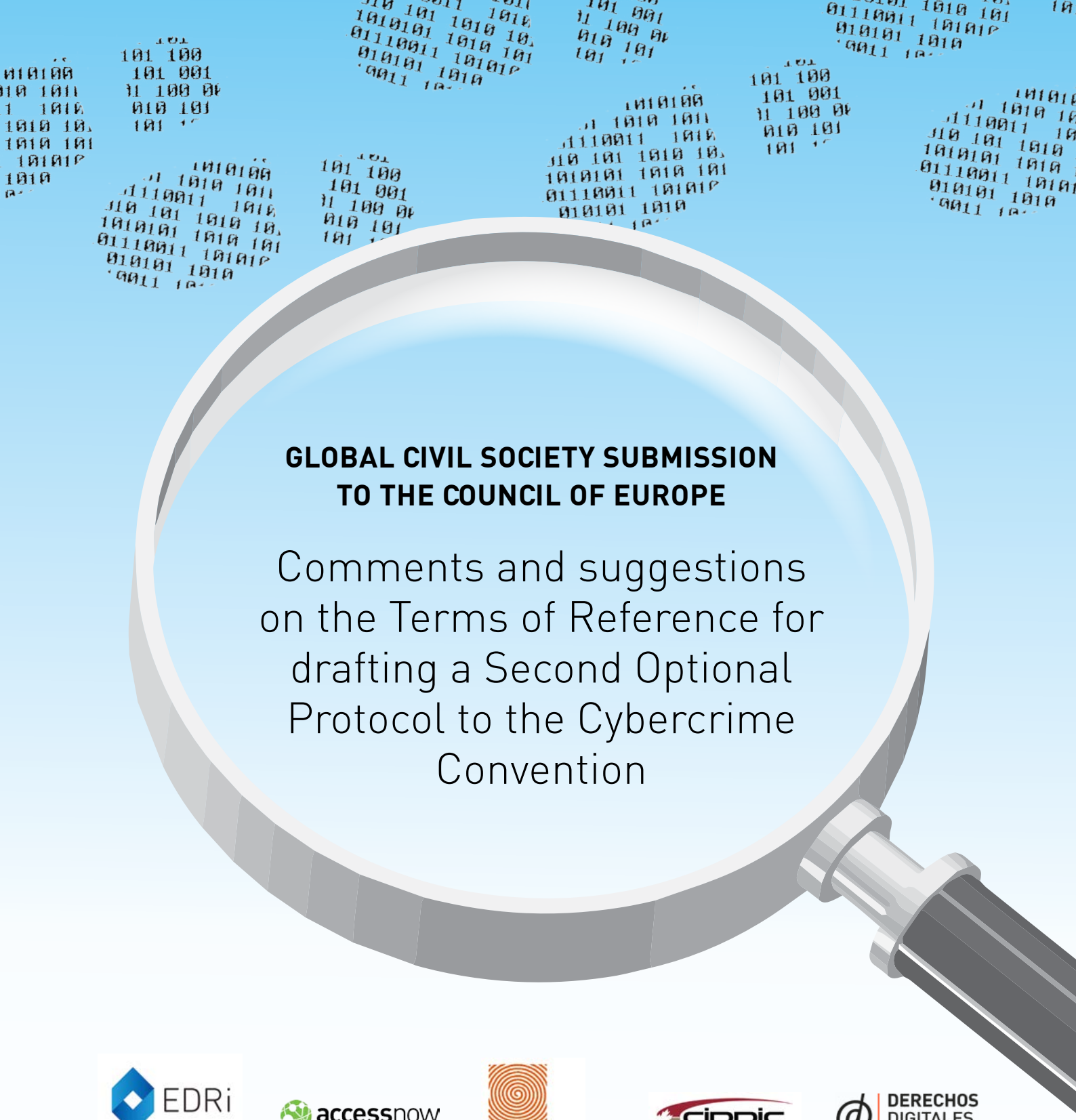

GLOBAL CIVIL SOCIETY SUBMISSION TO THE COUNCIL OF EUROPE

Comments and suggestions on the Terms of Reference for drafting a Second Optional Protocol to the Cybercrime Convention

EDRi
a coalition of 35 civil rights organisations

accessnow

Australian Privacy Foundation

cippic

DERECHOS DIGITALES América Latina

Digital Rights Ireland

ELECTRONIC FRONTIER FOUNDATION

epic.org

EPICENTER .WORKS for digital rights

IT-Politisk Forening www.itpol.dk

PRIVACY INTERNATIONAL

TEDIC

Xnet

We are a group of 14 civil society organisations from around the globe that fight for and defend human rights and fundamental freedoms online. We wish to engage with the Council of Europe throughout the drafting process, in order to support efforts to ensure that human rights are fully respected.

We are commenting on this process because of the human rights implications of cross-border access to electronic evidence. Electronic evidence ("e-evidence") refers to digital or electronic evidence, such as contents of social media, emails, messaging services or data held in the "cloud". Access to these data is often required in criminal investigations. Since geographical borders are often blurred in the digital environment, investigations require cross-border cooperation between public authorities, and between public authorities and the private sector.

Effective police investigations are important but requests for personal data across borders must comply with human rights protections. Electronic communications are subject to the protections that defend other spheres of personal lives, such as when law enforcement seeks access to homes. Access to personal data must be proportionate and necessary to the aim of a legitimate investigation and provided for by law.[1]

In view of the Terms of Reference for drafting a Second Optional Protocol to the Cybercrime Convention[2], we take this opportunity to submit comments and suggestions[3] in preparation for the first meeting of the Drafting Group on 19 and 20 September 2017.[4] It is vital that the new protocol include and respect three basic principles ("the basic principles"):

1. **Enforcement of jurisdiction by a State or State agency on the territory of another State cannot happen without the knowledge and agreement of the targeted State.**

2. **State-parties must comply with human rights principles and requirements, including under any powers granted or envisaged in or under the Cybercrime Convention and the proposed additional protocol.**

3. **Unjustified forced data localisation should be banned. Data transfers between jurisdictions should not occur in the absence of clear data protection standards.**

1 https://edri.org/access-to-e-evidence-inevitable-sacrifice-of-our-right-to-privacy/

2 Cybercrime Convention Committee, Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime – proposal prepared by the Cloud Evidence Group as well as Canada, France, Germany, Japan, Liechtenstein, Slovakia and USA for consideration by the T-CY, T-CY(2017)3, Strasbourg, 1 March 2017, approved by the 17th Plenary of the T-CY on 8 June 2017 https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b

3 This submission is built on expert input provided by Professor Douwe Korff.

4 https://rm.coe.int/t-cy-17-meeting-report-/168072366d

I. Working methods

We welcome the publication of relevant documents on the Council of Europe's website and the openness of Council of Europe's staff.

We urge the Cybercrime Convention Committee (T-CY) to provide transparency by, at a minimum, making the membership of the Drafting Group and the minutes of the Drafting group public. Due time should be given for public comment on relevant documents.

This means that the process should be inclusive, open, and built on consensus from all relevant stakeholder groups. We urge the T-CY to instruct the Drafting Group to consult broadly on the substance of the proposed new protocol, including with the Registry of the European Court of Human Rights, the Human Rights Directorate and the Data Protection Unit of the Council of Europe, the Council of Europe's Commissioner for Human Rights, the Parliamentary Assembly of the Council of Europe and civil society including the undersigned.

We urge that the Human Rights Directorate and the Data Protection Unit be asked to issue opinions on whether the final draft protocol meets the requirements of the European Convention on Human Rights (ECHR) and of the Convention on Data Protection (Convention No. 108); and that the draft protocol be submitted to the T-CY together with these opinions, for reflection and discussion, and amended in the light of those opinions and discussions.

II. Substantive work

Deficiencies and weaknesses in the Cybercrime Convention in facilitating law enforcement's access to data have become apparent in the changing technological, legal and political environment in the seventeen years since it was opened for signature. EDRi previously sent a letter to the Cloud evidence group outlining the following problems:[5]

- the lack of safeguards of the proposed measures, stemming partly from flaws in the Cybercrime Convention, with regard to non-Council of Europe countries, non-Convention 108 countries and free accession to that instrument;
- the repetition of the unexplained and unproven premise that MLATs cannot be reformed, which is used as a very thin justification for the far-reaching measures being proposed;
- the lack of solutions with regard to national measures by law enforcement authorities to circumvent the Cybercrime Convention and other parallel frameworks that can lead to human rights violations and fragmented rules and implementation;
- the lack of precision with regard to the scope of the term "subscriber data", which is open to broad interpretation, in a text that is supposed to provide a "common understanding" of the term;
- the rule of law implications of the "voluntary" arrangements under which US companies share - or do not share - data with law enforcement authorities, at their (the companies') discretion.

These deficiencies were not addressed in the report that led to the proposal for a new protocol that directed the drafting of the Terms of Reference.[6] However, as we are still at the beginning of the drafting process for the optional protocol, it is not too late for this acknowledgement and mitigation to still take place.

5 https://edri.org/files/surveillance/letter_coe_t-cy_accesstoe-evidence_cloud_20161110.pdf

6 See:
- https://edri.org/files/surveillance/letter_coe_t-cy_accesstoe-evidence_cloud_20161110.pdf
- https://edri.org/files/surveillance/korff_note_coereport_leaaccesstocloud%20data_final.pdf

For the Final Report of the CEG, criticised in the above, see: Cybercrime Convention Committee, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report of the T-CY Cloud Evidence Group, T-CY(2016)5-Provisional, Strasbourg, 16 September 2016, https://rm.coe.int/16806ab61a

The work should be done on the basis of the following basic principles:

1. **Enforcement of jurisdiction by a State or State agency on the territory of another State cannot happen without the knowledge and agreement of the targeted State.** State-parties should be barred from exercising "enforcement jurisdiction" including the carrying out of evidence-gathering, on the territory of another State – including through the Internet, in respect of ICT infrastructure or devices that are physically in another State – without the full knowledge and agreement of the targeted State.

2. **State-parties should not be permitted to use any authority, including any powers granted or envisaged in or under the Cybercrime Convention and the proposed additional protocol, in violation of their human rights obligations.** State-parties must be authorised and able to challenge any attempts or methods to seek information that are likely to involve or lead to violations of any fundamental rights of anyone, including notably as listed in the European Convention on Human Rights and the UN International Covenant on Civil and Political Rights. They will not be able to do so if they are not even aware of such attempts or methods.

   State-parties must comply with human rights principles and requirements, including under any powers granted or envisaged in or under the Cybercrime Convention and the proposed additional protocol,[7] including:

   - **Legality:** All measures that interfere with rights and freedoms of an individual must be prescribed by law. The law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the intrusion.

   - **Legitimate Aim:** Measures that interfere with rights and freedoms of an individual must achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

   - **Necessity:** All measures that interfere with rights and freedoms of an individual must be limited to those strictly and demonstrably necessary to achieve a legitimate aim. All less intrusive means to achieve the aim must have been exhausted or must manifestly be futile.

7 These principles are in line and sometimes use the wording of the Necessary and Proportionate Principles: https://necessaryandproportionate.org/

- **Competent Judicial Authority:** Prior to launching any measure that interferes with rights and freedoms of an individual, governments must make an application, demonstrating the necessity, including a high degree of probability that a serious crime or act(s) amounting to a specific, serious, threat to public order or national security, has been or will be carried out, or exists or is likely to arise, and that evidence relevant and material to the serious crime or act(s) will be obtained by the measure; and demonstrating proportionality, including minimisation procedures, of the method, extent, and duration, of the proposed measure. All measures taken by any State-party that interfere with the fundamental rights and freedoms of any individual within the jurisdiction of any State-party should be subject to Principle 1, above, and be authorised by or at least be under the effective and in principle control of, a judicial authority of the State where the individual in question is at the relevant time. By "judicial authority" we mean an official body separate and independent from the authorities conducting the investigation; conversant in issues related to and competent to make judicial decisions about the legality of the investigation, the technologies used and human rights; and which has adequate resources to exercise the functions assigned to it.

- **Transparency:** Governments must be transparent about the scope and use of their information-gathering powers, including transparency specific to access to data stored in the territory of another State. They should regularly publish, at a minimum, information on the number of applications to authorise these measures; the number and percentages of the applications granted and refused; the identity of the applying government authorities; the offences specified in the applications; the number of individuals affected by them; and the nature and duration of such measures.

- **Public Oversight:** Apart from effective judicial authorisation at the time of the launching such measures, such measures must also be subject to independent, effective, and impartial ex-post review (administrative, judicial, and/or parliamentary). Furthermore, Governments have an obligation to notify those who have been subject to these measures, and offer access to justice and a right to a remedy in the case of abuse of rights.

- **Safeguards for International Cooperation:** Any cross-border access to personal data must not be used to circumvent international or domestic legal constraints – including effective safeguards and oversight – that apply to access to data within the targeted State-party, or the State-party from which they are launched.

3. **Unjustified forced data localisation should be banned. Data transfers between jurisdictions should not occur in the absence of clear data protection standards.** The Drafting Group can use this process as an opportunity to address the issue of forced data localisation. Some States can and do prevent cross-border access altogether by legislating that companies must house their servers in the country so that data remain within the country's borders. This removes the need for any cross-border access agreements, but increases the risk of arbitrary surveillance, particularly of vulnerable groups. It is important to ensure that the T-CY does not confuse forced data localisation measures with national or regional data transfer limitations under data protection law. The latter allow transfers of data under certain, specific conditions, to ensure respect of users' human rights. The latter should not be impeded, as otherwise good data protection frameworks, such as that of the Council of Europe and the European Union, could be negatively impacted.

Reconciling human rights principles and the "Expected Results" of the drafting process

(The titles of the headings and sub-headings are taken directly from the Terms of Reference for the preparation of a draft Second Additional Protocol to the Convention on Cybercrime.[8])

I. Provisions for more effective mutual legal assistance (MLA)

Legal assistance under the Cybercrime Convention can indeed be made more effective and efficient. However, this should be done without reducing the crucial human rights and procedural safeguards surrounding such assistance, and in ways that ensure that MLA is at all times carried out in accordance with the basic principles. The European Commission's "non-paper" on "improving criminal justice in cyberspace" provides some useful insights into measures that can be taken to improve the MLA process.[9]

- **A simplified regime for mutual legal assistance requests for subscriber information**

  In line with Guidance Note 10, a simplified regime must include appropriate limits on the scope of "subscriber information," covering only the obtaining of the identities (and addresses) of persons holding a subscription of specific telephone numbers or IP addresses that are permanently assigned to the customer (as is done in Article 10(2)(e) of the EU Directive regarding the European Investigation Order, Directive 2014/41/EU). In particular, the "simplified regime" should not apply to the obtaining of information such as location data and dynamic IP addresses, which can be highly intrusive of an individual's privacy.

  The simplified regime must also respect the basic principles, be limited to subscriber information already held for commercial reasons, and not impose any new data retention obligations on service providers.

- **International production orders**

  We urge caution against following the example of the EU European Investigation Order (EIO), created by Directive 2014/41/EU, which has replaced most of the existing EU rules on the intra-EU cross-border obtaining of information in criminal cases, including those in the EU-Internal MLAT. Law enforcement agencies that operate

8 Pp. 3 – 4 of the Terms of Reference

9 European Commission Progress Report to the Council of the European Union, ST 15072/1/16, available from http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf

EIOs are subject to detailed data protection and human rights standards, such as those articulated in the Charter of Fundamental Rights and supervised of the Court of Justice of the EU. The Cybercrime Convention fails to ensure those same safeguards by imposing no requirements that State Parties be subject to any human rights instrument or human rights oversight mechanism. Indeed, there is not even a requirement that all States that are party to the Cybercrime Convention must also be a party to the European Convention of Human Rights (ECHR) or, for non-European States, the International Covenant on Civil and Political Rights (ICCPR), including their enforcement mechanisms, or to the Council of Europe Data Protection Convention (Convention No. 108). Without such a (relatively) strong human rights framework, instruments such as the proposed international production order, cannot be modelled on comparable EU instruments.

In addition, EIOs fail to provide adequate protections. Article 31 of Directive 2014/41/EU authorises EU Member States to engage in extraterritorial interceptions without actively attempting to identify the state where the data subject resides or where the data are located, beyond noting the geographical indication in the relevant phone number of static IP address, limiting the effectiveness of a notice requirement. The T-CY should depart from this approach.

However, international production orders would have to require States to provide notice and opportunity to challenge authorities in the country from which data are taken and the country of location of the data subject. The authorities issuing the orders must be "judicial authorities" in the proper sense, in line with European Court of Human Rights (ECtHR) case law and international human rights standards. International production orders must be subject to data protection and rule of law requirements and subject to oversight by domestic and international bodies.

The search for means to facilitate effective cross-border investigations should furthermore be accompanied by attempts to bring the substantive criminal laws of all State-parties fully in line with international human rights standards, in particular in relation to freedom of speech, so as to minimise the risks of individuals being subjected to intrusive measures, and possibly prosecutions, by authorities from States that impose excessive restrictions on human rights in general and free speech – including online free speech – in particular. It should not be the aim of the international community, or the Council of Europe, to make law enforcement across borders easier, without considering what laws are being enforced.

- **Direct cooperation between judicial authorities in mutual legal assistance requests**

  The Cybercrime Convention enables State-parties to designate as a "judicial authority" bodies that lack the attributes of a "judicial authority" as required by human rights law, including under the case law of the European Court of Human Rights (ECtHR). Some Budapest Convention State-Parties have designated law enforcement agencies or political officials such as ministers, or administrative bodies, or effectively any police office as "judicial authorities". Direct cooperation between judicial authorities is only acceptable if the judicial authorities satisfy the standards set for judicial officers in international and European human rights law.

- **Joint investigations and joint investigation teams**

  These are only acceptable provided they respect the basic principles. In practice, this means that the way in which joint intelligence task forces, such as the NSA-GCHQ joint bases, work, should not be replicated on the law enforcement level. Safeguards should be implemented to protect against risks of a joint task force, such as when one country attempts to bypass domestic safeguards. Additional oversight could include joint due diligence, obligations of clear logging and monitoring and public reporting, in order to ensure that accountability.

- **Requests in English language**

  This part falls outside our scope of work.

- **Audio/video hearing of witnesses, victims and experts**

  This part falls outside our scope of work.

- **Emergency MLA procedures**

  We fully endorse the need for effective, speedy procedures in cases of emergencies. Resorting to such emergency procedures should be limited to cases involving an immediate danger of death or serious physical injury to any person.

  However, there is no need to devise emergency procedures that do not comply with the basic principles. On the contrary, a core task of the Drafting Group should be to devise emergency MLA procedures that fully respect the basic principles.

II. Provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests

"Direct cooperation" as used here relates to the third special area of application of the proposed protocol: the direct requesting and obtaining of personal data by LEAs in one State-party from private-sector companies in another State-party. Direct cooperation across borders poses serious risks of violation of human rights law, particularly when it does not limit application to State-parties and does not require the knowledge and agreement of the country where the company is located and/or where the data subject resides. Direct cooperation risks the collection of personal data in contravention of data protection laws and in contradiction to the sovereignty of the targeted countries. Rather than first seeking to create a system that enables LEAs to act without the judicial authorisation of the country where the data are stored, to request "subscriber information, preservation requests, and emergency requests", priority should be given to making mutual legal assistance more effective.

Moreover, because of the heightened risk, additional protections are necessary. Once improvements to MLA procedures have been implemented, exceptional process for direct cooperation may be permissible. Given the risks, any regime to allow direct cooperation needs to be accompanied by effective safeguards and protections. Beyond the basic principles identified above, additional guarantees are necessary:

- The country making the request must inform and justify the use of the particular request in notices to the country where the data are stored and the country of residence of the data subject;
- Company responses must be permissive rather than mandatory;
- Appropriate and effective oversight of the companies' responses must be guaranteed, particularly to ensure that only data strictly necessary to the investigation are transferred to requesting countries;
- The data subject should be notified by the requesting authorities and by the company;
- The State-parties should publish annual transparency reports with the number, type, and temporal scope of the data requests. Companies should be allowed and indeed required to publish transparency reports with details on the requests and compliance rate;

- The information requested under the system may not be used for other purposes other than as described in the request and must be destroyed if shown to be unlawfully obtained or no longer needed.

III. Clearer framework and stronger safeguards for existing practices of transborder access to data

Some national laws allow for the direct, online gathering of electronic evidence by law enforcement agencies and -officials in one State-party, from ICT infrastructure and devices in another State-party (and perhaps even in non-State-parties).

In our view, provided the MLA processes can be made efficient and effective, it should be possible to devise procedures under which LEAs in any State-party can obtain access – and in appropriate cases, urgent and immediate access – to servers and devices in another State-party in full compliance with the basic principles.

Some national laws also allow for forms of government hacking without an appropriate framework in place. A number of civil society organisations have called for protections to ensure government hacking is conducted only with strict protections for human rights, particularly the rights to privacy, association and freedom of expression, as well as transparency and accountability. States currently hack for surveillance purposes, for instance by directly accessing companies' systems or causing the system to transmit data to the government. Hacking is commonly more intrusive than other existing surveillance techniques because it enables access to protected information in real time to data stored, or in transit and often to unintended data beyond the scope of the investigation.

Hacking can also create additional digital security risks. Exploits used in operations can act unpredictably, damaging hardware or software or infecting non-targets, compromising their devices and information. Even when a particular hack is narrowly designed, it can have unexpected and unforeseen impacts. Based on our analysis of human rights law, we conclude that there must be a presumptive prohibition on all government hacking. It is unacceptable that such a framework be established without the integration of protection for fundamental rights and property in national legislation.[10]

10 For a necessary human rights safeguards, see Appendix: Ten Human Rights Safeguards for Government Hacking: https://www.accessnow.org/governmenthackingdoc/

IV. Safeguards, including data protection requirements

We welcome the inclusion of this element and we believe that together with human rights and data protection the principles listed above should guide all aspects of the proposed protocol. Full compliance with international human rights law and respect for the sovereignty of States should be central to Drafting Group's work on the protocol.

V. Other possible elements

The Terms of Reference appear to leave it open to the Drafting Group to add further, as yet unspecified "other elements" to the draft protocol. In our view, the Drafting Group should be instructed not to do so unless further specifically authorised to do so by the T-CY.

EDRi

a coalition of 35 civil rights organisations

accessnow

Australian Privacy Foundation

cippic

@ DERECHOS DIGITALES América Latina

Digital Rights Ireland

ELECTRONIC FRONTIER FOUNDATION

epic.org

EPICENTER.WORKS for digital rights

IT-Politisk Forening www.itpol.dk

PRIVACY INTERNATIONAL

TEDIC

Xnet