EDRi submission to UN Special Rapporteur David Kaye's call on freedom of expression and the private sector in the digital age

Introduction

EDRi is a not-for-profit association of digital civil rights organisations. Our objectives are to promote, protect and uphold civil rights in the field of information and communication technology.

European Digital Rights (EDRi) welcomes the UN Special Rapporteur on freedom of opinion and expression David Kaye's public consultation on the role of ICT companies vis-à-vis freedom of expression in the digital environment to identify:

I. the categories of actors in the ICT sector whose activities implicate the freedom of opinion and expression;
II. the main legal issues raised for freedom of opinion and expression within the ICT sector; and
III. the conceptual and normative work already done to develop corporate responsibility and human rights frameworks in these spaces, including governmental, inter-governmental, civil society, corporate and multistakeholder efforts.

I. ICT actors with a potential to impact freedom of expression and opinion

In order to communicate online, it is necessary to rely on a chain of different service providers, often based in different jurisdictions and with whom one may have no direct relationship at all. For example, if "zero-rating" or even data caps are imposed by Internet access providers in a country and you have no organisational and financial capacity to be "zero-rated", your ability to communicate with people that are using such restricted services is limited and there is no "leverage" with the ISPs that connect your intended audience with the Internet.

Section 104 of the ill-fated "Stop Online Piracy Act" (SOPA) in the United States offers an interesting case study in terms of bad practice. It sought to offer an open-ended right for intermediaries ("service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar") for taking action against online services *believed* to be in breach of US law. For an online service - particularly a commercial online service - this would have meant that any one of seven different types of service that is relied upon to deliver a service could, with a significant degree of impunity, destroy or damage your online presence.

Subsequently, even though this initiative failed, the White House reached agreements with payment providers and advertising networks, whereby they agree to undertake that kinds of action - including extraterritorially - foreseen by SOPA. Indeed, there are examples of all of the types of service listed in SOPA. The issues which arise from such actions are:

1. **Extraterritoriality**.
The intended outcome of SOPA was the global implementation of US copyright, trademark and related laws. This circumvents national democratic processes, minimises opportunities for appeal and obviates due process of law. The" voluntary" measures agreed and/or unilaterally implemented by commercial operators leads to the same result.

2. **Constitutional rights and international law.**
By relying on the *ad hoc* actions of private companies, the US government has created mechanisms for undermining freedom of expression, but cannot be held accountable in court, as the operational decisions are taken by private companies and not the government. It is becoming standard practice for many governments to coerce, encourage or allow Internet companies to "voluntarily" restrict rights in ways that are not "prescribed by law", circumventing international law and constitutional free speech rights.

3. **Predictability**
The individuals impacted by any restrictive measures imposed, or potentially imposed, by such schemes need to comply with their own national laws, the national laws of the United States and the - arbitrary - interpretation of the service provider(s)' terms of service.

4. **Redress**
Where a "safe harbour" for liability for imposing restrictions is implemented – as threatened but not implemented by SOPA–, there is no reasonable hope of redress, unless the individual can prove, possibly in a foreign court and potentially in a foreign language, that the measures were not implemented in good faith.

What does this mean in practice for freedom of expression and opinion?

We can see this most clearly in relation to the global implementation of the United States Digital Millennium Copyright Act (DMCA) by the major online communications platforms. Under the DMCA, if complainants fulfil a set of criteria for reporting alleged breaches of copyright (the "notice"), the intermediary becomes liable if they fail to remove the content ("takedown") in question. This means that, from a real, practical perspective, Internet users worldwide that use services like Facebook and Google are subject to their own national laws, US copyright law *and* the (often unpredictable and vague) terms of service of online providers.[1]

In addition to obviously significant intermediaries, less obvious service providers can also have a major impact, such as:

- **Domain name registrars**. For example, in 2008, a US-based domain name registrar completely wiped out a Spanish company's online presence because it provided tourism services (not

[1] A list of abuses of this situation can be found at https://www.eff.org/nl/deeplinks/2014/12/copyright-law-tool-state-internet-censorship

directed at the US market) to Cuba.[2]

- **Global Internet governance organisation.** Basing itself on ICANN's Registrar Accreditation Agreement, the City of London Police threatened the Canadian domain name registrar EasyDNS with having its accreditation agreement removed (thereby destroying its business) if it did not revoke domain names *accused* of being used in association with "intellectual property" violations. Thankfully, EasyDNS rejected this pressure and took the case to arbitration and won.[3] Under a "safe harbour" as foreseen by SOPA, the already unbalanced incentives for EasyDNS to reject this abuse of due process and jurisdiction would have been minimal.

- **Payment providers**. PayPal has unilaterally removed services and frozen the assets of file hosting and even VPN (virtual private networks) services as a law enforcement measures.[4]

II. Legal issues for freedom of expression

Unfair contract terms, jurisdiction, applicable law, defending constitutional free speech and an international "prescribed by law" requirements, incentives of online companies not to restrict free speech, safe harbours for liability and for voluntary punitive measure are some of the legal issues that the Special Rapporteur could consider. EDRi has identified a non-exhaustive list of legal challenges that have an impact on freedom of expression, which includes the freedom to receive, seek and impart information as well as freedom of opinion.

- **Transparency**

Transparency is necessary, but it is only the first step. Transparency reporting is frequently not very "transparent", most particularly with regard to non-obligatory restrictions. One social media company, for example, does not include "voluntary" removals of content by individuals after court orders have been received.

Making restrictions to fundamental rights and freedoms more transparent does not legitimise or excuse them. Accountability and remedies for abuses are necessary as well. An essential part of transparency is *ex ante* transparency about the actual meaning of - and accessibility of - terms of service. It is unacceptable - as in the case of Amazon's withdrawal of services to Wikileaks[5] - for the service provider to decide *ex post* to give its terms of service a new meaning.

- **Content regulation on all platforms and by all services and providers**

There is no problem in principle with the notion that service providers be able to decide with whom they want to do business or not. However, this is not an unlimited right and will change depending

[2] http://www.nytimes.com/2008/03/04/us/04bar.html
[3] http://blog.easydns.org/2013/10/08/whatever-happened-to-due-process/
[4] https://torrentfreak.com/paypal-cuts-off-pirate-bay-vpn-ipredator-freezes-assets-130724/
[5] http://www.nytimes.com/2010/12/02/world/02amazon.html?_r=0

on the balance of other rights at stake. For example:

- Are the terms of service clear enough to allow the user to adapt their behaviour?
- Are there equivalent means of communication available, permitting individual to exercise their freedom of expression?
- Is there a wider public policy objective being pursued?
- If so, is the restriction based on coordination with public authorities and in respect of the rule of law?
- Have key performance indicators and review processes been created, in order to assess the proportionality of the restriction?
- How internal or external is the restriction (spam management is mainly an internal issue, for example, while a "three strikes" system is mainly external)?
- If the purpose is law enforcement, whose law is being enforced?
- Have unintended consequences such as counterproductive effects or anti-competitive outcomes been diligently examined?

It is also important to consider the nature of the content that is being rejected by the service provider. Prohibiting pictures of cats, for example, is of minimal free speech significance, as there is no public policy objective being pursued and lots of alternative services that do allow this legal content. On the other hand, banning allegedly "illegal" content raises multiple challenges for a whole variety of reasons including the following:

- normally this leads to a lack of clarity as regards whether the content being removed is due to an accusation of (criminal?) illegality or breach of terms of service;
- unilateral action to remove illegal content can interfere with government investigations;
- unilateral action to remove illegal content can disincentive government investigations and prosecutions of criminal activities.

- **Intermediary liability and balance of rights online**

Issues surrounding direct liability for illegal activity have been extensively studied, most recently by the Manila Principles[6] and also by the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Frank LaRue.

Although not strictly a content liability, more delicate issues surrounding the balance of rights online have been addressed by i*nter alia* the Court of Justice of the European Union, such as in cases C-314/12 (Telekabel)[7] and C-275/06 (Promusicae v Telefónica)[8]. The role of injunctions, in particular is a particular challenge. This is due, firstly, to the difficulties for courts to make complex proportionality assessments and, secondly, faced with a constantly changing online environment, developing review processes to ensure that measures remain proportionate.

[6] https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf
[7] https://edri.org/web-blocking-austria-law-with-the-law-taken-out/
[8] https://edri.org/edrigramnumber6-2ecj-traffic-copyright/

Overall, EDRi sees a consistent problem when restrictions on fundamental rights are imposed "voluntarily". In practice, online companies are increasingly being given the role of ultimate arbiter and decision-maker over the "reasonable" balance to make between different rights, with the fear of facing liability or public relations damage in case of not monitoring, filtering, blocking or deleting the content in question.

States are often directly encouraging "self-regulatory" restrictions on rights outside of the rule of law that are based on vague and unclear terms of service. This situation is clearly contrary to basic principles of human rights law, particularly as regards the requirement for restrictions to be prescribed by law, necessary in a democratic society and proportionate.

Intermediaries generally lack counterbalancing obligations to respect human rights and fundamental freedoms. States should not delegate their human rights obligations to the private sector. The liability of Internet intermediaries is not a solution to issues such as child abuse, child protection, terrorism, hate speech or defamation, especially when the counterbalance to the actions taken by intermediaries is absent and one interest is disproportionately prioritised over the other.

- **Political power of online companies**

This includes mandates or requests to take down content or services, mandates or requests to develop/alter discourse online or mandates/requests to withdraw services. The demands of governments for "reasonable" interventions by private companies into political dialogue and online communications is often based on an either naive or reckless hope that these profit-driven companies will act in a way which:

- is necessary and proportionate
- will remain necessary and proportionate in a changing environment
- will not be exploited for anti-competitive reasons
- will not have counterproductive effects for the intended public policy outcome
- will not have anti-competitive effects.

When we consider the vast amount of personal data controlled by some online companies, experiments such as Facebook's controversial "mood" experiment, Facebook's proven ability to manipulate elections, research on Google's putative ability to manipulate elections, etc, the limits of the involvement of private companies in online discourse needs to be considered.

- **Government mandates or requests to cooperate with government surveillance**

- **Security and privacy**

EDRi encourages the rapporteur to address the benefits of a strong privacy policy; the use of encryption for creating a secure and anonymised environment; adopting privacy-by-design models; respecting the principles of purpose limitation and data minimisation, etc.

In this regard, EDRi would like to stress the need to differentiate between mandatory or forced

data localisation and local data storage requirements for specific purposes, such as data protection. Whereas the former is worrisome, the latter is legal and necessary under EU law. As stated elsewhere,[9]

> On the one hand, mandatory data localisation measures putting an obligation on suppliers that operate on the Internet to store data within a specific country, rather than on servers in other countries, undermines the fundamental openness and interoperability of the Internet, and create a serious risk for security. Such data localisation practices increase the possibility of government's abuses as data is kept in limited number of easily identifiable locations, putting people's human right to privacy and freedom of expression at risk. These practices must be prevented.[10]
>
> On the other hand, a local data storage requirement for the protection of data does not raise the same concerns as with forced data localisation because data are not "blocked" in a country, but can be transferred at any time within the EU or to third countries under the conditions set by EU Data protection laws.

- **Remedies**

Restrictions to human rights and fundamental freedoms must have a legal basis and effective and enforceable remedies shall be available.

- **Prevention**

To solve problems such as hate speech, a long-term solution is to implement high quality media education, but the short term solution is more speech. As Frank LaRue has frequently said, the answer to hate speech is more speech.

III. Existing approaches to solve the issues

We encourage the rapporteur to study the suitability of a legal approach that would create legally-binding and enforceable obligations on private entities to respect human rights and fundamental freedoms online. In this sense, there are many sources which deserve some consideration. We present a non-exhaustive list of reports, studies, guidelines or principles developed to solve the legal challenges identified in the previous section:

- **Human Rights and the ICT Sector: A thought leadership agenda for action for GeSi**

http://gesi.org/files/Reports/Human%20Rights%20and%20the%20ICT%20Sector%20-%20A%20Thought%20Leadership%20Agenda%20for%20Action_FINAL.pdf

- **EDRi Privatised online enforcement series**

http://history.edri.org/edrigram/number9.6/abandonment-rule-of-law
https://edri.org/edrigramnumber9-7self-regulation-worse-useless/

[9] https://edri.org/files/TiSA_Position_Jan2016e.pdf
[10] https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights

https://edri.org/edrigramnumber9-8self-regulation-sabam-scarlet-case/
https://edri.org/edrigramnumber9-9anatomy-self-regulation-proposal/
https://edri.org/edrigramnumber9-10online-trading-platforms-sell-out/

- EDRi Booklet: Slide from Self-Regulation to Corporate Censorship

https://edri.org/wp-content/uploads/2010/01/selfregualation_paper_20110925_web.pdf

- EDRi Booklet: Human rights and privatised law enforcement

https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf

- Council of Europe, Human Rights Violations Online, drafted by European Digital Rights, DGI(2014)31

https://edri.org/files/EDRI_CoE.pdf
https://edri.org/edri-coe-human-rights-online/

- Outcomes of "unconference" at Stockholm Internet Forum 2013

https://edri.org/sif13

- Ranking Digital Rights

https://rankingdigitalrights.org/

- UN Guiding Principles on Business and Human Rights

http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

- ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights

http://shiftproject.org/sites/default/files/ECHRSG.ICT_.pdf

- Manila Principles

www.manilaprinciples.org

- (draft)Treaty on Transnational Corporations

http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/26/9