**Cybercrime Convention Committee (T-CY)**
**Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime**
**Discussion Guide for consultations with civil society, data protection authorities and industry**
**Octopus Conference, 11-13 July 2018 Council of Europe, Strasbourg, France**

**CDT comments:**

The Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and other human rights issues affecting the Internet, other communications networks and associated technologies. With offices in Washington, D.C. and Brussels, CDT represents the public's interest in an open internet and promotes the democratic values of free expression, privacy and individual liberty. CDT submitted Comments on the European Commission Consultation on Improving Cross-Border Access to Electronic Evidence in Criminal Matters, assessed the European Commission's E-Evidence Proposals compliance with Human Rights, and submitted interventions in a number of cases at the European Court of Human Rights that raise surveillance and human rights issues that guide the Council of Europe's work, including in *Szabo and Vissy v. Hungary* (37138/14), *Big Brother Watch and Others v. the United Kingdom* (58170/13), and *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* (62322/14).

CDT welcomes the opportunity to contribute the observations below in support of the ongoing preparation of a 2nd Additional Protocol to the Budapest Convention. The advance of technology means that law enforcement entities investigating a crime in one county are increasingly seeking data held by a communications service provider in another country. CDT continues to urge that human rights considerations guide cross-border data demands, as discussed in our responses below.

**3.1 Context: Rationale for the Protocol – Recap and recent developments**

Access to electronic evidence for criminal investigations, especially across borders, has been a major theme for policy makers in recent years. Both law enforcement authorities, service providers holding data, and users of those services, have an interest in sensible policy solutions. CDT supports solutions that balance and consider the interests of all three sets of stakeholders.

The recently adopted US CLOUD Act (attached to omnibus spending bill H.R. 1625) and the European Commission's E-Evidence proposals are departures from the principle that location of data determines which country's law enforcement agencies can claim jurisdiction over that data.

The CLOUD Act grants U.S. law enforcement entities new powers to compel U.S. companies to disclose communications and data on U.S. and foreign users that are stored overseas. It also allows qualifying foreign governments to enter into an executive agreement to bypass

the MLAT process when seeking data in criminal investigations and to seek data directly from U.S. technology companies. The CLOUD Act does not adequately ensure human rights protection in these agreements. In certifying these bilateral agreements the bill requires that the Attorney General (AG) determine that "the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties." The factors the AG must consider in making this determination include whether the country prohibits torture, guarantees fair trials and prohibits arbitrary arrests, protects against wrongful interference with privacy, and protects free expression. However, given the political nature of determining a country is not human rights compliant, the AG may well certify a country in spite of such failings. Furthermore, the CLOUD Act does not clearly mandate judicial authorization for data requests, and permits certifications to last for five years, a timeframe during which it is foreseeable that a country's adherence to human rights principles may change.

The E-Evidence proposals require communications service providers to disclose data they hold on individuals, regardless of nationality, residence, or location, to an investigating authority in any EU Member State. The obligation applies to any provider regardless of the country in which its main establishment is located, as well as to providers with no establishment in the EU, if the provider's services can be used in the EU, and if the services are to some extent targeted to an EU Member State. The E-Evidence proposals require providers to nominate a representative in the EU who can receive and process production orders.

Both the E-evidence proposals and the CLOUD Act expand dramatically the ability for law enforcement authorities to access information about people across the world, for criminal investigations.

There is a clear need for expanded ability to access data to be bounded by strong privacy and procedural protections. In addition, it should be ensured that only countries with strong fundamental rights protections are able to benefit from agreements. Further, new legislative tools must include measures that prevent or mitigate conflicts of law that would compel providers to disclose data to one country's authorities that they are prohibited from disclosing by another country's laws.

It is sensible that the CoE's work on direct cooperation with providers in other jurisdictions is focused on subscriber information. Other categories of data, notably content and metadata, are far more sensitive and require a higher level of protection.

**3.2 Provisions for more efficient mutual legal assistance**

We are pleased with the Council of Europe's focus on making MLATs work more efficiently and effectively. MLATs are, and should remain, the preferred method for requesting data for law enforcement purposes held in other jurisdictions. While we recognise that MLATs may not always be able to scale with demand, and we are not opposed to other rights-respecting solutions, given the right safeguards, MLATs should not be replaced - de facto - by less solid

arrangements. We are conscious of legitimate concerns about their efficiency and the time it can take to process MLAT requests for data.

That is why CDT has supported efforts to improve the effectiveness and efficiency of MLATs. There are many steps authorities can take to make agreements work more efficiently. Among those steps are increased funding, training of officials, use of standardised electronic formats, etc. In the European Commission's work leading up to the publication of the E-Evidence proposals, many areas for improvement were identified. European Ministers of Justice have requested that efforts be undertaken to streamline MLA processes in a variety of ways. The need to enhance the functioning of MLATs is considerable and has been well documented. For example, already in 2014, CDT submitted, jointly with other organisations, a letter to Members of the US Congress on this matter.

**3.3 Direct cooperation with providers across jurisdictions - mandatory production orders**

As mentioned, both the US and the EU have taken and are taking legislative steps to facilitate direct cooperation with providers. These legislative steps are mandatory with respect to providers, and we focus our observations on these questions.

We have already discussed the CLOUD Act and the E-Evidence proposals above. The fact that they provide for compelled disclosure makes it essential that privacy and procedural safeguards are strong. These orders concern broad and very sensitive categories of data, and can be used to compel disclosure of data on anybody regardless of citizenship, residence, or location. They can be used for a very broad set of criminal investigations, and with very limited scope for review either by providers receiving production orders or by authorities of the country in which the provider is based. The proposals assume harmonised European standards for criminal justice and fundamental rights, and place a high level of confidence in the ability and willingness of the issuing authority to respect the principles of necessity and proportionality.

CDT published an initial analysis of the E-Evidence proposals, identified a number of areas for improvement, and measured the proposals against ten fundamental human rights principles. We commend those human rights principles to the CoE and urge that whatever proposals the CoE puts forward respecting mandatory production orders in a protocol to the Budapest Convention must ensure compliance of signatory countries with those principles. Our work on the E-Evidence proposals is still ongoing, and we will be submitting more detailed drafting recommendations to the European policy makers currently reviewing the proposals.