27 October 2017

Annex to EDRi's response to the public consultation on improving cross-border access to electronic evidence in criminal matters organised by the European Commission

European Digital Rights (EDRi) is an alliance of 35 civil society organisations working in Europe and worldwide to defend fundamental rights and freedoms in the digital environment.

EDRi takes note of the European Commission's public consultation on improving cross-border access to electronic evidence in criminal matters. We take this opportunity to clarify our position and present some additional comments related to both the processes (I) and the substance (II) of any future EU action.[1]

I. Comments related to the process

- **Expert meetings**

EDRi welcomes the fact that the expert meetings were organised, as well as the openness and transparency shown by the European Commission. EDRi takes pride in having participated in these meetings, together with other civil society organisations. Nevertheless, we are deeply disappointed that we did not receive an invitation to any of the "targeted expert meetings and workshops with relevant stakeholders [that were scheduled to] be organised in September/October."[2]

- **Inception impact assessment and consultation process**

EDRi regrets that:

- The Inception Impact Assessment's legislative options do not include expressly MLAT reform nor the implementation of the European Investigation Order, which replaces "most of the existing laws in a key area of judicial cooperation – the transfer of evidence between Member States [excluding Denmark and Ireland] in criminal cases – by a single new instrument which will make cross-border investigations faster and more efficient"[3];
- Questions on how to improve MLATs are missing in the consultation;
- The consultation does not ask a single question regarding Option 5 of the Inception Impact Assessment, namely, "assessing the role of the EU towards the Council of Europe Budapest Convention on Cybercrime, in view of the negotiations on a second Additional Protocol to the Convention". We call on the Commission to:

1 This submission was written by Maryant Fernández Pérez. We are grateful to comments received by Professor Douwe Korff (FIPR), Katitza Rodríguez (EFF), Fanny Hidvégi (Access Now) and Walter van Holst (Vrijschrift).

2 https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en (page 6)

3 https://eulawanalysis.blogspot.be/2014/05/the-european-investigation-order-new.html

- ensure, in cooperation with Member States, that any adopted text is unequivocally in line with case law of the Court of Justice of the European Union (CJEU).
- advocate against any proposal that would lower the current standards of protection for human rights, such as the recent bill from the US Department of Justice (DOJ)[4];
- ensure that no text is adopted that would have the effect of lowering or circumventing high European standards of protection, including high guarantees of protection of the fundamental rights to privacy, data protection and due process.
- report to the European Parliament about its efforts to ensure opposition to "unfettered remote access for law enforcement authorities to servers and computers located in other jurisdictions without recourse to MLAs or other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process, including in particular Council of Europe Convention 108"[5];

- The consultation does not allow respondents like EDRi:
  - to respond to certain questions of importance, such as questions 23, 25 or 34;
  - to explain the reasoning of our answers – for instance, in questions 22 and 24 you can only explain "In what sense?" if you chose "yes". This can only lead to misleading results and statistics;
  - to explain that some questions are framed in a way that makes it impossible for us to respond due to the implications of all of the possible options available. This is the case of question 61, which misleadingly ties together "subscriber information" and "metadata".

- **Next steps**

EDRi welcomes the Commission's honesty in recognising that "[a]dditional data is needed in particular on the fundamental rights...aspects of the options considered by the Commission".[6] This is something that the European Commission needs to carefully assess *before* making any legislative proposal. EDRi trusts the European Commission to take institutional fundamental rights safeguards and assessments very seriously.

We consider that the current timeline for publishing a proposal (early 2018)[7] is unduly short. We encourage the Commission not to needlessly rush the process without having collected enough data on the effects any future EU action could have on fundamental rights and freedoms. It is in everybody's interest that any legislative action is of a quality that would meet the standards of the CJEU and the European Court of Human Rights (ECtHR).

4 https://www.eff.org/deeplinks/2017/09/protect-privacy-cross-border-data-stop-doj-bill
5 http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0366&format=XML&language=EN
6 https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en
7 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf (page 9)

II. Comments regarding the substance of the consultation

The only way to credibly propose any legislation in this area is to comprehensively address MLAT reform first.

Prioritisation problem

The public consultation seems to prioritise a legal framework on direct cooperation with service providers (option 1 of the Inception Impact Assessment (IIA)) "without having to go through a law enforcement or judicial authority in the other Member State" (question 58 of the consultation) and government hacking (option 3 of the IIA and questions 64-66).

We encourage the Commission to focus on MLAT reform. This could first start with assessing the implementation of the Digital Rights Ireland CJEU case that declared the EU Data Retention Directive illegal; the efficiency and implementation of the current European Investigation Order, including its impact on fundamental rights in practice; the complementary nature of the EU and national frameworks and the forthcoming Second Protocol to the Cybercrime Convention, etc.

Neither in the IIA nor in the consultation does the Commission refer to Ireland or Denmark, neither of which are part of the European Investigation Order Directive. In addition, according to a recent survey by the European Commission, neither Ireland nor Denmark cover/allow for direct cooperation.[8]

Subsidiarity check

On the other hand, it is worth noting that according to the Commission's own survey on direct cooperation, "the majority of national legislations" "*do not cover/allow* that service providers established in a Member State respond to direct requests from law enforcement authorities from another EU Member State or third country." "Moreover, the domestic law of *only 2 Member States allows* service providers established in those countries to cooperate directly with law enforcement authorities from other Member States or third countries", namely France and Spain.[9] In other words, this would imply a substantial change in the laws of the vast majority of the Member States. Adding an extra element to a framework that is already in considerable flux and chaotic is not advisable.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf (page 3)

9 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf (page 3)

27 October 2017

Recommendations in view of a potential EU legal framework on direct cooperation

EDRi would like to emphasise that we oppose direct cooperation with regard to both content and and non-content data, including metadata[10], both in the EU and outside the EU (the latter being particularly relevant in view of the objectionable US DOJ bill)[11]. The EU should focus on fixing MLATs and its internal mutual recognition framework first instead of finding ways to bypass them. This would also make any subsequent steps, if such are proven necessary by real-world experience, much easier to agree, from a political perspective.

If, despite this unpropitious background, the Commission insists on moving forward with proposing legislation to allow or facilitate direct cooperation between LEAs and service providers, bypassing MLATs, we urge the Commission to give serious consideration to the following points regarding:

A. Legal basis

In the Commission's Inception Impact Assessment[12], the Commission states that the "legal basis for EU action is Art. 82(1) and (2) TFEU, which specifies that *judicial cooperation* in criminal matters shall be based on the principle of mutual recognition" (emphasis added).

EDRi has serious doubts that this legal basis could be extended to direct cooperation between judicial authorities and/or LEAs and service providers as it refers to "judicial cooperation". In the same vein, this legal basis relates to the establishment of minimum rules, which could lead to low (or lower) standards of protection for fundamental rights. If direct cooperation ends up being used as a way to bypass MLATs, it should not be used as a harmonisation exercise to lower the level of protection or a way to bypass domestic legal standards, including privacy and data protection standards.

On the other hand, we have concerns whether the EU would be acting within the limits of the Union's competence, duly respecting the principle of subsidiarity.

B. Objective

The reasoning behind moving forward towards an EU legal framework on direct cooperation with service providers seems unjustified mainly for three reasons:

First, EDRi shares the Commission's view that Mutual Legal Assistance Treaties (MLATs) need improvement.[13] The Commission's insightful non-paper offers practical solutions to some of the problems that can ease the difficulties of the system, such as a global and secure online portal, better training for LEAs on how to use MLATs, simplifying and standarising forms, single points of

10 Content and metadata deserve equal level of protection. See https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf
11 https://www.eff.org/deeplinks/2017/09/protect-privacy-cross-border-data-stop-doj-bill
12 https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en
13 http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf (pages 6, 8-9, 12)

contact for providers and the police or streamlining of providers' policies.[14] However, there seems to be an assumption that direct cooperation with service providers, bypassing MLATs altogether, will solve all problems in an adequate, predictable way.

Second, recognising the failures of MLATs does not necessarily mean that the solution is direct cooperation with service providers. It is important to remember the Commission that it pointed to problems with MLATs as part of its justification for launching the Data Retention Directive when it was proposed 12 years ago.[15] Fixing the MLAT problems identified then would have been appropriate in 2005 and remains appropriate in 2017.

Third, the Commission seems to assume that because criminals are increasingly using information society services, this poses "an obstacle for effective criminal investigations". In this sense, question 22 in the consultation is framed inappropriately because in the digital era we leave more digital traces and therefore, information society services both create new investigative possibilities as well as obstacles. In fact, this is correctly pointed out in recital 3 of Directive (EU) 2016/680: "The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."

In case access to content data is more difficult (often for justified reasons), the UN Special Rapporteur on privacy clearly stated that metadata is "at least as revealing of a person's individual activity as the actual content of a conversation"[16]. This view is shared by the CJEU in its Tele 2 judgement, when it says that metadata "taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (...). In particular, that data provides the means (...) of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."[17]

As a result, it is clear that we live in a golden age for LEAs when it comes to collecting electronic information.

14 http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf (pages 16-17)
15 http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/sec/2005/1131/COM_SEC(2005)1131_EN.pdf (page 5)
16 United Nations Special Rapporteur's Report on the right to privacy, A/HRC/34/60, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Pages/ListReports.aspx
17 CJEU Judgment in Joint Cases -C-203/15 and C-698/15 ("Tele 2 judgment"), para. 99. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5bb65a5a48ae14841b104e29b8d03161f.e34KaxiLc3eQc40LaxqMbN4PaNaTe0?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=811969

C. Scope

As we have stated elsewhere, in relation to the related issue of the proposed Second Protocol to the Cybercrime Convention,[18] direct cooperation "poses serious risks of violation of human rights law, particularly when it does not limit application to [States that are bound by and in practice also fully adhere to, human rights requirements] 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."

Failing this, we call on the Commission to have a clearly and narrowly-defined scope. This includes scope in terms of:

- Situations in which this framework could be resorted to: direct cooperation should only be used as a last resort. In the Tele 2 judgment, the CJEU was very clear stating that "it is essential that access of the competent national authorities to retained data should, *as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities* submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime" (paragraph 120, *emphasis added*). The European Court of Human Rights (ECtHR) ruled in a similar way in its case Szabó v. Hungary (paragraph 77). In addition, authorities must need clear and strong "factual basis" for accessing the data, following the ECtHR in its Zakharovv Russia judgment (paragraph 260) and in its Szabó v. Hungary judgement, where the Court stated the need for "a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measures" (paragraph 71). While referring to surveillance in that instance, the same standard should apply to other types of government access to all types of data.

- Mandatory or Voluntary cooperation?: As we stated elsewhere,[19] "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." These include that "company responses must be permissive rather than mandatory". Question 58 of the consultation refers to this issue. However, the question is framed in a misleading way as it states that this would happen "without having to go through a law enforcement or judicial authority in the other Member State". It is our view that the authority making the request must inform and justify the use of direct cooperation to the other Member State.

18 https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf
19 https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf

- Authorities that would be able to make a production request: this is important in light of case law of the CJEU. We draw your attention to CJEU Opinion 1/15, where it stated that "the legal basis which permits the interference with [the exercise of fundamental rights] must itself define the scope of the limitation on the exercise of the right concerned" (paragraph 139). EDRi calls on the Commission to ensure that access to data must be authorised by an independent judicial authority, in line with the ECtHR's judgements and CJEU case law.[20]

- The data that may constitute digital evidence or "e-evidence" and therefore be subject to "direct cooperation". According to EU rules on data protection and privacy of communications, regardless of the type of personal data involved, these all deserve the same protection. Whatever categorisation chosen by the Commission must:

    - follow the definitions provided in EU e-privacy and data protection legislation. For unknown reasons, the European Commission does not allow respondents like EDRi to reply to the consultation's question 34. It is important to stress that research funded by the European Commission under the EVIDENCE project clearly states that "[s]o far there is no evidence that a lack of a common definition of what is electronic evidence has kept Member States from working together on the collection, preservation and use of electronic evidence. Neither is there evidence that the lack of a definition of what constitutes 'evidence' in the European Convention on Mutual Assistance in Criminal Matters, has been an impediment for the mutual assistance between European countries."[21]

    - be consistent with the Cybercrime Convention, especially if the Commission adds any extra-EU cross-border access provisions, while being more precise and clearer, since the definitions are very vague. In this sense, it is worth pointing out that the way in which question 61 of the consultation has been drafted prevented us from providing a meaningful answer. All types of data referred to in the question are different and asking the question in that way is inappropriate because the boundaries between content and non-content data are not clear.

      In light of the European Commission's intention highlighted in the IIA of "initiating negotiations with key partner countries such as the US in order to enable reciprocal cross-border access to electronic evidence, in particular on content data", EDRi would like to reiterate that we oppose direct cooperation with regards to both content and and non-content data, including metadata[22], both in the EU and outside the EU (the latter being particularly relevant in view of the objectionable US DOJ bill)[23]. Some

20 See *Zakharov v. Russia*, *Szabó v. Hungary*, *Digital Rights Ireland v. Minister for Communications et al* and *Tele2 Sverige AB v. Post*

21 Cf. page 28, http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-2-412.pdf

22 Content and metadata deserve equal level of protection. See https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf

23 https://www.eff.org/deeplinks/2017/09/protect-privacy-cross-border-data-stop-doj-bill

stakeholders see a need for this due to elaboration of relevant international instruments that could cover content data. However, in the absence of specific evidence to suggest that the EIO framework is unable to adequately handle questions around electronic data, it appears premature to impose such a far-reaching solution at this stage. In addition, we are concerned that this "cooperation" could undermine existing workstreams in the Commission on encryption.[24]

- respect the "Dual privacy protection principle": while the EU has a high degree of harmonisation on both data protection and privacy, a wide flexibility is given to Member States.[25] The Commission should promote high levels of protection within the EU. This means that the Commission should ensure that those authorities pursuing direct cooperation do not bypass the higher privacy safeguards among the Member States involved, by ensuring that requests for cross border access to data satisfy the privacy rules of both the requesting Member State and the other State involved, meaning each country would apply its ordinary legal test. So, if an authority of country A seeks data stored in country B, first a judge in Country A will have to ensure compliance with national standards, then the corresponding authority of country A will ask country B for the data, and then the ordinary country B competent authority will apply the ordinary country B privacy rules. In this scenario, we would also need minimum safeguards, such as the "necessary and proportionate" principles to ensure that minimum implementation of existing safeguards are established (see section D of this paper).

- Types of offences: our position is outlined in our response to question 59 of the consultation: double criminality and the seriousness of the offence are key. Cases of child abuse or terrorism are often brought up, but it should be noted that, in many countries, offences classified as "terrorist offences" include relatively minor acts, including non-violent acts such as verbally or in writing "supporting or glorifying terrorism" or even "supporting the aims of terrorist organisations" or attending rallies or displaying symbols or flags deemed by the authorities to be supportive of terrorism (with some organisations – such as secessionist movements – moreover deemed to be "terrorist" in some countries but not in others). Investigating non-violent and/or less serious criminal offences, e.g. related to freedom of expression restrictions, should not lead to direct cooperation with service providers. Failing this recommendation, specific safeguards provided of high quality of protection acquire even more importance.

- the addressee: EDRi would like to point out that there is not a one-fits-all solution for all types of companies highlighted in question 62 of the consultation. The Commission should

24 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf (page 9)

25 For instance, in the General Data Protection Regulation (GDPR), there are a lot of flexibilities which can and will certainly lead to disparities among Member States. See https://edri.org/analysis-flexibilities-gdpr/ In the context of criminal law, harmonisation was brought via a Directive (Directive (EU) 2016/680), leading to different implementations of the latter in the Member States.

take into account the differences of data architectures among companies, the data they collect, the size of the companies, their resources, among other elements. This implies that different safeguards may be needed for different companies subject to a production order/request. In addition, in case of direct cooperation, and provided there are safeguards in place, the legislative proposal should distinguish between data controllers and data processors: if a data controller (for example, a hospital) is using an information society service provider as a processor, the judicial authority should resort to the data controller (i.e. the hospital, in this case) directly. For example, if you are an operator of a SaaS ("software as a service") providing for General Practitioner's information systems, you would be faced by requests that could be declined by the controller (medial professional's privilege), but as a processor you would be in a much weaker position to do so.

D. Safeguards

The Commission rightly refers in its IIA to the fact that "additional data is needed in particular on the fundamental rights... aspects of the [legislative] options considered by the Commission". According to the Commission, "this will be gathered *partly* through the Joint Research Centre" (emphasis added). EDRi is looking forward to the conclusions of the Joint Research Centre and invites the Commission to have a targeted session with civil society organisations to assess the fundamental rights impacts of any EU future action in this subject matter.

On the other hand, EDRi would like to highlight that referring to fundamental rights in very broad terms or referring to "specific safeguards" without clarifying which fundamental rights safeguards are being proposed would not be enough. The specificity of the safeguards are as relevant as providing the highest level of protection to people's fundamental rights and freedoms. In this framework, we are not talking about convicted criminals, but persons subject to criminal investigations. The Necessity and Proportionality principles[26], which have been endorsed by over 600 organisations and thousands of individuals, are a good starting point.[27] EDRi urges the Commission to take into particular account the following elements within the Necessary and Proportionality principles:

1. **Legality:** according to the CJEU in Opinion 1/15 (paragraph 139), "the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned".

2. **Legitimate aim**: we refer to our comments to point B above.

3. **Necessity**, in line with case law of the CJEU, in particular its Tele 2 judgment that stated that "it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a

26 https://necessaryandproportionate.org/

27 As per the necessary and proportionate principles, access to data, interception of communications, etc fall under the definition of "communication surveillance".

prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a *reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime*" (paragraph 120, *emphasis added*).

4. **Adequacy or Appropriateness** to fulfil the specific legitimate aim.

5. **Proportionality**, which includes the need for a judicial competent authority to establish that[28]:
   - "there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out; and
   - there is a high degree of probability that evidence of relevance and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought; and
   - other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option; and
   - information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and
   - any excess information collected will not be retained, but instead will be promptly destroyed or returned; and
   - information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given; and
   - that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms."

6. **Access to data must only be authorised by a competent judicial authority**, in line with case law of the CJEU, which in its Tele 2 judgment stated that "it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a *prior* review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime" (paragraph 120, *emphasis added*).

7. **Due process,** by ensuring lawful, accountable and transparent procedures. This includes that "mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation".[29] As the Court stated in its Tele2 judgement, providers shall also "take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of

28 https://necessaryandproportionate.org/principles
29 https://necessaryandproportionate.org/principles

protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraphs 66 to 68)." (cf. paragraph 122).

8. **User notification by default and effective remedy:** according to the CJEU's Tele2 judgement, "the competent national authorities to whom access to the retained data has been granted *must notify the persons affected*, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. *That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy*, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 95)." (cf. Paragraph 121, emphasis added).

9. **Transparency** from all parties involved. For instance, it is completely unacceptable that the US-UK bilateral deal remains secret. This should not happen within the EU and we urge the Commission as Guardian of the Treaties to demand transparency and accountability from the UK.

10. **Public Oversight should be effective and accountable,** in line with the Necessary and Proportionality principles.

11. **Integrity of communications and systems**, in line with the Tele 2 judgment and our recommendations with regards to the use of hacking techniques (see the following below of this paper).

12. **Safeguards for international cooperation.** According to the Necessary and Proportionality Principles, where laws of more than one State apply, "the available standard with the higher level of protection for individuals is required". In this sense, dual privacy protection echoes the international norm of "dual criminality." Under this norm, a responding nation will not assist a requesting nation unless the crime being investigated is a crime not just in the requesting nation, but also in the responding nation. Dual privacy protection will also help ensure that as nations seek to harmonise their respective privacy standards, they do so on the basis of the highest privacy standards. Absent a dual privacy protection rule, nations may be tempted to harmonise at the lowest common denominator.

    The adoption of international agreements could be a clear indication that the Commission would be bypassing MLATs. While in MLATs, there are various safeguards against the further passing on of data (such as, typically, a right of the country that provided the data to have to consent, or at least object, to such onward transfers), there are no such safeguards when data are directly obtained from service providers, be that by the latter at their

discretion, or through direct access to the data by LEAs ("hacking"). This means that data obtained directly in these ways may well end up in the hands of regimes with whom we would not normally cooperate - which can be especially dangerous if they are onwardly transferred with a "flag" marking the data subject as a "possible" suspect (or even as a "possible" terrorist). EDRi encourages the Commission to assess the relationship between the Umbrella Agreement and any potential bilateral agreement with the US, for example. The Umbrella Agreement has significant flaws[30] and should not serve as a model for other data protection agreements.

13. **Safeguards against illegitimate access**, including, but not limited to, specific provisions stating that:
    - the service provider and the notified State can object to the measure[31];
    - "any information obtained in a manner that is inconsistent with these [safeguards] is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information"; and that
    - any data obtained must be used for the purpose for which the data was given, failing which "the material must not be retained, but instead destroyed or returned to those affected".[32]

Government hacking

Part IV of the consultation refers to "direct access to e-evidence through an information system without any intermediary (e.g. a service provider involved)". For the purposes of this paper, we will refer to this as "government hacking". As we stated elsewhere,[33] EDRi member Access Now conducted an investigation[34] into the human -rights implications of government hacking. Following their research and that of other EDRi members, we call for a ban on government hacking practices in principle.

Governments conducting these activities should be mindful of best practices and set up a clear, coordinated vulnerability disclosure system and commit to not stockpiling flaws for future use. The potential adverse effects of this type of stockpiling are exemplified by the Wannacry attack, where unpatched vulnerabilities previously withheld by the US government were used to compromise computers and install ransomware.

Following EDRi-member Access Now's lead, we call for a presumptive ban on the practice until the following safeguards are met:

30 See https://www.accessnow.org/umbrella-agreement-just-isnt-good-enough-protect-rights/ and http://sophieintveld.eu/commission-allows-exemptions-to-the-us-privacy-act-to-stay-in-place-umbrella-agreement-cannot-be-effectively-implemented/

31 Note this is already permitted in the EIO, Article 11, including refusal due to incompatibility of the measure "with the executing State's obligations in accordance with Article 6 TEU and the Charter".

32 https://necessaryandproportionate.org/principles

33 https://edri.org/files/encryption/workarounds_edriposition_20170912.pdf

34 http://www.accessnow.org/GovernmentHackingDoc

1. Government hacking must be provided for by law which is both clearly written and publicly available and which specifies the narrow circumstances in which it could be authorised. Government hacking must never occur with either a discriminatory purpose or effect;

2. Government actors must be able to clearly explain why hacking is the least invasive means for getting protected information in any case where it is to be authorised. In each of these cases they must also connect that necessity back to one of the statutory purposes provided. The necessity should be demonstrated for every type of protected information that is sought, which must be identified, and every user (and device) that is targeted. Mass hacking must be prohibited, including not just the hacking of large numbers of devices but also the use of hacking techniques to collect information on large numbers of people from centralised systems.

To illustrate the importance of this safeguard, it is worth remembering that Snowden revealed that GCHQ was harvesting gmail and other Google data in bulk from the backup data flows between Google data centres in different countries. This is no more acceptable than the EU Data Retention Directive's warrantless and suspicionless collection of the communications data of hundreds of millions of Europeans, which the CJEU found to infringe fundamental rights;

3. Government hacking operations must never occur in perpetuity. Authorisations for government hacking must include a plan and specific dates to develop and conclude the operation. Government hacking operations must be narrowly designed to return only specific types of authorised information from specific targets and to not affect non-target users or broad categories of users. Protected information returned outside of that for which hacking was necessary should be purged immediately;

4. Applications for government hacking must be sufficiently detailed and approved by a competent judicial authority that is legally and practically independent from the entity requesting the authorisation. This judicial authority should also have access to sufficient technical expertise to understand the full nature of the application and any likely collateral damage that may result. Government hacking should never occur prior to judicial authorisation;

5. Government hacking must always provide actual notice to the target of the operation and, when practicable, also to all owners of devices or networks directly impacted by the tool or technique once the investigation phase is finished or otherwise once the national legislation allows the disclosure of this information in analogous situations, such as wiretapping;

6. Agencies conducting government hacking should publish at least annual reports that indicate the extent of government hacking operations, including at a minimum the users impacted, the devices impacted, the length of the operations, and any unexpected consequences of the operation;

7. Government hacking operations must never compel private entities to engage in activity that impacts their own products and services in a way that undermines digital security;

8. If a government hacking operation exceeds the scope of its authorisation, the agency in charge of the authorisation should report back to the judicial authority the extent of and reason for this;

9. Extraterritorial government hacking should not occur absent authorisation under principles of dual criminality and without respecting other principles of international law;

10. Agencies conducting government hacking should not stock vulnerabilities and, instead, should disclose vulnerabilities either discovered or purchased unless circumstances weigh heavily against disclosure. Governments should release reports at least annually on the acquisition and disclosure of vulnerabilities.

We are looking forward to continuing to work with the Commission in a constructive way. We remain at the disposal of the European Commission to provide more input or to clarify any doubts and questions it may have.

For more information and clarification, please contact

Maryant Fernández Pérez

maryant.fernandez-perez (at) edri.org