15 March 2018

EDRi's response to the UNESCO Consultation on Internet Universality Indicators Phase II

European Digital rights (EDRi) is an association of civil and human rights organisations from across Europe. We defend rights and freedoms in the digital environment. We welcome the opportunity to give feedback on UNESCO's public consultation on Internet Universality Indicators Phase II and in particular on the first draft indicators document.

Personal information

Only information concerning name and organisation will be included when contributions are published online. As indicated below, please state if you do not wish your contribution to be published.

E-mail address: maryant.fernandez-perez@edri.org

Country/region: Europe

Gender: F

How would you define the stakeholder community or communities to which you belong?
Civil society

Questions

Are there any additional themes, questions or indicators which you believe should be included in the framework?

Digital Literacy:

- Are citizens aware of their rights and freedoms online?
- Does the government seek to encourage or coerce internet companies to restrict fundamental rights outside the rule of law, through public pressure, liability rules or other
- Are strategies in place to inform citizens of security and privacy threats online and how to mitigate them?

Freedom of Expression:

- Are restrictions on freedom of expression provided by law, necessary and proportionate to the aim pursued?

- Are restrictions regularly reviewed?

- Freedom of expression restrictions can result from the processing of personal data and sensitive data in particular (e.g. data about political activity or potential offenses, for example). Are personal data processed appropriately?

Open Content, Open Markets, Freedom of expression and Accessibility:

- Are net neutrality violations such as zero rating permitted?

- Are there effective rules regarding competition for online and network services?

Children and Young People

- Are children and young people aware of their rights online?

- Are there comprehensive education programmes concerning how children and young people can protect and defend their rights?

- Are there independent research programmes, such as Global Kids Online, on which evidence-based policy for online child development can be based?

See below for more specific suggestions.

Are there any suggestions that you wish to make in respect of the proposed themes, questions and indicators which are included in the framework as it stands?

CATEGORY R - RIGHTS

Theme A – Policy, Legal and Regulatory Framework

A number of regional rights agreements have also been agreed.

EDRi suggestion: We recommend to add a footnote indicating some of these rights agreements, including the EU Charter of Fundamental Rights and the European Convention on Human Rights.

A3. *Do citizens have access to due process to address violations of rights, online and offline, by state or non-state actors?*

Indicator:
- *Legal framework for due process*
- *Availability of arrangements for redress in terms of service of online service providers*

EDRi suggestion: We recommend to add "effective" before "access" in the question and to add "quality" after "availability" in the indicator since citizens are often notified in very broad terms and without meaningful information on how to seek redress. Moreover, we recommend to remove "in" and to add "for restrictions imposed through the" between "redress" and "terms" in the indicator. In addition, we suggest to add another indicator, namely "Availability of court proceedings against a decision by online service providers".

A4. *Are law officers, judges and legal professionals trained in issues relating to the Internet and human rights?*

Indicator:

- *Availability of relevant courses and proportions of relevant personnel who have undertaken or completed training.*

EDRi suggestion: We suggest adding "Existence of public budget line to include digital rights into judicial training programmes" as an indicator. Also, we suggest replacing "relevant" with "independent" and "relevant" with "judicial" in the existing indicator.

Theme B – Freedom of Expression

B1. *Is freedom of expression guaranteed in law, respected in practice, and widely exercised?*

Indicators:

- *Constitutional or legal guarantees of freedom of expression consistent with ICCPR Article 19 and evidence that it is respected and enforced by government*
- *(...)*

EDRi suggestion: We recommend changing "government" to "the State". Government is not the only relevant branch. The executive, legislative and judicial powers are relevant. The same should apply to the indicator **B.2 and others where references to "government" are made. We also recommend replacing "consistent with" with "implementing" in the indicator.**

B.4 *Under what conditions does the law hold platforms and other online service providers liable for content published by them?*

Indicator: legal framework for intermediary liability and content regulation is consistent with international rights agreements (including regional agreements) and proportionally implemented.

EDRi suggestion: Given on-going developments in privatised law enforcement i.e the increasing devolution of responsibility for the control/restriction of potentially "illegal content" from law enforcement authorities to private companies, it will be important to observe if said international rights agreements (including regional agreements) ensure that public authorities (e.g. law enforcement authorities) are responsible for the (admissible) restrictions, not the private companies imposed as a result of state pressure through, for example, rules on liability.
As per Article 52.1 of the EU Charter on Fundamental Rights, "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the

essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others"

We recommend UNESCO to duly take into account the Council of Europe's Recommendation on intermediaries: https://www.coe.int/en/web/portal/-/protecting-human-rights-online-new-guidelines-on-internet-intermediaries
https://edri.org/council-europe-takes-world-leading-step-towards-protecting-online-rights/

B.6 *Are low-cost online services available which enable citizens and civil society organisations to make use of the Internet to express their views?*

Indicators:

- *Availability of low-cost blogging and webhosting services*
- *Legal restrictions, if any, on access to such services*
- *Incidence of use of social media and blogging services*

EDRi suggestion: we suggest deleting this question and related indicators completely. There is a misleading perception that some online services are "low cost" when, in fact, they raise considerable privacy risks. These businesses are funded by the processing of personal data which is leading to very unfortunate outcomes. One does not have a healthier internet by having the presence of such ostensibly "low cost" online services rather than an open, decentralised, competitive range of online services. Having these indicators can only encourage the consolidation of market power of big businesses and restrain development. If this suggestion is not acceptable, we would recommend at least the additional indicator "availability of privacy-friendly low-cost services."

B.8 *Do journalists or citizens practice self-censorship in order to avoid harassment by government or online abuse?*

EDRi suggestion: we suggest making the question broader (i.e. "Do journalists or citizens practice self-censorship?") and keeping the specificity of harassment and online abuse as an indicator. Self-censorship is often a chilling effect of rights' and freedoms' restrictions that can be based on grounds other than government harassment or online abuse. For instance, if you are an anti-establishment rapper in Spain you may think twice before tweeting because there have been several instances whereby rappers have been sentenced to prison and monetary penalties for expressing themselves. See, for example, https://www.liberties.eu/en/news/sentencing-of-a-twitter-user-imperils-freedom-of-speech/11352. Similarly, the simple existence of unpredictable terms of service, such as a "three strikes" policy, run by one leading video-sharing platform.

Theme E – Privacy:

E.1 *Is the right to privacy guaranteed in law and respected in practice?*

Indicator: constitutional or legal definition of privacy and right to privacy

EDRi suggestion: in order to assess whether privacy is respected in practice (which is of utmost importance for privacy, security and freedom of expression), more indicators than the one proposed are needed, in line with E.2:

- 'Existence of a legal framework for the protection of privacy and confidentiality of communications'
- 'Existence of supervisory mechanisms and means of recourse and redress'
- 'Existence of an independent data protection authority which is equipped with sufficient resources to perform their tasks'

In the European Union, for example, we have a comprehensive framework composed of two elements: the General Data Protection Regulation (GDPR), which will be fully applied from 25 May 2018, and the e-Privacy Directive, which is in the process of being reformed and which complements the GDPR. This legislation covers not just your right to privacy and data protection, but also your freedom of communication and freedom of expression. Without legislation providing clarity on what these fundamental rights mean in this complex environment, the protection of confidentiality and security of communications would be less predictable and less enforceable. A lack of precise rules also makes it more difficult for companies to develop new and innovative services.

E.2 *Is the protection of personal data guaranteed in law and enforced in practice, with respect to governments, businesses and other organisations, including rights of access to information held and to redress?*

EDRi suggestion is twofold:

I: Reference should be made at some point to the nature of the way in which personal data is obtained. Data controllers should be compelled to obtain meaningful consent unless any other specific narrow exception is foreseen in the legislation. In order for consent to be meaningful, user consent must be explicit, specific, well-informed (i.e. the nature of what a user is consenting to should not be obfuscated by legal jargon), and freely given. It must also be possible for this consent to be withdrawn. In case processing using other legal bases similar guarantees (as expressed in the Council of Europe Convention 108 and in the EU General Data Protection Regulation) should be available.

Further information on user consent can be found in the European Data Protection Supervisor (EDPS) opinion on the Proposal for a Regulation on Privacy and Electronic Communications: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf
and in EDRi's paper on 'An Introduction to Data Protection' under 'consent to data processing': https://edri.org/wp-content/uploads/2013/10/paper06_web_20130128.pdf

II: Is the gathering of personal data subject to purpose limitation? The data needs to be collected

for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes. (See GDPR, Art. 5.b).

Such parameters may provide a useful context for the framework.
In conclusion, it may be advisable to add more indicators. The existence of a legal framework and an independent data protection authority are not enough to ensure data protection is guaranteed in law and enforced in practice. See, for instance, what happened with the EU Directive on Data Protection and the Max Shrems/Safe Harbor case before the Court of Justice of the European Union: http://www.europe-v-facebook.org/EN/en.html

III: Is the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)?

IV: Is the data accurate and kept up to date?

V: Are there measures of effective deletion or, at least, meaningful anonymisation once the data is not needed anymore (storage limitation)?

VI: Is the data processed in a manner that ensures appropriate security of the personal data (integrity and confidentiality)?

VII: Is the data controller responsible for the compliance with data protection rules (accountability)?

See: GDPR Article 5 for the other principles defining how personal data should be processed.

E.3 *Are the powers of law enforcement and other agencies for surveillance of Internet users necessary, proportionate and limited to circumstances which are consistent with international rights agreements?*

Indicator: Legal framework for surveillance, and evidence concerning implementation

EDRi suggestion: Given the huge increase in surveillance during the last decade - and the difficulty in repealing security measures regardless of their effect on freedoms, the consequences, and effectiveness - it is necessary to check and ensure whether or not new measures are subject to parliamentary scrutiny and are made available to civil society ahead of their adoption. For example, The Hague Programme 'principles of availability', which aimed to facilitate co-operation between the police and judicial authorities bypassed such scrutiny which resulted in law-enforcement agencies becoming increasingly 'self-regulated' and in unprecedented levels of processing of personal data.

Further information can be found in EDRi's paper on EU Surveillance: https://edri.org/wp-content/uploads/2013/10/paper02_web_20120123.pdf

CATEGORY O: OPENNESS

Theme D – Open Content:

D.1 *Does the government actively promote access to knowledge through its policies for education, culture and science?*

D.2 *Do arrangements for intellectual property protection balance the interests of copyright holders and information users in ways that promote innovation and creativity?*

EDRi suggestion:

Question D2 is badly phrased. The default should be openness, with restrictions on availability of access to culture being a restriction. It is not a question of "balance", the question is whether the right to information is excessively restricted by measures that create and implement "intellectual property".

Access to knowledge, education, culture, and science are to a high extent conditioned by copyright policies. These copyright policies, albeit originally aimed at protecting authors and to ensure that the creative process is encouraged, often lead to the empowerment of the oligopolies of publishers and editors that abusively restrict the access to cultural, educational, and scientific material. Indeed question D2 talks about "copyright holders" rather than "creators", This choice of wording is meaningful.

According to Farida Shaheed, the United Nations (UN) Special Rapporteur in the field of cultural rights, this has caused increasing tension between copyright law and human rights law. Her report on "Copyright policy and the right to science and culture" argues strongly that we need to pay more attention to the human rights repercussions of granting authors – and rights holders – exclusive rights over authorial works.

Much of the report is based on the two principles enshrined in Article 27 of the Universal Declaration of Human Rights. Paragraph one thereof bestows upon everyone the right to culture and science,the right to participate in the cultural life of a community and to profit from the advancement of science. This paragraph is complemented by a second one, which asserts that authors' moral and material interests must be protected.

The second paragraph of Article 27 is often interpreted as supporting copyright protection (while the first paragraph provides the rationale for exceptions and limitations). Shaheed's central thesis is that this analysis is wrong. She writes that "[t]he human right to protection of authorship is [...] not simply a synonym for, or reference to, copyright protection, but a related concept against which copyright law should be judged. Protection of authorship as a human right requires in some ways more and in other ways less than what is currently found in the copyright laws of most countries."

We call UNESCO's attention also to Article 2.1 of the UNESCO Convention on Cultural Diversity:

Cultural diversity can be protected and promoted **only** if human rights and fundamental freedoms, such as freedom of expression, information and communication, as well as the ability of individuals to choose cultural expressions, **are guaranteed.**

Indicators:

- Are copyright policies flexible enough to allow for legal access to cultural, education and scientific knowledge?
- Are copyright enforcement policies effective enough without leading to over-enforcement by private companies and governments when no significant impact on the general exploitation of the work by the author?
- Do copyright enforcement measures guarantee freedom of expression, information, and communication in practice?

D.5 *Does the government require ISPs to manage network traffic in a way that is transparent, evenly applied and does not discriminate against particular types of content or content from particular sources?*

Indicator: regulatory arrangements concerning net neutrality

EDRi suggestion: Net neutrality is one of the foundational principles of the internet. Government should not require traffic discrimination. If the question is about ensuring net neutrality, the question should be reformulated: "Does the government require ISPs to treat traffic equally without discrimination on the basis of origin, destination, or type of data?"
We also advise to include net neutrality questions under other headings. "Open content" may not be the best place. Examples:

- Are net neutrality violations such as zero rating permitted?
- Are there effective rules regarding competition for online and network services?

E.4 *Are provisions concerning the location and duration of data retention consistent with international standards of data protection and supportive of effective access?*

Indicator: Legal and regulatory provisions concerning data retention and cross-border data flows

EDRi suggestion: The context of this question gives no clues whatsoever about what data is being collected and retained, whether it is personal data or not, under what type of legal framework, who should have the right to access it, etc.

In the absence of clues about the actual meaning of the question, we will assume that it refers to mandatory communications data retention for law enforcement purposes.

This being the case, the premise that it is possible to have mandatory data retention for law enforcement purposes that is consistent with international standards is questionable.

The bulk retention of all citizens communications data regardless of any link to serious crimes (i.e.: existence of suspicion in a given judicial process) on them is against human rights standards since it is "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance" as established in Digital Rights Ireland case by the

Court of Justice of the European Union.[1] Leading experts convincingly argue that in order to ensure that measures respect necessity and proportionality effectively in data retention norms both the retention and the access stages need to be carefully designed.[2] The fact that data retention laws store metadata about electronic communications does not mean that the norm is less intrusive. From the retained data, it is relatively easy to obtain the entire "social graph" (personal contacts and intensity of each contact) of a person. Furthermore, when talking about retained location data (cell ID), a complete profile of a person's movement can be constructed. In combination, all of this data can reveal very personal aspects of a person's private life. When implementing data retention policies, the following characteristics are, according to relevant case law, some of the main issues to be taken into consideration to analyse the existence of an interference with the right to privacy and data protection:

Indicators:

- **The retention needs to show evidence that the measures are strictly necessary and that the data is used for a specific and limited purpose**. This has not been proved in either of the two CJEU cases that have dealt with the issue.
- **There can be no bulk (indiscriminate) data retention**. Data collection needs to be targeted at both the collection and access stages. This has not been fulfilled by any of the instruments.
- **When engaging in data retention, a link (even if indirect) between the data subject and serious crimes needs to be done, based on objective criteria**. The link to serious crimes has not been found in the collection stage for any of the instruments.
- **The retention period needs to be justified and connected with the purposes that the law is meant to achieve**. No justification has been shown for the specific data retention periods in each of the instruments.
- **The access by law enforcement authorities needs to be clearly defined and include safeguards that protects individuals from abuses.** This can be done via the supervision of independent authorities (Data Protection Authorities), authorisation by judicial authorities, and notifications ex-post (once the investigations has ended). Some of the instruments allow for the supervision of DAPs (Spanish data retention law), while others allow for ex-post notification for certain metadata (phone calls metadata). There does not seem to exist a comprehensive system of safeguards in any of the instruments analysed.
- **Finally, the retention of data needs to be done only for specific cases and not a systematic, untargeted practice.**

1 Digital Rights Ireland Ltd (C-293/12), para. 37

2 Specifically, Privacy International (2017) specifically states that: "safeguards must be put in place to ensure that the interference with fundamental rights is minimised at both the retention and the access stages."

CROSS-CUTTING INDICATORS

Group B – Children and young people

EDRi suggestion: section should expand beyond simply access and safe/effective use to consider the rights of children and young people (e.g. to privacy) and their awareness thereof, as well as the educational programmes designed to inform them of their rights.

For further information you can read EDRi's booklet on Privacy for Kids: https://edri.org/wp-content/uploads/2016/12/privacy4kids_booklet_web.pdf

Additionally, it is worthwhile to note that simply the existence of a legal framework for each of the rights denoted is insufficient, but that said legal frameworks/laws are upheld, comprehensive, and well-enforced. Also, that exceptions in the case of security are proportionate, clear, transparent, and subject to oversight.

What sources and means of verification would you recommend, from your experience, in relation to any of the questions and indicators that have been proposed?

In addition to the indicators that we have already listed, we stress that, in relation to the protection of children online, rigorous, sober, independent and ongoing monitoring of the experience of children and the effectiveness of all policies implemented must be undertaken.

Our network has activists and experts on the ground which gather evidence, defend and advocate for the respect and protection of digital rights in Europe:

- https://edri.org/
- https://edri.org/members/