March 2021

GLOBAL WITNESS: RECOMMENDATIONS FOR THE DIGITAL SERVICES ACT

About us: *Global Witness is an international advocacy organisation that investigates and challenges abuses of power to protect human rights and secure the future of the planet. We carry out hard-hitting investigations, expose the facts, and push for systemic change. Our campaigns have looked at issues ranging from blood diamonds - for which we were co-nominated for the Nobel Peace Prize in 2003 – to fighting money laundering and pushing for transparency reforms in the oil, gas and mining sectors. In 2020, we launched a new campaign on tackling digital threats to democracy. We have over 100 staff and offices in London, Washington DC and Brussels. We are independent and not-for-profit.*

Please find below an overview of Global Witness' recommendations for improving the proposed Digital Services Act, which include:

- **Online advertising**
- **Risk assessment and audit**
- **Algorithms**
- **Data access and scrutiny**
- **Other**

I. ONLINE ADVERTISING

Comments: We welcome the inclusion of ad transparency requirements in the DSA proposal. However, there are critical gaps in terms of the format, verification and level of detail of disclosure on online ads. The ad repositories, as required for Very Large Online Platforms (VLOPs), will take time and resources to set up. For this investment to be worthwhile, careful consideration needs to be given to whether the format and scope of information is conducive for effective scrutiny by a diverse set of stakeholders.

Article	Recommendation	Rationale / Evidence
Access and format		
30	**Repository access & format**: the data contained in the ad repository should be made available under a permissive open license and free of charge. In addition to access to the API, there should also be access via i) structured data releases such as spreadsheets ii) a web interface.	While APIs are useful for developers, they are not as useful and accessible for non-technical researchers. Ease of access to the data for a range of audiences is critical for ensuring the data is used.

24	**User access:** Online platforms should provide information on funding and targeting one click away from the ad itself (not just in an ad library).	Few users are going to regularly look at information in an ad library; the key information about an advert, including who funded it and how it was targeted should be more easily available to users.
24	**Individual ad libraries**: A user should be able to see all the ads they've been shown.	This will enable a user to have a deeper and more holistic understanding of how they are targeted with ads - a process which currently happens largely without users' awareness. It should also help users challenge unwanted targeting and to uphold their data protection rights.
34	**Interoperability:** Advertising repositories should be obliged to follow certain standards such that they are interoperable across platforms and member states, instead of this being a voluntary requirement.	By enabling interoperability between repositories this will enable deeper analysis of influence campaigns and cross-platform comparison. It is important to set these standards from the outset to avoid the need for retrofitting further down the line and further costs for platforms to comply. For example, the EU's 5th Anti-Money Laundering Directive required Member States to set up public registers of company owners, but only made interoperability a requirement after the initial deadline. As a result Member States have had widely varying approaches, making interoperability more complex and costly to organise.
30	**Unique identifiers:** Each ad and each advertiser should have a unique identifier and this should be published.	This will allow for trend analysis over time and scrutiny across platforms.
Targeting transparency		
24, 30	**Targeting**: Rather than limiting transparency only to the "main parameters of targeting", the text should be changed to ensure it covers the same level of granularity of targeting as chosen by the advertiser. This must cover all interest-based, demographic, and behavioural categories chosen, as well any exclusions used to refine targeting. Use of custom or any other audience tools must be disclosed, including the source of the custom audience (e.g. customer list, political party members, data bought from third parties such as data brokers), and the name of any data broker used.	By only requiring the "main parameters of targeting" this gives too much discretion to platforms to provide information which isn't meaningful and doesn't allow for proper scrutiny of the targeting applied. "Main parameters" could be interpreted as meaning the parameters which led to the largest number of people seeing the ad, which are likely to be geographic location or demography. More controversial targeting such as interest-based targeting could be hidden. This scrutiny is essential to detect rights breaches such as discrimination, aggressive advertising at vulnerable groups, and threats to democratic debate and elections. Given advertisers are able to choose targeting at a granular level, it is reasonable to require this same information to be disclosed publicly. With regard to custom audiences, this information is essential to identify and provide recourse for potential illegal datasets being used for ad targeting – including data which may have been illegally collated or collected via Real-Time Bidding processes. It would also bring more parity between on and offline

		advertising, as users may be totally unaware of their selection for an online audience, unlike ads in newspapers or flyers received through the door.
24, 30	**Ad optimisation:** There should be disclosure of all ad optimisation parameters used. This must include the optimisation goal selected by the advertiser and general information on the optimisation logic used by the platform.	It is not just advertisers who get to determine who does and does not see an advert via the targeting parameters they select. The platforms themselves may also determine who sees the advert through ad targeting and ad optimisation algorithms. Therefore the parameters of these algorithms should also be disclosed.
Targeting restriction		
24	**Ban targeting based on inferred and observed data:** Online platforms should present personalised advertising only on the basis of data explicitly and directly provided to them or declared by recipients of service AND provided that they have been granted consent for the use of this data, within the meaning of Article 4 (11) of the GDPR (Regulation EU 2016/679), for the purposes of delivering personalised advertising. As part of this, **lookalike audiences should be banned.**	The DSA should make explicit that personalised advertising is permitted as long as it only relies on data directly provided or declared by users (e.g. in their profile or data management settings). This would prohibit personalised advertising based on pervasive and systemic monitoring of user behaviour beyond their consent, while still enabling targeting based on consent. This creates a balance between the protection of users' fundamental rights, information autonomy and the needs of advertisers and online platforms. Users will have full control over how their data is used for advertising purposes. In addition, there are huge challenges for using lookalike audiences in a GDPR-compliant way.
24	**Automated withholding of consent**: Users should be able to communicate their decision to withhold consent for receiving personalised advertising via automated means. Online platforms shall respect this communication, including through the settings of dedicated software.	By enabling users to set up a "do not consent for personalised advertising" signal (e.g. via their browser) to be shared with platforms, this should lighten the burden on users to respond to consent requests, and limit the growing problem of consent fatigue. This provision builds on the GDPR's requirements for privacy by design and by default, as well as improving users' online experience.
24	*To consider: banning ad targeting based on Special Category Data (as defined by the GDPR)*	Special Category Data is by definition highly personal information which faces important conditions for its use under the GDPR. The DSA can play an important role in going further and giving advertisers legal certainty by removing the limited possibilities of using this type of information for ad targeting purposes. This will help level the playing field between advertisers and tackle pervasive illegal data practices. This measure would build on existing, albeit limited, self-regulation. For example, in response to litigation Facebook restricted ad targeting options for housing, credit and job ads in the US to address discrimination risks, removing targeting based on multi-cultural affinity.

User-level control & transparency		
24	**Transparency of consent:** Ads should display to the recipient: i) where they gave consent for their data to be used for this purpose by the advertiser; ii) where they can review and withdraw consent for their data to be used for this purpose; iii) the source/s of data about the recipient which were processed in order to target the recipient with the ad. Whether a custom audience is used should be disclosed. Information should be provided on the provenance of the data for custom audience (e.g. customer list, political party members, data bought from third parties such as data brokers), including the name of any data broker used. The ad should also disclose to the recipient the legal basis for processing this data under GDPR, as shared by the advertiser.	These amendments would give recipients a clear line of sight between the ad they are being shown and where they gave consent for their data to be collected and processed for that purpose. It would also allow them to understand the legal basis on which they are being shown the advertisement and facilitate their active consent to being profiled for that purpose as per the GDPR.
Verification & accountability		
24, 30	**Verification**: Ad information should be verified. Specifically there should be checks conducted by the platform regarding i) the person on whose behalf the ad is played, and ii) the funder. This should include requesting and verifying IDs (for natural persons) and company numbers (for companies).	Verification is necessary to ensure the information on ads can be trusted and advertisers can be held to account.
24, 30	**Advertiser registrations**: Advertisers should disclose details of relevant registrations with regulators (company registration or tax number, data protection registration, electoral commission registration).	This will help ensure avenues for advertiser accountability as well as enable cross-checking the veracity of the information provided.
Additional disclosure		
24, 30	**Sponsor**: Ad disclosures should cover both the sponsor who pays for the ad as well as the natural or legal person on whose behalf the ad is being displayed (which may not be the same person/entity).	Information on the sponsor of an ad is critical for public interest investigations - including consumer fraud, dark money in politics, amongst other issues.
24, 30	**Spend**: The exact spend for an ad should be disclosed.	Broad spend ranges do not provide meaningful information for users, researchers, or regulators

30	**Recipients**: there should be disclosure of the number of impressions an ad received broken down by gender, location, age.	This information will help for comparison between intended target groups and those who actually received the ad. It could also help identify discrimination via job, credit, housing or other ads.
30	**Engagement:** Provide non-personal information on the amount of engagements that an ad received, including user actions beyond viewing an ad (comments, likes, shares, reactions).	Information on engagement is important for studying the potential additional non-paid reach and polarising effects of specific content.
30 **(12)**	**Influencers:** Sponsored content from influencers should be disclosed in ad repositories. Platform's Terms and Conditions should specify transparency and accountability requirements for influencers.	Unless users who are paid to promote content are similarly required to self-identify and disclose information, this could provide an important loophole for advertisers who want to evade scrutiny.
30	**Historic data**: The timeframe for providing historic information on ads should be extended from 1 year to 10 years.	For the purpose of public interest investigations itis highly unsatisfactory to only include data from the past year.
30	**Audit trails:** the ad libraries should include clear audit trails for content which has been removed, including the reasoning for its removal while maintaining data on the advertiser, funder, spend, and targeting.	This will support public interest investigations into improper use of online ads, including disinformation and foreign interference campaigns and allow users and researchers to see how effectively platforms are implementing their policies
24	**Ad approval process:** Platforms should be required to provide detailed descriptions of their ad approval processes in their terms and conditions.	This is an important measure to ensure transparency of decision making and ad approval processes for all advertisers.

RISK ASSESSMENTS AND AUDITS

Comments: One of the central components of the DSA proposal is that VLOPs will have to identify significant systemic risks that their services pose. It is our view that the risks that have to be identified are too narrowly defined. VLOPs pose a risk to many fundamental rights, including protection of personal data, consumer protection and environmental protection.

Article	Recommendation	Rationale / Evidence
26	**Broaden risk assessments:** VLOPs should have to identify significant systemic risks stemming from the functioning and use of their services relating to: ● "any negative effects for the exercise of fundamental rights, **including** respect for private and family life, freedom of expression and information, the prohibition of	VLOPs can pose a risk to more fundamental rights than those listed in Article 26. For example: ● the way data is collected, bought and sold for targeting adverts poses a grave to risk to our right to protection of personal data

	discrimination, the rights of the child, **consumer protection, environmental protection and protection of personal data.”** ● “intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, **the climate system,** minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.”	● platforms that sell goods can undermine consumer rights by selling products that do not conform to EU standards and for which consumers may have no recourse. ● platforms that allow the spread of climate-related disinformation pose a risk to our right to environmental protection as well as commitments under international climate agreements (Paris Agreement, Art 3 UNFCCC).
33	As part of reporting requirements related to risk assessments, VLOPs must publish the **Data Protection Impact Assessments** they carry out as per Article 35 of the GDPR. The DPIA should, at minimum, include a description of the envisaged processing operations and the purpose of the processing; an assessment of the necessity and proportionality of the processing; an assessment of the risks to the rights and freedoms of data subjects; and the measures envisaged to address the risks and demonstrate compliance with GDPR. It is reasonable for VLOPs to redact elements of their DPIAs which relate to their legitimate interests (i.e. commercial sensitivity and security) and for the interests of any individuals.	Given VLOPs should already be carrying out these assessments under the GDPR, and their significance for understanding risks for the right to data protection in the processing of user profiles, it is both desirable and reasonable to have these assessments published.
33	VLOPs should have to **apply to the DSC for permission to redact information** from their risk assessments, risk mitigation measures, audit reports and audit implementation reports. If granted, VLOPs should have to include the statement of the reasons for removing the information in the report that is made public.	As the DSA is currently worded, VLOPs may redact information from any of the reports that are made public if the information “may result in the disclosure of confidential information of that platform or of the recipients of the service, may cause significant vulnerabilities for the security of its service, may undermine public security or may harm recipients.” All of these reasons are highly subjective. If a VLOP abuses this clause by redacting more information than is necessary, the DSA does not give powers to the DSC or the Commission to prevent this.
32	VLOPs should have to make public the **name of the person on the board** to whom the compliance officer reports	Naming a person on the board will help ensure accountability at the most senior level for compliance with the rules.

ALGORITHMS

Comments: It is our view that the DSA proposal does not allow for sufficient scrutiny or user control of the algorithms used by VLOPs. Such algorithms have the power to determine what we see online and how prominently we see it, including content that breaches our fundamental rights.

Article	Recommendation	Rationale / Evidence
54, 57	During **on-site inspections** the Commission and auditors or experts appointed by it may require the VLOP concerned or other persons referred to in Article 52(1) to: ● provide access to the data used to train any algorithms; ● provide information on what any algorithms are being optimized to do; and ● allow the on-site inspectors to conduct tests of how any of the algorithms work.	At present, the DSA only requires VLOPs to provide on-site inspectors with 'explanations' of their algorithms, and to answer questions about them. The Commission has the powers to order the platforms to provide access to its algorithms, but we assume that such access will not be routinely requested nor will it be granted to auditors or their experts. The way that platforms' content recommendation and ad distribution algorithms work has a significant potential to undermine fundamental rights, particularly around discrimination. Auditors and DSCs will require more evidence than the platforms' own explanations of how the algorithms work in order to hold them to account. In particular, they will require the ability to carry out 'black box' audits of the algorithms to quantify how they work. Such audits can be carried out without compromising platforms' trade secrets.
29	**Recommender systems** should have to make not being profiled the default option. In other words, users should have to opt in to profiling, not opt out.	Polling of European citizens shows that a large majority of people are deeply concerned about profiling. It should not be incumbent upon users to have to find the option of how to switch profiling off. With so many people using so many platforms, it is burdensome to expect people to have to do this.
29	Users should by default be given options to modify or influence the main parameters used by **recommendation systems.**	Users should always be able to modify the parameters of recommender systems, rather than only when the platform allows. This would increase users' choice, safety, and control over their experience.
29	The requirement to disclose information on **recommender systems** in platforms' Terms and Conditions should apply to all online platforms, not just VLOPs.	It is important to ensure basic transparency for users in all instances. In addition to disclosing the parameters used to recommend content (i.e. amplify or prioritise certain content), the platform should also reveal how the visibility of certain content or accounts is restricted – also known as "shadow bans".

29	When setting out the main parameters of a platform's **recommender systems** in their terms and conditions, this must include: ● how users' data and profile will be used to automate what they see; and ● the optimisation goal of each recommender system.	This specific information is needed to ensure the information on recommender systems is sufficiently detailed to allow for meaningful public scrutiny and for users to be able to exercise their informed consent

DATA ACCESS AND SCRUTINY

Comments: It is our view that the DSA proposal too narrowly restricts who is allowed access to data for the purpose of conducting research that contributes to the identification and understanding of systemic risks present on VLOPs. Broadening access to independent researchers, including investigative journalists and civil society organisations would better facilitate the detection of harms and enable scrutiny of platforms, their infrastructure and their efforts to mitigate risks, and allow for better informed public conversation about the social and personal risks posed by VLOPs.

Article	Recommendation	Rationale / Evidence
31	Independent researchers, including **investigative journalists and civil society organisations**, that can demonstrate a legitimate interest and meet the proposed standards (i.e. free from commercial interest, proven track record of expertise, and committed to data security and confidentiality) should be given access to data for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks. **Delegated acts** which establish the technical conditions for sharing data from VLOPs should be reviewed periodically to account for new types of data and data access.	This amendment would address the enormous information asymmetry between platforms and third parties, enabling scrutiny of the systemic risks, accountability for the mitigation efforts undertaken by platforms, and satisfy the public's interest in understanding the social and personal risks posed by VLOPs.

OTHER

Article	Recommendation	Rationale / Evidence
2	**Search engines** should come under the definition of an intermediary service.	Search engines such as Google pose a risk to the fundamental rights of Europeans including, for example, in the way that their ranking algorithms promote disinformation, hate speech and discrimination. It would be remiss to exclude them from this legislation.
37	The types of situations in which the Board can recommend the Commission to draw up **crisis**	At present, the DSA defines crisis situations as being "extraordinary circumstances

	protocols should be extended to include extraordinary threats to electoral processes. Rather than potentially involving Members States' authorities, civil society organisations and others in drawing up the crisis protocols, the Commission **should** do so as a matter of course.	affecting public security or public health". The threat that online platforms pose to elections and to democracy more generally has the potential to be severe enough that it warrants also being included as a possible crisis situation, as witnessed in the 2020 US Presidential election
34	The **voluntary industry standards on transmission of data between advertising intermediaries** should also include standards on data rights, including the provenance of the data, and the form of GDPR consent obtained.	
46	*For consideration: The **oversight of Digital Services Coordinators** should be strengthened such that, if a DSC of establishment fails to satisfactorily investigate breaches of the Act, then there is scope for the Board to investigate. At present, the Board may 'recommend' that the DSC of establishment investigates and subsequently the Commission may 'request' it does so.*	The DSA should learn from the difficulties experienced with enforcement of the GDPR, where Ireland, the member state with responsibility for overseeing Google, Facebook, Microsoft and Twitter, has a poor record of enforcement. If a DSC of establishment fails to satisfactorily investigate, then ultimately another body should have the right to investigate. The current system encourages a race to the bottom between member states competing to host big, powerful companies.