

European Digital Rights' response to UN Special Rapporteur David Kaye's consultation on the Study on freedom of expression in the Telecommunications and Internet Access Sector

European Digital Rights ([EDRi](#)) is a not-for-profit association of [civil and human rights organisations](#) from across Europe and beyond. We defend rights and freedoms in the digital environment, including the right to privacy and the freedom to seek, receive and impart information.

EDRi welcomes the [public consultation](#) of UN Special Rapporteur on freedom of opinion and expression, David Kaye, on the Study on Telecommunications and Internet Access Sector and the promotion and protection of the right to freedom of opinion and expression. Our comments are a follow-up to our [submission](#) to the [previous consultation](#). In our response, we focus on the current EU and Member-States' regulation in the Telecommunications and Internet Access Sector and its impact on the right to freedom of opinion and expression and the right to privacy.

I. Internet Access Providers

a) suspension or restriction of access to websites or Internet and telecommunication networks:

The adoption of the [Regulation \(EU\) 2015/2120](#) represents a significant and exemplary set forward for the European Union. It is a step forward both for net neutrality and with regard to arbitrary blocking:

- [Net neutrality](#): The European Commission attempted to legislate to destroy net neutrality. Fortunately, the final outcome, in conjunction with the [guidelines](#) adopted by BEREC (the Body of European Regulators), creates solid, law-based protections for net neutrality and for the freedom to seek, receive and impart information. Nonetheless, the issue of price discrimination ("[zero-rating](#)") remains an open question that still needs to be addressed, despite some helpful clarifications from BEREC.

Sources: <https://edri.org/net-neutrality-wins-europe/>
<https://edri.org/net-neutrality-document-pool-2/>
https://edri.org/files/netneutrality/consultation_berec_edriresponse.pdf
https://edri.org/files/netneutrality/consultation_berec_edripolicyanalysis.pdf

Despite the good result, there is strong lobbying against the new EU rules through the implementation of 5G:

Sources: <https://edri.org/endorsement-5g-terrible-telecoms-providers-claim/>
<https://edri.org/telcos-commission-attack-net-neutrality-berecs-independence/>
<https://www.article19.org/join-the-debate.php/252/view/>

- Arbitrary interferences: While the original draft from the European Commission proposed open-ended "rights" to block content (in clear contravention of the ICCPR, ECHR and EU Charter of Fundamental Rights), the final text imposes a law-based approach to blocking of content. However, certain vested interests are lobbying the European Commission to try again to introduce opportunities for arbitrary interferences.

Sources: <https://edri.org/coe-study-blocking-content-respect-fundamental-rights/>
<https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>

b) provision or facilitation of access to consumer data:

We encourage the UN Special Rapporteur to consider several different elements:

- "National security": With regard to "national security", the lawlessness and unpredictability of state access to data remains prevalent. Courts repeatedly rule that state measures are unconstitutional or otherwise illegal, but this does not seem to deter governments from piling one illegal measure on top of another, in the apparent hope that the cost and time it takes to overturn the laws generates a degree of impunity.

We are also gravely concerned about the multiple efforts (at the Council of Europe, European Commission and Council, bilaterally among States and also among certain parts of industry) to reinvent the entire approach to cross-border access to personal data, with inadequate concern for appropriate safeguards for individuals' human rights.

Sources: <https://edri.org/council-data-retention-can-we-please-just-have-it-back/>
<https://edri.org/european-court-confirms-strict-safeguards-essential-data-retention/>
<https://edri.org/uks-mass-surveillance-law-being-rushed-through-legislative-process/>

- General data protection law: After several years of debate, the EU adopted its General Data Protection Regulation at the end of 2015. This establishes a good baseline, the over-generous "flexibilities" for exceptions in the public interest reasons notwithstanding.

Sources: <https://edri.org/gdpr-document-pool/>
<https://edri.org/analysis-flexibilities-gdpr/>

- Communications-specific data protection law: After adopting the original data protection Directive in 1995, the European institutions made the insightful decision to adopt legislation to "complement and particularise" data protection law in the electronic communications environment. This became known as the "ePrivacy Directive" and was reviewed in 2002 and 2009.

There are various solid reasons for having such legislation, including the need for specific legislation to defend confidentiality of communications, specific guidance on the application

of general data protection rules in the complex electronic communications environment and the need to address challenging issues such as online tracking and spam.

The European Commission is expected to announce its plans for a review in January 2017. This creates an important opportunity to, again, provide specific guidelines to help individuals and businesses understand their rights and obligations in the electronic communications environment. Faced with the security and privacy implications of the "internet of things" and all-pervasive online tracking, the review creates significant opportunities to protect privacy and freedom of communication online. It also creates an opportunity to address the fact that traditional telecommunications services (such as SMS, that is covered by the legislation) are being replaced by functionally identical services (Signal, Whatsapp, etc). However, there is a challenge - possibly unavoidable - that expanding the range of businesses covered by the Directive will make it easier to impose surveillance and access to data obligations to a wider range of companies. On the other hand, it seems unlikely that the absence of an extension of the scope of the Directive would prevent Member States from implementing such measures, so this privacy cost appears to be outweighed by more comprehensive rules. It also creates the opportunity to create new issues, such as access to consumer devices.

Sources: https://edri.org/files/epd-revision/EDRI_ePrivacyDir-final.pdf
<https://edri.org/epd-faq/>
<https://edri.org/epd-revision-analysis/>

II. Other ISPs:

- The "[Umbrella Agreement](#)" is an agreement between the European Union and the US with regards to the (minimum) data protection standards that must apply to data transfers between law enforcement authorities, [without authorising any data transfer](#). The agreement was signed on 2 June 2016, but the Council is seeking the consent of the European Parliament to finalise the process. The Article 29 Data Protection Working Party (WP29) has expressed concerns about this agreement from the beginning of the process (e.g. see [here](#) and [here](#)) and it has recently asked for further clarifications and assurances, as well as for information on its compliance with fundamental rights.

Sources:

http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20161026_statement_of_the_wp29_on_the_eu_umbrella_agreement_en.pdf
<https://www.accessnow.org/eu-council-greenlights-umbrella-agreement-parliament-hasnt-given-final-consent-yet/>

- "[Follow the money](#)": In line with the failed US legislative proposal, the "Stop Online Piracy Act" (SOPA), the European Commission is seeking to broaden the concept of "intermediary", to cover possibly any company that could be used to take punitive action against a perceived infringer of the so-called 'Intellectual Property Rights' (IPR). Also in line with SOPA, the

Commission is putting pressure on companies to "voluntarily" impose sanctions on online services accused of infringements.

Perhaps due to the fact that the issues are economic rather than societal, the approach is somewhat less chaotic than some of the Commission's other "voluntary" initiatives, such as the "hate speech" "code of conduct". However, the core problem is the outsourcing of law enforcement activities to private companies, with little transparency or accountability.

Sources: <https://edri.org/following-money-easy-to-say-hard-to-do/>
<https://edri.org/follow-money-following-some-positive-paths>
<https://edri.org/faq-code-conduct-illegal-hate-speech>
<https://edri.org/guide-code-conduct-hate-speech/>

- "Export controls": The European Commission has recently [proposed](#) rules on export controls of dual-use goods with the purpose of *inter alia* limiting the proliferation of surveillance and censorship technologies. It is important to push States for a strong human rights focus, explicitly considering human rights as one of the key constraints on trade in dual-use goods. At the same time, legitimate security research should not be restricted through updates in export controls.

Sources: <https://edri.org/commissions-proposal-new-regulation-dual-use-goods/>
https://edri.org/files/export_controls_edri.pdf