.

Article 12 incentivizes members of the investigative team to select investigative techniques with the fewest safeguards.

Electronic evidence is frequently controlled by multinational companies and stored in multiple jurisdictions. The Convention encodes a robust principle of territoriality, and early guidance from T-CY emphasized that requesting personal data from a multinational company will generally require a mutual assistance request if that data is physically located in another jurisdiction.[26] However, T-CY's more recent guidance has sought to erode this principle of territoriality, suggesting instead that states have jurisdiction over any personal data within the general control

[24] While Article 12.5 does affirm that law enforcement agencies cannot exceed lawful authority granted to them by their domestic law when seeking to undertake investigative measures in other territories, these agencies are under no obligation to respect the laws of the territory in which those investigative measures are undertaken (see Explanatory Memorandum, paragraph 212).

[25] See paragraphs 20.3.b, 20.6 and 20.7

[26] Cybercrime Convention, Article 32; T-CY Guidance Note GN #3.

of a multinational company offering services within its territory.[27]

Under T-CY's more expansive definition of territoriality, multiple participants in a joint investigation team will be able to access the same personal data from the same multinational company, incentivizing these teams to rely on investigative paths with fewer safeguards and leading to an overall erosion of privacy.

As joint investigative teams are also empowered to transfer obtained evidence between participants, the dedicated access regimes adopted in Articles 6 – 10 of the Protocol may also be bypassed by tasking those authorities with direct access to the multinational in question with any investigative measures that would otherwise require reliance on those Articles.

This capacity for forum shopping is a major flaw in the nature of joint investigative teams. We ask that the explanatory text be amended to preclude forum shopping and to confirm that Articles 6-10 are otherwise respected when investigative teams seek to access information otherwise covered by those articles.

> **Recommendation 13: Prevent JITs from forum shopping techniques to avoid privacy safeguards.**
>
> The explanatory text must be amended to preclude joint investigative teams from choosing the investigative path of least privacy resistance when gathering evidence from multinational companies. The explanatory text must in particular confirm that Articles 6-10 of the Protocol must be respected by participants in joint investigation teams.

Section 3. Mitigate Secrecy Provisions

Several of the investigative powers authorized by the Protocol include confidentiality provisions.[28]

While some measure of investigative confidentiality is certainly required, secrecy provisions can also shield problematic investigations into journalists, politicians, whistleblowers or political dissidents.[29] This risk is particularly heightened where the judiciary is not engaged, and even more so in cross-border contexts. Currently, confidentiality provisions are imposed largely at the

[27] T-CY Guidance Not GN #10, https://rm.coe.int/16806f943e.

[28] See Articles 6.3.d, 7.4, 8.8, 9.3.g, 11.2.b, 12.2, 14.11.c, and 14.12.a.i (paras 272-273).

[29] https://www.nytimes.com/2021/06/11/technology/apple-google-leak-investigation-data-requests.html.

discretion of a requesting Party and it is largely at the discretion a responding Party to determine whether to respect a request or demand.

Investigative secrecy and confidentiality should not be discretionary in cross-border contexts, and should only be permitted where revealing particular details threatens to compromise an ongoing investigation or where necessary to protect the rights and freedoms of others.

We suggest that the Protocol be amended to confirm that confidentiality provisions should only be invoked where doing so is strictly necessary to achieve an important objective of general public interest or to protect the rights and freedoms of others.

Recommendation 14: Ensure investigative confidentiality conditions are not abused.

Article **13b – Confidentiality**

Where a Party requests confidentiality in the exercise of any power or procedure provided for in this Protocol, it shall only do so to the extent and duration that it is strictly necessary to achieve important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned or to protect the rights and freedoms of others and only in manner consistent with the adequate protection of fundamental human rights and liberties, and with the principle of proportionality.

~~71~~**287**. ~~Finally, a~~ **A** number of provisions of Chapter II and elsewhere in the Protocol permit the imposition of **confidentiality restriction** ~~use limitations or conditions, such as confidentiality. When, I~~ **In** accordance with the provisions of this Protocol, receipt of the evidence or information sought ~~is~~ **can only be** subject to such a **confidentiality restriction "to the extent that it is strictly necessary to achieve important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned or to to protect the rights and freedoms of others"** ~~use limitation or condition, exceptions were recognised by the negotiators and are implicit in the text~~. **The rights and freedoms of others may, for instance, include the privacy of other individuals whose personal data would be revealed in the event access is granted. Important objectives of general public interest may, for instance, include the protection of national security and public safety (for example, information on potential terrorist threats or serious risks to law enforcement officials); and the prevention, detection, investigation or prosecution of criminal offences (for example, where disclosure would threaten the integrity of an ongoing investigation, official inquiry or proceeding).**

288. Finally, additional exceptions to confidentiality have been recognised by the negotiators and are implicit in the text. First, as a measure for protecting human rights and liberties in

accordance with Article 13, under the fundamental legal principles of many States, if material furnished to the receiving Party is considered by it to be exculpatory to an accused person, it must be disclosed to the defence or a judicial authority. This principle is without prejudice to the text of Article 12, paragraph 6.b, and Explanatory Report, paragraph 215 that may be applied where Parties have established a joint investigation team. It was understood by the drafters that, in such cases, the receiving Party would notify the transferring Party prior to disclosure and, if so requested, consult with the transferring Party. …

Recommendation 15: Ensure individual access rights are not unduly limited.

Article 14.12.a.1 … access in a particular case may be subject to the application of proportionate restrictions permitted under its domestic legal framework, needed, at the time of adjudication, to protect the rights and freedoms of others or **strictly necessary to achieve** important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned;

272. The ability to obtain such access in a particular case may be subject to proportionate restrictions permitted under a Party's domestic legal framework, "needed at the time of adjudication, to protect the rights and freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned." … Important objectives of general public interest may, for instance, include the protection of national security and public safety (for example, information on potential terrorist threats or serious risks to law enforcement officials); **and** the prevention, detection, investigation or prosecution of criminal offences **(for example, where disclosure would threaten the integrity of an ongoing investigation, official inquiry or proceeding)**~~; and avoiding prejudice to official inquiries, investigations and proceedings~~.

Section 4. Data Protection Safeguards

The inclusion of data protection safeguards in the Protocol is a welcome addition. Regrettably, we are concerned that Article 14 as drafted effectively operates to undermine rather than enhance privacy and data protection, in particular measures aimed at ensuring the continuity of a high level of data protection when personal data is transferred to other States. In particular, Article 14 allows Parties to bypass its core safeguards, undermining its utility and standing in stark contrast to the mandatory nature of the Protocol's lawful access obligations.

One of the most problematic aspects of the Protocol and its underlying Convention has been that it mandates specific lawful access obligations while requiring human rights and privacy safeguards in only a general sense, to be determined by national law in each of its diverse

signatories. To some degree, paragraphs 14.2 – 14.15 of the Protocol address this shortcoming by harmonizing specific data protection obligations for Parties.[30] However, these provisions do not ensure a level of data protection which is consistent with modern data protection instruments such as Convention 108/108+. This is highly problematic as the draft Protocol includes provisions for international transfers of personal data on a systematic scale, including between private service providers and law enforcement authorities in Parties that have not ratified Convention 108/108+.

Under paragraphs 14.1.b and 14.1.c, Parties can bypass the already limited protections encoded in paragraphs 14.2 - 14.15 by entering into agreements. The Protocol places no requirements regarding the adequacy of protections included in these agreements or the minimum standards of protection such agreements should include. Paragraph 14.1.b requires an international agreement that is 'comprehensive' in nature. But any agreement that applies the national data protection laws of the two Parties in question to transfers governed by the Protocol qualifies, even if the substantive protections themselves fall far short of those outlined in paragraphs 14.2 – 14.15.[31] Under paragraph 14.1.c, agreements do not need to be binding, comprehensive or even public. A secret informal arrangement with no meaningful safeguards at all could seemingly qualify. Even where transfers between two Parties occur under a public binding agreement, paragraph 14.1.c can be invoked on an ad hoc basis to secretly exempt specific investigative measures from specific safeguards.

By contrast, few of the Protocol's lawful access obligations are optional, and most of those that are may only be reserved under very limited conditions (e.g. Article 7, see our section 1 above). No rationale is provided for this asymmetry other than the desire to maintain flexibility for law enforcement.[32] We find this asymmetry deeply problematic and an indication of the Protocol's general willingness to disregard privacy and human rights in favour of investigative convenience.

[30] For some examples, see: Katitza Rodriguez & Tamir Israel, "Global Law Enforcement Convention Weakens Privacy & Human Rights", *Electronic Frontier Foundation*, June 8, 2021, https://www.eff.org/deeplinks/2021/06/global-law-enforcement-convention-weakens-privacy-human-rights.

[31] Explanatory Memorandum, paragraph 222: "In this context, a framework would generally be considered as being "comprehensive" where it comprehensively covers the data protection aspects of the data transfers." Indeed, the explanatory memorandum relies on an example agreement (the so-called 'Umbrella' agreement between the United States and the European Union) as a paradigmatic example of a qualifying agreement (paragraph 222). But the Umbrella agreement has been questioned for its compliance with the European Union Charter of Fundamental Rights: Douwe Kourff, "EU-US Umbrella Data Protection Agreement: Detailed Analysis", October 14, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/.

[32] Explanatory Memorandum, paragraph 223: "This ensures that Parties retain flexibility in determining the data protection safeguards that apply to transfers between them under the Protocol. In order to provide for legal certainty and transparency for individuals and for the providers and entities involved in data transfers pursuant to measures in Chapter 2, Section II of this Protocol, the Parties are encouraged to clearly communicate to the public their mutual determination that such an agreement or arrangement governs the data protection aspects of personal data transfers between them."

Paragraph 14.1.c is particularly troubling for its ability to exclude safeguards on an ad hoc basis, inviting agreements based on pure investigative expediency.

Recommendation 16: Prevent Parties from bypassing data protection safeguards

Remove paragraphs 14.1.b and 14.1.c.

We are further concerned that paragraph 14.1.d inappropriately undermines the role and powers of data protection authorities of signatories. Paragraph 14.d deems that the safeguards set out in Article 14 are sufficient for any restrictions on law enforcement-initiated transfers established in national law, and that no other approval can be required as a condition of facilitating such transfers. This effectively provides a legal basis for international transfers of personal data to any State which is Party to the draft Protocol, even when the transfer could circumvent existing data protection provisions in domestic law under e.g. the GDPR or Convention 108/108+.

Paragraph 14.15 further states that transfers to a given Party may only be suspended if there is substantial evidence of systematic or material facial breach of those safeguards. This risks unduly restraining the powers of data protection authorities in some jurisdictions, in particular in the European Union, from fulfilling their obligation under national law to exercise their supervision and enforcement powers so as to ensure that data protection standards are not undermined through international transfers—jurisdiction confirmed by the Court of Justice of the European Union in Case C-362/14 and Case C-311/18 (Schrems I & II).

Recommendation 17: Do not usurp data protection authority's supervision and enforcement role with respect to cross-border transfers

Remove paragraphs 14.1.d. and 14.15.

We are further concerned that paragraph 14.1.d specifically prohibits Parties from imposing any privacy safeguards beyond those recognized in Article 14 when processing requests made under the Protocol by other Parties.[33] For these privacy safeguards to be meaningful, they must establish a minimum level of protection, not a ceiling.

[33] Explanatory Memorandum, paras 225-226: "…paragraph 1.e. is not intended to permit Parties to impose additional data protection requirements for data transfers under the Protocol beyond those specifically allowed in this article."

Recommendation 18: Data protection standards must establish a minimum level of protection

Article14.e. Nothing in this article shall prevent a Party from applying stronger safeguards ~~to the processing by its own authorities~~ **for the protection** of personal data received **or transferred** under this Protocol.

Additionally, as noted above, the substantive protections encoded in paragraphs 14.2 – 14.15 do not meet modern privacy and data protection standards. As a result, Parties should be permitted to reserve some of the Protocol's most intrusive powers with respect to Parties that have not ratified Convention 108+ (CETS 223).

Recommendation 19: Parties should be able to reserve the Protocol's most intrusive powers with respect to any other Party that has not ratified Convention 108+

Article 14.**f At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may reserve the right not to apply Article 6 and Article 7 to Parties which have not ratified Convention 108+ (CETS No. 223).**

Finally, as we and others have noted on several occasions, the drafting process for this Protocol was significantly deficient to date and failed to incorporate meaningful participation from external stakeholders including, notably, civil society groups and independent regulators.[34]

These deficiencies cannot carry forward into the implementation and review mechanisms of the draft Protocol should it be adopted. Currently, Article 23 of the draft Protocol incorporates mechanisms for ongoing consultation on its provisions and their implementation, adoption of Guidance Notes, and the ability to review the impact of declarations and reservations. Article 21 outlines the process for future amendments to the Protocol.

While the Council's European Committee on Crime Problems (CDPC) must be kept informed of such consultations and amendments,[35] no measures are taken to ensure involvement from data protection authorities or even from the Council's own data protection committee (T-PD).

Formalizing the need for input from independent and external data protection and privacy

[34] See: https://www.eff.org/deeplinks/2018/03/nearly-100-public-interest-organizations-urge-council-europe-ensure-high; https://edri.org/our-work/new-cybercrime-protocol-weak-safeguards-against-big-risks-of-abuse/ ; https://edpb.europa.eu/sites/default/files/files/file1/statement022021onbudapestconventionnewprovisions_en.pdf; https://rm.coe.int/0900001680a26108; https://rm.coe.int/opinion-of-the-committee-of-convention-108-on-the-draft-second-additio/1680a26489.

[35] Paragraphs 21.2 and 23.1; Budapest Convention on Cybercrime, CETS 185, paragraph 46.2.

authorities in particular is vital to ensuring that the draft Protocol is implemented in a manner that respects human rights.

Recommendation 20: Prevent data protection authorities and committees from being locked out of consultations regarding the implementation of the draft Protocol

Article 21.2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC) **and the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD)**, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC **and T-PD** and, following consultation with the Parties to the Convention, may adopt the amendment.

Article 23.

3. **The T-PD shall be included in any consultations that occur further to this Article.**

~~3~~**4**. The review of Article 14 shall commence once ten Parties to the Convention have expressed their consent to be bound by this Protocol. **Independent oversight authorities, including data protection authorities and independent experts shall participate in this review.**

322. ... In view of the relevant expertise necessary for the assessment of the use and implementation of some of the provisions of this Protocol, including on Article 14 on data protection, **the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) must be consulted and** Parties ~~may~~ **should also** consider involving **independent oversight authorities, including data protection authorities, as well as** their subject-matter experts in the assessments.

...

324. Given the relevance of the data protection safeguards contained in Article 14, the drafters considered that this article should be assessed as soon as there is a sufficient record of co-operation under this Protocol to effectively review Parties' use and implementation of this provision. Paragraph 3, therefore, provides that the assessment of this article shall commence once ten Parties to the Convention have expressed their consent to be bound by this Protocol. **This review shall verify the implementation of data protection measures provided for in this Protocol and that the domestic law of assessed Parties provides for the adequate protection of human rights and liberties as established in Article 13. Reviews under**

Paragraph 3 will be conducted with the participation of independent oversight authorities, including data protection authorities and independent subject-matter experts, and the outcome of these reviews shall be made public.

FIN.