Initial Observations of the Center for Democracy & Technology
on the provisional draft text of the
Second additional Protocol to the Budapest Convention on Cybercrime
November 8, 2019

The Center for Democracy & Technology (CDT) submits these initial observations on the Cybercrime Convention Committee (TC-Y) provisional draft Second Additional Protocol (Protocol) to the Budapest Cybercrime Convention. These observations are submitted in anticipation of the consultations to be conducted at the Octopus Conference November 20-22 in Strasbourg. As these are initial observations, we reserve the right to submit additional supplementary information at a later date. We believe the Protocol needs substantial improvement in order to protect the rights of the users whose data will be disclosed under it.

CDT is a non-profit civil society organization based in Washington, D.C. with an office in Brussels. As a public interest organization focused on privacy and other human rights issues affecting the Internet, other communications networks, and associated technologies, CDT represents the public's interest in an open Internet and promotes the democratic values of free expression, privacy and individual liberty. CDT has been heavily engaged on the issue of cross-border data demands, having issued, among other things, Ten Human Rights Criteria for Cross Border Data Demands, a brief in the cross border data demands US Supreme Court case, U.S. v. Microsoft, recommendations for improving the European Union's E-Evidence proposals in August of 2018, and observations submitted to this process in June of 2018.

We focus these initial observations on Protocol provisions four (4) and five (5) relating to, respectively, direct disclosure of subscriber information (Direct Disclosure Provision) and giving effect to orders from another Party for expedited production of data (Giving Effect Provision). The Direct Disclosure Provision would require countries that sign the Protocol to enact legislation as necessary, (i) to empower their authorities to issue orders for disclosure of subscriber information that could be *served directly on communications service providers* in other countries, and (ii) for service providers in their territory to disclose their users' subscriber information in response to orders coming from other signatories to the Protocol. The Giving Effect provision would require countries that sign the Protocol to enact legislation as necessary to (i) empower their authorities to issue orders *to authorities in other signatory countries* for the purpose of compelling disclosure of subscriber information and traffic data held by service providers in those signatory countries; and (ii) to give effect to orders for such disclosures submitted by signatories to the Protocol.

1401 K Street NW, Suite 200, Washington, DC 20005

Thus, the Direct Disclosure Provision relates to cross border disclosure orders for subscriber information that are issued directly to service providers in other Parties to the Protocol. The Giving Effect Provision relates to cross border disclosure orders for both subscriber and traffic information that are issued to the authorities of other Parties to the Protocol, which Parties are to "give effect" to such orders by compelling the service provider to disclose the subscriber and/or traffic data at issue. A Party can, at its option, "give effect" to a disclosure order issued by another Party by accepting it as equivalent to a domestic order, by endorsing it to give it the same effect as a domestic order, or by issuing its own production order.

Direct Disclosures Provision

The Direct Disclosures Provision will result in countries around the world issuing orders for disclosure of subscriber information directly on service providers who have a global user base. Under the Protocol, the orders need not always:

(i) Be issued an independent judicial authority;
(ii) Be issued only on a factual basis specified in the Protocol that establishes criminality and a strong link of the subscriber information sought to the crime being investigated;
(iii) Pertain to a serious crime, and to conduct that is criminal both in the country issuing the order and the country in which the order is received;
(iv) Be noticed to the country in which the service provider is located;
(v) Be noticed to the person who is the subject of the demand for subscriber information;
(vi) Contain facts adequate for a service provider to determine whether the order is properly issued and whether compliance would violate a person's human rights;
(vii) Be accompanied by a commitment to pay the costs of producing the subscriber information that is sought.

These are serious shortcomings that can and should be remedied, as indicated below.

Judicial authorization: Paragraph one of the Protocol permits signatory countries to require that orders for subscriber information, "…must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision." It seems unwise to leave something as important as requiring independent judicial authorization to the discretion of countries signing the protocol. They may be unaware of the vagaries of the systems in other Parties. Moreover, in at least some countries, "prosecutors" are not at all independent, as is implied by this language. Given the uncertainty that has been identified by others about the types of information that could constitute subscriber information subject to direct disclosure (including IP address information that is more properly categorized as traffic data than as subscriber information) a uniform judicial authorization rule seems warranted.

Factual basis: Instead of specifying the factual basis that must support issuing an order for subscriber information, the Protocol allows for such orders when they are "needed" for a criminal investigation. It assumes signatory countries in Europe will abide by the Necessary and Proportionate standard, and that other signatory countries will adopt their own relevance or other standards regarding the required factual basis, and that those standards will be adequate. Instead, the Protocol should specify the factual basis that must be met, as well as the required tie of the information sought to the crime being investigated.

Serious crimes: The Protocol seems to extend the ability to issue orders for compelled disclosure of subscriber information to all crimes, not just to serious crimes, such as those with a maximum term of imprisonment of three years or more. Adoption of the Protocol risks inundating service providers with orders to disclose subscriber information related to petty crimes, leaving them less able to respond quickly to orders to make disclosures in serious cases.

Dual criminality and country notice: The Protocol permits a country that, for example, makes blasphemy a crime, to issue an order for disclosure of subscriber information to prosecute that crime to a service provider in a country in which the blasphemy is protected free expression. This puts the free expression rights of people around the world at risk if they use a service provider with a global user base. Protocol provisions permitting Parties to require simultaneous notice to the Party in which a service provider is located of demands for subscriber information, and permitting Parties to require that a service provider consult with the Party's authorities in specified circumstances, may mitigate this problem somewhat, but a dual criminality requirement would go further. Paragraph 5.c. on country notice should be expanded to permit authorities in the receiving country to instruct a service provider in the receiving country not to disclose subscriber information any time such authority determines that disclosure would pose a serious risk to a person's human rights.

Individual notice: Instead of requiring individual notice, the Protocol allows the country issuing the order to gag the service provider that receives the disclosure order, and the gag need not be approved by a judicial authority based on a showing of need. This should be reversed: the Protocol should be amended so that user notice by service providers is permitted, but can be delayed for a set period of time based on a judicial finding that simultaneous notice would compromise an investigation or have other adverse impacts set forth in the Protocol. In addition, the issuing country should be required to give user notice as well, and such notice could be delayed based on the same criteria and findings as would apply to provider notice.

Facts given service providers: Many service providers have undertaken the responsibility to push back on data demands that would violate the rights of their users. This is conduct that should be encouraged. Providers should be given enough information about the factual basis for the order to push back when necessary to protect the rights of their users. Instead, the Protocol indicates that the service provider will receive only the name of the offense that is the

subject of the criminal investigation and other information that does not indicate the factual basis for the demand.

Compliance costs: To discourage subscriber information orders in minor cases, Parties issuing demands should be required to pay service providers' costs for complying with those demands.

Transparency: The Protocol should require that countries annually report the number of orders for subscriber information that they issue under the Protocol, the categories of crimes for which those orders are issued, the number of subscribers whose data is sought or obtained.

Giving Effect Provision

The Giving Effect Provision will result in compelled disclosure of both subscriber information, and the more sensitive traffic data, which, for example, includes email logs and browsing history. Because more sensitive data is at issue in the Giving Effect Provision, one would expect the protections afforded in it to reflect that sensitivity. Yet, the Giving Effect Provision suffers from many of the same defects as does the Direct Disclosure Provision.

Judicial authorization: Though traffic data may be the subject of the order, the Protocol does not require that either the order issued by the requesting Party, or the "giving effect" measure adopted by the requested Party, be approved by a judge or another independent decision maker. If the laws of both Parties authorize orders to compel disclosure of sensitive traffic data without judicial authorization, the Protocol will facilitate such violations of basic privacy rights. The Protocol should require judicial or other independent authorization for orders compelling disclosure of traffic data and of subscriber information, especially if such subscriber information includes IP address information that functions as traffic data. At a minimum, the law of the requested Party must impose this requirement.

Factual basis: As is the case with the Direct Disclosure Provision, the Giving Effect Provision of the Protocol does not specify the required factual basis for the issue of an order by the requesting country. It also does not specify the required factual basis for the issue of any legal process in the requested country to "give effect" to the order. The standard each country puts in place, however weak, will be the standard governing disclosure. Unlike the Direct Disclosure Provision, the Giving Effect Provision requires that the requesting country disclose a "summary of the facts related to the investigation" and the relevance to the investigation of the information sought. 5.1.3.b. However, the summary of the facts goes only to the requested country to facilitate its ability to give effect to the order it has received from the requesting country. The factual summary is not given the service provider. This will thwart the efforts of service providers to protect the rights of their users. In addition to this summary of facts, the requested country may require additional supporting information but must describe such information in advance.

As is the case with the Direct Disclosure Provision, the Giving Effect Provision does not require: that orders be issued only for investigation of serious crimes, dual criminality, the giving of notice of the disclosure to the user (which notice can be delayed), payment of compliance costs, nor transparency about the number and nature of the disclosures being compelled.

Conclusion

Unless substantially improved to protect the rights of internet users, adoption of the Protocol will result in more disclosures of traffic data and subscriber information that violate the privacy rights and interests of those users. We look forward to working on improvements to the Protocol to address these and other problems.

[For more information, contact CDT's Greg Nojeim, Director of the Freedom, Security and Technology Project, gnojeim@cdt.org]