Testimony and Statement of Record of

Katitza Rodriguez Pereda
Electronic Frontier Foundation
Policy Director for Global Privacy

Hearing on

Draft Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence

Before the

Committee on Legal Affairs and Human Rights
Parliamentary Assembly
Council of Europe

Rapporteur: Mr Kamal Jafarov, Azerbaijan, EC/DA

September 14, 2021

STATEMENT

I appreciate the opportunity to appear before the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe. My name is Katitza Rodriguez, I'm EFF Policy Director for Global Privacy, and I have studied and advocated for privacy and data protection policy principles since 2002, more than 19 years ago, eleven in EFF. Before joining EFF, I was director of the international privacy program at the Electronic Privacy Information Center in Washington D.C., where amongst other things, I worked on The Privacy and Human Rights Report, an international survey of privacy laws and developments in more than 60 countries. I have also acted as a liaison of the Civil Society Information Society Advisory Council at the Organisation for Economic Co-operation and Development from 2008 to 2010, and I sit in the Multi-stakeholder Advisory group of the Internet Governance Forum. In 2018, CNET named me one of the 20 most influential Latinos in technology in the United States. In 2014, I was also named one of "The heroes in the fight to save the Internet".

I would like to extend my thanks to the PACE Committee Members and to the organizers of this hearing, for cultivating a fruitful exchange of ideas on issues related to international cooperation in combating cybercrime, specifically in the context of the Second Additional Protocol to the Budapest Convention. EFF is particularly grateful for the opportunity to share our and our colleagues' analysis and recommendations to fix problems we've identified in the Protocol. These recommendations are set out in our written submission and a series of posts,[1] and I'm happy to share today a few of our specific concerns.

At the highest level, the current Protocol should establish clear and enforceable baseline safeguards in cross-border evidence gathering, but fails to do so. Though new police powers are mandatory, corresponding privacy protections are

[1] https://www.eff.org/deeplinks/2021/08/eff-council-europe-flawed-cross-border-police-surveillance-treaty-needs-fixing

frequently optional, and the Protocol repeatedly defers to national law or case-by-case agreements to define how people will be protected against abuses. Indeed, the Protocol openly avoids imposing strong harmonised safeguards in an active attempt to entice states with weaker human rights records to sign on. The result is a net dilution of privacy and human rights on a global scale. But the right to privacy is a universal right.

International law enforcement powers should come with detailed legal safeguards for privacy and data protection. When it comes to data protection, Convention 108+ should be the global reference. By its recommendations to the Council of Ministers, PACE has an opportunity to establish a commonly acceptable legal framework for international law enforcement that places privacy and human rights at its core.

1. Protecting Online Anonymity

Substantively, we have concerns regarding Article 7 of the Protocol, which permits direct access by law enforcement in one country to subscriber identity information held by a company in another country. In our opinion, Article 7 fails to provide, or excludes, critical safeguards contained in many national laws. For example, Article 7 does not include any explicit restrictions on targeting activities which implicate fundamental rights, such as freedom of expression or association, and prevents Parties from requiring foreign police to demonstrate that the subscriber data they seek will advance a criminal investigation.

We are particularly concerned that Article 7's explanatory text fails to acknowledge that subscriber data can be highly intrusive. Your IP address can tell authorities what websites you visit and what accounts you used. Police can also request the name and address associated with your IP address in order to link your identity to your online activity, and that can be used to learn deeply intimate aspects of your daily habits. Article 7's identification power undermines online anonymity in a context that embraces legal systems with widely divergent approaches to criminal justice, including some governments that are autocratic in nature. The resulting threat to journalists, human rights defenders, politicians,

political dissidents, whistleblowers and others is indefensible. The Pegasus scandal demonstrates that the government is willing to target civil society in this manner. This is why we've urged PACE to remove Article 7 entirely from the text of the Protocol. States would still be able to access subscriber data in cross-border contexts, but would instead rely on Article 8, which includes more safeguards for human rights. If Article 7 is retained, we've urged for additional minimum safeguards, such as:

- Ensuring that the explanatory text properly acknowledges that access to subscriber data can be highly intrusive.
- Providing Parties with the option, at least, of requiring prior judicial authorization for requests made under Article 7.
- Requiring Parties to establish a clear evidentiary basis for Article 7 requests.
- Ensuring that Article 7 requests provide enough factual background to assess compliance with human rights standards and protected privileges.
- Requiring notification or consultation with a responding state for all Article 7 demands.
- Requiring refusal of Article 7 requests when necessary to address lack of double criminality or protection of legal privileges.
- Providing the ability to reserve Article 7 in a more nuanced and timely manner.
- Ensuring that Article 7 demands include details regarding legal remedies for and obligations for service provider refusal.

2. Raising the Bar for Data Protection

When it comes to Article 14's data protection safeguards, we have asked that the Protocol be amended so that signatories may refuse to apply its most intrusive powers (Articles 7 and 12) when dealing with any other signatory that has not also ratified Convention 108+. We also hope the Parliamentary Assembly will support the Committee of Convention 108's mission, and remember that the Committee of Ministers supports making Convention 108 the global reference for data protection, including in the implementation of this Protocol. Article 14 itself

falls short of modern data protection requirements and, in some contexts, will actively undermine emerging international standards. Two examples:

- Fails to require independent oversight of law enforcement investigative activities. For example, many oversight functions can be exercised by government officials housed within the same agencies directing the investigations;
- Article 14 limits the situations in which biometric data can be considered 'sensitive and in need of additional protection despite a growing international consensus that biometric data is categorically sensitive.

But even with the weak standards contained in Article 14, signatories are explicitly permitted to bypass these safeguards through various mechanisms, none of which provide any assurance that adequate privacy protections will be in place. For example, any two or more signatories can enter into an international data protection agreement that will supersede the safeguards outlined in Article 14. The agreement does not need to provide a comparable or adequate level of protection to the default rules.

Signatories can even adopt less protective standards in secret agreements or arrangements and continue to rely on the Protocol's law enforcement powers. We have therefore recommended that the Protocol be amended to ensure a minimum threshold of data protection in Article 14, one which may be supplemented with more rigorous protections but cannot be replaced by weaker standards. This would also be done in a vein to avoid the fragmentation of privacy regimes.

3. Make Joint Investigative Team Limitations Explicit

Under Article 12, signatories can form joint investigative teams that can bypass core existing frameworks such as the MLAT regime when using highly intrusive cross-border investigative techniques or when transferring personal information between team members.

We have asked that the Protocol be amended so that some of its core intended limitations are made explicit. This is particularly important given that many teams may ultimately be operating with a higher level of informality and driven by police officers without input or supervision from other government bodies typically involved in overseeing cross-border investigations. Specifically, we have asked that the Protocol (or, alternatively, the explanatory text) clearly and unequivocally state that participants in a joint investigative team must no**t** take investigative measures within the territory of another participant in the team and that **no** participant may violate the laws of another participant of that team.

We also ask that the Protocol be amended so that Parties are obligated to involve their central authorities (and, preferably, the entity responsible for data protection oversight) in the formation and general operation of an investigative team, and that agreements governing investigative teams be made public except to the degree that doing so would threaten investigative secrecy or is necessary to achieve other important public interest objectives.

Those are my opening remarks. I thank you once again for providing us with an opportunity to present to you today, and I welcome your questions.

Question on Joint Investigative Teams*:* How do investigative measures taken by a JIT interact with the specific mechanisms in Articles 7-8 when these overlap? Where multiple members of a JIT can take an investigative measure (e.g. where we are dealing with multinational service providers) how do we ensure the most privacy and human rights-respective option is used?

***Question on procedural and data protection safeguards*: *Question on procedural and data protection safeguards*:** Does any Committee at the Council of Europe is planning to assess, on an ongoing basis, Parties' compliance with the Protocol's human rights and data protection safeguards obligations, and what's the role of the data protection committee on such type of assessment.?