



AMNESTY INTERNATIONAL SUBMISSION TO THE EUROPEAN COMMISSION'S CONSULTATION ON THE DIGITAL SERVICES ACT PACKAGE

September 2020

Amnesty International welcomes the opportunity to provide feedback to the European Commission's Digital Services Act package. In this document, we outline key policy recommendations to guide the development of the Digital Services Act.

Amnesty International is a worldwide organisation committed to protecting human rights, including in the digital space. In our 2019 report "*Surveillance Giants: How the business model of Google and Facebook threatens human rights*",¹ we set out an analysis of the concentration of power in dominant online platforms, so-called 'gate keepers', and the impact of their surveillance-based business model on the exercise of human rights online.

BACKGROUND

The rise of social media and other online platforms has brought unprecedented global connectivity. Despite the real value of online platforms enabling human rights online, the services come at a serious human rights cost.² The increasing power of online platform companies has led to a systemic erosion of the right to privacy in the digital space, and corresponding impacts on a range of other rights including non-discrimination, freedom of expression and opinion, and freedom of thought. It has become virtually impossible for users to engage in the digital world without being subject to ubiquitous corporate surveillance and intrusive profiling. Such practices are only increasing in breadth and depth in parallel with the erosion of any meaningful alternatives. As with all systems of surveillance, this has disproportionate impacts on marginalised groups, and exacerbates existing structural inequalities.³

The impacts on human rights go hand in hand with the concentration of platform power generated, among others, by network and lock-in effects, increased entry barriers, leveraging dominance in one sector to increase dominance in another, downranking the services offered by would-be competitors, and buying-off competitors. These corporate practices are characteristic of the gatekeeper platforms, in particular Google and Facebook. This dominance is directly linked to the companies' surveillance-based model. This business model increases revenues by leveraging vast amounts of people's data to fuel algorithmic systems that shape and influence our information ecosystem and make predictions about our behaviour, primarily to derive profit through advertising.⁴ This incentivizes platforms to amplify extremist, racist, hateful, and 'fake' content to maximise users' attention and drive profits. In this environment, users lack meaningful control over their own data or options to 'opt-out' of this surveillance-dependent use of online platforms.

Additionally, the asymmetrical position of users vis-à-vis platform companies, and the inherently collective as well as individual nature of the harms, obstructs individuals from exercising their rights or obtaining effective remedy from adverse human rights impacts. Mass extraction, sharing, resharing, fusing and retaining of data creates a situation in which privacy breaches are difficult to undo.⁵ Even where data protection laws are implemented, their

¹ Amnesty International, *Surveillance Giants: How the business model of Google and Facebook threatens human rights*, 2019, <https://www.amnesty.org/en/documents/pol30/1404/2019/en/>

² Amnesty International, *Surveillance Giants*.

³ See for example Pratyusha Kalluri, co-creator of the Radical AI Network, *Don't ask if artificial intelligence is good or fair, ask how it shifts power*, in Nature, July 2020, <https://www.nature.com/articles/d41586-020-02003-2>; Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*, 2019

⁴ Amnesty International, *Surveillance Giants*; UK House of Commons, *Disinformation and 'fake news': Final Report*, 2019, <https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/1791/1791.pdf>; and Cohan Peter, "*Does Facebook Generate Over Half of Its Ad Revenue From Fake News?*", Forbes, November 25 2016, <https://www.forbes.com/sites/petercohan/2016/11/25/does-facebook-generate-over-half-its-revenue-from-fake-news/#e633dda375f5>.

⁵ OHCHR, *Right to Privacy in the Digital Age*, A/HRC/39/29, 2018, para 56

enforcement remains a challenge due to the opaque use of automated systems, lack of users' knowledge of their rights, financial costs, complex procedures and lack of adequate resourcing of data protection authorities.⁶

Any state regulation governing online content poses high risks of undermining freedom of opinion and expression and must be carefully crafted and implemented in line with human rights law and standards.⁷ It is therefore vital that future EU regulation addresses not only online content itself but also the root causes of the spread of disinformation and other harmful content – namely the dominance of the 'gatekeeper' platforms and their business models predicated on intrusive surveillance, profiling and manipulation at scale.⁸

RECOMMENDATIONS

Amnesty International presents the following key policy recommendations:

- 1. Ensure that access to online platforms and digital services is not made conditional upon surveillance, and enforce interoperability**

Amnesty International welcomes the Commission's focus on levelling the playing field and addressing the dominant role of gatekeeper platforms over the online environment. Platform companies such as Google and Facebook make their services conditional upon ubiquitous surveillance of their users, from search preferences to location tracking, which provide them extensive powers to exploit individual vulnerabilities.⁹ This is achieved by creating lock-in effects, which discourage users from selecting privacy-friendly alternatives to surveillance-based business models.

The dominance of the 'gatekeeper' platforms means in practice people have become reliant on their services to facilitate the enjoyment of rights such as freedom of expression, the rights of peaceful assembly and association.¹⁰ This has created a paradoxical situation where for people to exercise their rights in the digital age, they are forced to accede to a business model that inherently undermines their human rights. This false choice and its impact on people's rights was recently recognised by Germany's federal court in a ruling on Facebook and antitrust.¹¹

The Digital Services Act should affirm the principle that access to and use of essential digital services and infrastructure cannot be made conditional on ubiquitous surveillance and profiling. Platform companies must be prevented from making access to their service conditional on individuals "consenting" to the collection, processing or sharing of their data for marketing or advertising. Such practices are already contrary to requirements set out in the GDPR, and subject to ongoing legal challenge.¹² Moreover, the default must be for users to opt-in rather than opt-out of the use of behavioural data for targeted advertising and personalisation.

The Commission must also ensure that 'gatekeeper' platforms become interoperable with other internet services.¹³ Interoperability implemented at the EU-level would ensure that users can move between platforms without detrimental consequences, for example, to their ability to communicate with members of their networks. Decentralized social media platforms, which are created through interoperability requirements, promote privacy protection, non-discrimination, and freedom of expression by providing users with alternatives to surveillance.

⁶ Brave, *Europe's governments are failing the GDPR*, April 2020, <https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf>

⁷ UN Special Rapporteur on freedom of opinion and expression, *Online content regulation*, Report to the Human Rights Council, April 2018, A/HRC/38/35

⁸ Ranking Digital Rights, *It's the Business Model: How Big Tech's Profit Machine is Distorting the Public Sphere and Threatening Democracy*, 2020, <https://rankingdigitalrights.org/its-the-business-model/>

⁹ Amnesty International, *Surveillance Giants*.

¹⁰ "In the digital age, the exercise of the rights of peaceful assembly and association has become largely dependent on business enterprises, whose legal obligations, policies, technical standards, financial models and algorithms can affect these freedoms." Clément Nyaletsossi Voule, Special Rapporteur on the rights to freedom of peaceful assembly and of association,

¹¹ Natasha Lomas, TechCrunch, *Antitrust case against Facebook's 'super profiling' back on track after German federal court ruling*, 23 June 2020, <https://techcrunch.com/2020/06/23/antitrust-case-against-facebooks-super-profiling-back-on-track-after-german-federal-court-ruling/>

¹² noyb, *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook*, May 2018

¹³ Amnesty International, *Surveillance Giants*; La Quadrature du Net, *For the interoperability of the Web's Giants: An Open Letter from 70 organisations*, 14 June 2019, <https://www.laquadrature.net/en/2019/06/14/for-the-interoperability-of-the-webs-giants-an-open-letter-from-70-organisations/>; and EDRI, *Open letter demands interoperability of the big online platforms*, 03 July 2019, <https://edri.org/open-letter-demands-interoperability-of-the-big-online-platforms/>.

2. Legally require platform companies to carry out human rights due diligence to address systemic and widespread human rights impacts of their services, including through the use of algorithmic systems.

Governments should legally enforce the responsibility of companies to respect human rights, as set out in the UN Guiding Principles on Business and Human Rights.¹⁴ Platform companies should be mandated to carry out human rights due diligence to identify and address human rights impacts related to their operations, use of algorithmic decision-making, and business model as a whole. Introducing mandatory human rights due diligence for platform companies is consistent with efforts to introduce such measures for all business enterprises based in or active in the EU.¹⁵ Companies should take effective action to prevent and mitigate against human rights abuses and be transparent about their efforts in this regard (see point 3 below). In particular, platform companies must put in place measures to ensure that during the development and deployment of algorithmic systems, the algorithms do not disproportionately undermine the rights of any group in society, particularly marginalised communities.¹⁶

3. Improve transparency of online platforms' practices

A key priority for the Digital Services Act must be increasing transparency of online platforms, including the use of algorithmic systems, the use of (targeted) advertising, and content moderation practices. A range of internationally accepted standards on the accountability of companies and responsible business operations underline the importance of companies disclosing information that is necessary for stakeholders to understand the business's impact on human rights.¹⁷ Specifically, platforms that develop and implement algorithmic systems should disclose the process of identifying risks, the risks that have been identified, and the concrete steps taken to prevent and mitigate identified human rights risks. Users must be able to understand the ways in which algorithms shape their experiences online, including what criteria about their profiles and activities determines content and ads they see. This includes transparency about the parties involved in the funding and creating online advertising: who targets and why (i.e. explanation of criteria that resulted in the selection of ads).¹⁸

Amnesty International also supports calls by numerous other civil society organisations to enhance access to platform data for independent researchers, including journalists, academics and civil society.¹⁹

4. Establish external (third-party) auditing and oversight mechanisms to prevent abuse of power by 'gatekeeper' platforms and provide access to remedy

Given the opaque nature online algorithmic tools and the disproportionate power of online platforms, users are often powerless to confront decisions made by the companies or their algorithmic systems. Experience has shown that platforms cannot be left to self-regulate and implement sufficient human rights protections without independent regulatory oversight. The regulatory framework must address obstacles to effective remedy for people whose rights are impacted by the operations of platform companies – effective remedy must be seen as a central tenet of holding algorithmic systems to human rights standards, and not as an afterthought. This is particularly important for systems and practices implemented on a scale seen with the 'gatekeeper' platforms.

We agree with the European Parliament's Committee on the Internal Market and Consumer Protection that "pressing consumer protection concerns about profiling, targeting and personalised pricing cannot be addressed by transparency obligations and left to consumer choice alone."²⁰ Regulators must have powers to oversee companies' practices, including the application and impact of algorithmic systems, through mandatory third-party

¹⁴ UN Guiding Principles on Business and Human Rights, UN Doc HR/PUB/11/04, 2011, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

¹⁵ Business & Human Rights Resource Centre, *EU Commissioner for Justice commits to legislation on mandatory due diligence for companies*, April 2020, <https://www.business-humanrights.org/en/latest-news/eu-commissioner-for-justice-commits-to-legislation-on-mandatory-due-diligence-for-companies/>; Joint open letter signed by Amnesty International and ten other civil society organizations, *EU Mandatory Due Diligence Legislation To Promote Businesses' Respect For Human Rights And The Environment*, 1 September 2020, <https://www.amnesty.org/en/documents/ior60/2959/2020/en/>

¹⁶ Amnesty International and Access Now, *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems*, May 2018, <https://www.torontodeclaration.org/>

¹⁷ See for example, the UN Guiding Principles on Business and Human Rights, The OECD Guidelines on Multinational Enterprises, and EU Directive 2014/95/EU (the non-financial reporting directive).

¹⁸ Amnesty International, *Surveillance Giants*, p.32; and Panoptikon, *Who really targets you?*, 2020, <https://panoptikon.org/political-ads-report>.

¹⁹ See for example, Algorithm Watch, *The only way to hold Facebook, Google and others accountable: More access to platform data*, May 2020 <https://algorithmwatch.org/en/governing-platforms-studies-may-2020/>; Access Now, *Submission to the Consultation on the Roadmap for Digital Services Act*, July 2020

²⁰ European Parliament Committee on the Internal Market and Consumer Protection, 'Draft report with re-commendations to the Commission on Digital Services Act: Improving the functioning of the Single Market', PE648.474v02-00, 24 April 2020

audits. Platform companies should be held liable for human rights harms linked to their algorithmic systems or if they fail to carry out meaningful due diligence. Oversight bodies must also regularly engage in consultation and dialogue with relevant stakeholders, including civil society and representatives of marginalised groups.²¹ Finally, oversight bodies must be adequately resourced, independent and given enough authority to meaningfully hold powerful technology companies to account.

CONCLUSION

The Digital Services Act is a major opportunity to significantly curtail the surveillance-based business model of the dominant online platforms that day-by-day undermines privacy and other rights of users all around Europe and worldwide. The Commission must address the core issue of the business model and dominance of 'gatekeeper' platforms. It requires a careful act of balancing, wherein, on the one hand, users are provided greater control over their data and online experience, and on the other hand platforms are held accountable for their practices.

²¹ Council of Europe, *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*, April 2020, Preamble para. 5