20 December 2017

Submission to study on social media, search, and freedom of expression

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.

EDRi welcomes the opportunity[1] to submit comments for the June 2018 Human Rights Council.

We strongly believe that the issues addressed by the UN Special Rapporteur on Freedom of Expression and Opinion are very serious for freedom of expression worldwide and should be treated with utmost seriousness by the Human Rights Council.

Company compliance with State laws:
a. What processes have companies developed to deal with content regulation laws and measures imposed by governments, particularly those concerning:
i. Terrorism-related and extremist content;

For instance, the Europol Regulation (Regulation 2016/794)[2] of the European Union provides some useful insights into haphazard, arbitrary approaches to potentially dangerous content. The Regulation gives Europol – a police cooperation agency – the job of identifying content that may be in breach of service providers' terms of service, as part of the fight against serious crime and terrorism:

> Article 4.1.: Europol shall perform the following tasks in order to achieve the objectives set out in Article 3:
>
> (...)
>
> (m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned **for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions.** (emphasis added)

Referrals by the EU Internet Referral Unit (EU IRU) are made to service providers without an accusation of illegality, with no apparent instructions about how to handle associated personal data, with no apparent (or no automatic) referral to law enforcement authorities and no records kept regarding if there are any associated investigations or prosecutions related to the content in question. Somehow, the content is serious enough to require this arbitrary, unregulated framework and not serious enough to require investigations, freezing of data nor, indeed, any kind of diligent record-keeping.

1 https://freedex.org/wp-content/blogs.dir/2015/files/2017/09/Call-for-Submissions-Social-Media-Search-and-FOE.pdf
2 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794

European Digital Rights | 20 Rue Belliard, 1040 Brussels, Belgium | Tel. +32 2 274 25 70 | www.edri.org

In response to Parliamentary Question E-1772/2017, the European Commission confirmed that "the EU IRU does not keep any statistics of how many of the referrals to Member States led to the opening of an investigation"[3].

About 90% of the content referred is deleted by service providers, according the European Commission press release[4].

ii. False news, disinformation and propaganda; and/or
iii. The "right to be forgotten" framework?

It is not clear what "framework" means in this context.

EU background:

The Court of Justice of the European Union ruled (in case c-131/12[5]) that the act of providing a search engine as being an independent act of data processing that renders the search engine a "data controller". It also found that search engines had an obligation to mitigate the harm caused by search results that are "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine."

Following a broadly similar logic, Google had previously acted, on its own initiative, to demote links to "mugshot" websites (globally)[6] and has since decided to de-index "revenge porn"[7] websites globally.

On this basis, it appears clear that both Google and the European Court recognise that harm can be caused to individuals by the way a search engine processes personal data and that mitigating action is necessary in some cases.

It is not clear how the European Court could have taken a view on the fundamental right to data protection (as defined by the EU Charter of Fundamental Rights, part of the primary law of the European Union) that would be weaker than that of Google. The Court took the view that, rather than removing the sites in question from the search index (rendering them unfindable) or ordering the removal of the page itself from the internet, the least restrictive alternative available would be to remove the relevant pages from search results, when the search is done using the person's name.

Challenges

The fact that the least restrictive alternative was chosen does not mean that the ruling is without

3 http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2017-001772&language=EN
4 http://europa.eu/rapid/press-release_IP-17-544_en.htm
5 http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065
6 https://searchengineland.com/google-launches-fix-to-stop-mugshot-sites-from-ranking-googles-mugshot-algorithm-173672
7 https://support.google.com/websearch/answer/6302812?hl=en

European Digital Rights | 20 Rue Belliard, 1040 Brussels, Belgium | Tel. +32 2 274 25 70 | www.edri.org

challenges for freedom of expression.

Looking at the decision-making process Google has to go through, it always seems easier to impose the restriction than not to impose it:

- Google has to balance an obligation to act (in accordance with its obligations under the ruling) with not changing its index (which may lead to an appeal or court case).
- It has to balance a decision to act (which has no appeals mechanism), with a decision not to act (which is subject to an appeals mechanism).
- It has to balance a decision to act (where there is secondary law protecting privacy), with a decision not to act (where there is limited legislation on protection of freedom of expression).

The fact that, even in a reasonably narrow restriction (de-linking specific names to specific search results that are inadequate, irrelevant, or excessive), the search engine has to find a balance between the fundamental rights to privacy and data protection on the one hand, and freedom of expression on the other, raises concerns about predictability and the rule of law.

For such a framework to function in a way that respects the rule of law and predictability, it is important to have oversight and a balance of incentives that does not push excessively in one direction or another. While the underlying logic of the ruling appears unavoidable, the process of implementing the ruling raises concerns.

b. How should companies respond to State content regulation laws and measures that may be inconsistent with international human rights standards?

Companies need to be as consistent as possible in their attitudes towards content regulation and other measures. It is politically and logically difficult to have terms of service or community guidelines which permit companies to impose arbitrary restrictions to freedom of expression or the right to privacy on the one hand, and for those companies to take a principled stand against arbitrary restrictions to freedom of expression and the right to privacy requested by (particularly democratically elected) governments on the other.

We have seen several examples, in a European context, where the EU and its Member States have been inspired by the terms of service and community guidelines of companies in formulating their requests for restrictions that are inconsistent with international human rights law.

For instance, the EU's "hate speech" code of conduct explicitly downgrades the law behind company terms of service.[8] The code requires companies to "requests against their rules and community guidelines and where necessary national laws." [9]

8 https://edri.org/new-documents-reveal-truth-behind-hate-speech-code/
https://edri.org/faq-code-conduct-illegal-hate-speech/

9 http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

European Digital Rights | 20 Rue Belliard, 1040 Brussels, Belgium | Tel. +32 2 274 25 70 | www.edri.org

2. Other State Requests: Do companies handle State requests for content removals under their terms of service differently from those made by non-State actors?

The statistics quoted by the European Commission suggest that there is a far higher level of compliance with requests from Europol compared with from other sources. However, data gathering in the EU on such activities is of a very low quality and consistency, as noted in December 2017 by a Resolution of the European Parliament, commenting on Member State and European Commission data on takedown and blocking of child abuse material. For example:

> *D: whereas the Commission's implementation report does not provide any statistics on the take-down and blocking of websites containing or disseminating images of child sexual abuse, especially statistics on the speed of removal of content, the frequency with which reports are followed up by law enforcement authorities, the delays in take-downs due to the need to avoid interference with ongoing investigations, or the frequency with which any such stored data is actually used by judicial or law enforcement authorities;*[10]

Do companies receive any kind of content-related requests from States other than those based on law or the company's terms of service (for example, requests for collaboration with counter speech measures)?

The dispute between EasyDNS is an interesting case or a state request based neither on law nor the provider's terms of service. The City of London Police addressed a request to EasyDNS for a domain name to be revoked (despite having no legal power to do this). It argued, incorrectly, that failure to comply was a breach of ICANN's Registrar Accreditation Agreement, implicitly threatening that ICANN would withdraw EasyDNS' accreditation if the order was not complied with. So, it was not the terms of service governing the relationship between EasyDNS and its customer that the state authorities sought to rely on, but the agreement between EasyDNS and ICANN.[11]

2. Global removals: How do / should companies deal with demands in one jurisdiction to take down content so that it is inaccessible in other jurisdictions (e.g., globally)?

Firstly, companies should be consistent in order to have any chance of pushing back against any human rights restrictions. Google deindexes millions of URLs globally every week, on the basis of US copyright law, but is prepared to go to Court to avoid a similar obligation because it is opposed in principle to extra-territorial impact of the EU Costeja ruling. This position is not without merit but risks appearing contradictory in the wider context of Google's "voluntary" content restrictions.

As a general rule, companies should do everything they can to avoid extra-territorial effects of content restriction measures.

6. Appeals and remedies: How should companies enable users to appeal mistaken or

10 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0501+0+DOC+XML+V0//EN&language=EN

11 https://www.easydns.com/blog/2014/01/09/domains-locked-in-london-police-takedown-ordered-to-be-transferred/

European Digital Rights | 20 Rue Belliard, 1040 Brussels, Belgium | Tel. +32 2 274 25 70 | www.edri.org

inappropriate restrictions, takedowns or account suspensions? What grievance mechanisms or remedies do companies provide?

It seems reasonable to assume that there would be a chilling effect on users that are notified – or simply notice – that a decision has been taken that has already led to a restriction being imposed. Where this is possible, and as an absolute minimum, an easily accessible, well-explained predictable counter-notice procedure should be offered to individuals *before* the restriction has been imposed. When an ex-ante counter-notice procedure is not possible, an easily accessible, well-explained, predictable counter-notice procedure should be made available.

7. Automation and content moderation: What role does automation or algorithmic filtering play in regulating content? How should technology as well as human and other resources be employed to standardize content regulation on platforms?

This question is extremely broad and deserves a consultation process of its own. The answers depend on whether the content moderation is for commercial (such as copyright) issues, for minor breaches of the law, for serious criminality, for legal content that is prohibited by the platform in question, for content that is legal in some jurisdictions but illegal in others, etc. In relation to criminal content, further issues to be addressed are treatment of associated personal data, whether or not automatic reporting to law enforcement authorities should happen, transparency reporting in relation to such moderation decisions, etc. The risks of collateral damage for freedom of expression, for crime-fighting and transparency are vast.

8. Transparency:
a. Are users notified about content restrictions, takedowns, and account suspensions? Are they notified of the reasons for such action? Are they notified about the procedure they must follow to seek reversal of such action?
b. What information should companies disclose about how content regulation standards under their terms of service are interpreted and enforced? Is the transparency reporting they currently conduct sufficient?

We are not in possession of empirical data on this point. As a general point, it appears that, with regard to the largest providers at least, there is a welcome willingness to be transparent with regard to the number of government requests received and acted upon, but a distinct unwillingness to be transparent about "voluntary" restrictions. These restrictions are often "encouraged" by governments or state authorities, as in the Europol example above. Therefore, we conclude that transparency reporting is not sufficient.

9. Examples: Please share any examples of content regulation that raise freedom of expression concerns (e.g., account suspension or deactivation, post or video takedown, etc.), including as much detail as possible.

We recommend onlinecensorship.org for answers to this question. In addition, we recommend the Special Rapporteur to consult the chapter that EDRi's Executive Director Joe McNamee and EDRi's Senior Policy Advisor Maryant Fernández Pérez wrote in the book "Platform regulations: how platforms are regulated and how they regulate us", pp. 99-123.[12]

12 http://hdl.handle.net/10438/19402

European Digital Rights | 20 Rue Belliard, 1040 Brussels, Belgium | Tel. +32 2 274 25 70 | www.edri.org