

Your response

Question	Your response
Question 1: How, and to what extent, are persons carrying out independent research into online safety related issues currently able to obtain information from providers of regulated services to inform their research?	Confidential? – N Global Witness is a non-profit organisation. We carry out investigations and advocacy to seek justice for those disproportionately affected by the climate crisis, and so that corporations respect the planet and human rights, governments protect and listen to their citizens, and the online world is free from misinformation and hate. Our Digital Threats to Democracy team works to hold companies and governments to account via campaigns and investigations to tackle the spread of division, hate and disinformation on digital platforms. We welcome Ofcom carrying out this consultation as access to information from providers of regulated services is essential to our independent investigations. We recognise that within the Online Safety Act, Ofcom has a narrow mandate on data access. We hope that our response helps Ofcom in developing ways to support researcher access. We also hope that this consultation can help demonstrate to the Government that where Ofcom is limited in what it can do, there is a strong case to revisit the legislation to expand Ofcom's mandate in this area. There are currently three main forms of barrier to accessing information from providers of regulated services. Technical barriers to access Independent researchers into online safety matters face increasing barriers to obtaining information from online platforms. Regarding access tools for programmatic access to open social media data, there is a move away from access, with the deprecation of key transparency tools such as Crowdtangle. Where platforms do have access tools, EU-based researchers enjoy greater levels of access than UK-based researchers. Financial barriers to access We make use of expensive commercial suppliers that provide us with access to data including from X, Facebook, Reddit & YouTube. Some of this data is restricted, such as Facebook data where we are limited to collecting data from public pages. Researchers can apply for free access under Article 40 of the DSA (see e.g. X DSA Researcher Application) but 'The applicant must meet the criteria defined in Article 40 Sections 8 & 12 to receive

Question	Your response
	access to public X data’ - otherwise a paid subscription is required. However, these criteria require that this research contributes to the detection, identification and understanding of systemic risks in the Union. This means that independent researchers and journalists face significant financial burdens in order to research systemic risks to users in the United Kingdom. Limitations on information types Access conversations are also focused primarily on API access to collect public user data from social media platforms (posts, comments, etc.). This also highlights the lack of effective routes to gain other kinds of information about how platforms operate, such as platform internal policies, risk assessment procedures, algorithmic design, without the platforms deciding to do so on their own.
Question 1a: What kinds of online safety research does the current level of access to information enable? • What type of independent researchers are carrying out research into online safety matters? • What topics/issues they are researching?	Confidential? – N Using commercial access via a third-party provider (which is unaffordable for many organisations) we have used data to expose: suspected bot-like accounts or coordinated behaviour; hate speech and harassment directed at politicians; the use of advertising services by banned users. However, this access is limited, which reduced the strength of the research, and requires a substantial financial investment which many CSOs are unable to make. We also employ manual methods to observe and test platform policies that protect human rights and election integrity by submitting adverts through their advertising portals. This does not require additional data collection via third party suppliers of APIs. This is small-scale, and thus we can test it using the platform’s regular interface. However, conducting more scaled tests – which would be more reliable – is not possible using this interface, and the platforms regularly challenge our results for this reason.
Question 1b: Are there types of information that independent researchers are currently unable to access that may be relevant to the study of online safety matters? If so, what are they and what kind of research would they facilitate?	Confidential? – N Without access to public data on social media data and accounts we cannot easily investigate threats to human rights, online safety, election integrity and climate disinformation.

Question	Your response
	Where platforms such as TikTok do have access tools, EU-based researchers enjoy greater levels of access than UK-based researchers. With access to TikTok's research API, civil society researchers based in the UK could make use of methodologies such as those developed by Italian researcher Fabio Giglittero which uses data collection via TikTok's research API to track coordinated activity on the platform. Another key focus for our research is looking at the way platforms monetize content that contains hate speech, election or climate disinformation. Recent changes to the source code of YouTube channels mean that researchers can no longer check if a page is monetized, even as Google lower the eligibility requirement for users to make money on their platform. Similarly platforms don't often give access to data from their monetization programmes making it difficult to know which content is creating revenue for both users and social media company.
Question 1c: What data governance models are currently used to allow access to online services' information for researchers? • This might include: open-access forms of information-sharing, such as publicly-accessible information libraries or databases; information-sharing models that rely on vetting or accreditation of individuals or organisations; and/or models that rely on the accreditation of the specific use cases for the information. • Please provide relevant examples of these governance models used in the online services industry.	Confidential? – N Meta's Ad Library API is the most successful example of a data governance model that provides relevant, publicly accessible data to independent researchers. Similar but less comprehensive services are offered by other platforms such as TikTok. Researchers using TikTok's ad library have reportedly encountered a number of issues including delays with showing data, lack of details for some ad types, and limited search parameters, which restrict its usefulness. Meta's CrowdTangle platform, which closed in 2024, was a good standard for publicly accessible information. Despite some issues around researcher vetting and data reliability, our researchers had previously used this to monitor public pages and groups, and viral posts online on Facebook and Instagram. Its replacement, the Meta Content Library is less transparent and accessible. The Twitter API (before restrictions were brought in during 2023) was a good model for information sharing by a platform but after the company introduced burdensome prices for using it, it is no longer accessible to most researchers and NGOs. Without API access, it is challenging to extract data from X.

Question	Your response
Question 1d: What technologies are typically used by providers of online services to facilitate existing information access?	Confidential? – Y / N
Question 1e: Have services and/or researchers made use of privacy-enhancing technologies to enable access?	Confidential? – Y / N

Question	Your response
Question 2: What are the challenges that currently constrain the sharing of information for the purpose of research into online safety related issues?	Confidential? – Y / N
Question 2a: What are the legal challenges/risks to sharing information from online services with independent researchers?	Confidential? – Y / N
Question 2b: What are the technical challenges relating to sharing information from online services with independent researchers? What are the challenges relating to the scale and complexity of the information involved?	Confidential? – Y / N
Question 2c: What are the security challenges relating to sharing information from online services with independent researchers? • What are the security challenges relating to the potential sensitivity of information? • What are the security protocols required to protect information from misuse?	Confidential? – Y / N

Question	Your response
To what extent do you view security as a governance issue compared to a technical infrastructure issue?	
Question 2d: What are the information quality challenges relating to online services sharing information with independent researchers?	Confidential? – Y / N
Question 2e: What are the financial costs to online services relating to online services sharing information with independent researchers?	Confidential? – Y / N
Question 2f: What are the financial costs to researcher trying to make use of information shared by online services?	Confidential? – Y / N

Question	Your response
Question 3: How might greater access to information for the purpose of research into online safety issues be achieved?	Confidential? – Y / N
Question 3a: What models, arrangements or frameworks exist for allowing researchers access to sensitive information beyond the online services industry? What are the benefits and risks of those models, and how might they apply to the online services context?	Confidential? – Y / N
Question 3b: Are there any models or arrangements that exist in the online services industry already that might provide increased access to information for research purposes if applied more generally across the industry? If so,	

Question	Your response
what are these and what are the benefits and disadvantages of these models/arrangements?	
Question 3c: What are some possible models for providing researchers with access to relevant information that may not exist or be widely used yet, but which might be implemented by industry?	Confidential? – Y / N
Question 3d: What are the advantages and disadvantages of this approach? • These may include elements pertaining to financial, legal, security, technical or feasibility issues	Confidential? – Y / N
Question 3e: What role could third party organisations, such as regulatory bodies, civil society or public sector organisations have in facilitating researcher access to online safety information?	Confidential? – Y / N
Question 3f: What could these third-party models look like, and what are some of the benefits and challenges associated with this approach?	Confidential? – Y / N
Question 3g: What categories of information should online service providers give researchers access for the study of online safety matters? Why would this information be valuable for the study of online safety matters?	Confidential? – N Generally our research is based on publicly available data such as public posts on social media platforms. However, often the purpose of studying this data is to try to infer information about the operation of platforms, given their opacity about how their systems and processes work. Being able to audit this information directly would increase the efficacy of this research. Such information would include, for instance: internal versions of content moderation policies or content moderation guidelines given to moderators; full risk assessments; details of how algorithmic systems are developed and tested.

Question	Your response
	Having a framework to facilitate access to stores of data, including user posts or adverts, which have been removed for violating platform policies, would also enable more accurate and effective research. This would help investigate questions around the accuracy of platform's moderation systems, and how online harms of different kinds are evolving on the platform. Currently, once data is deleted by a platform, unless it has been archived, this can no longer be accessed by researchers, meaning we often have to take platforms' word for how effective their systems are. It also means that we are unable to assess things like the details of how ads which violate platforms terms have been targeted, which would be valuable in understanding the methods and tactics of disinformation actors. Previously, platforms including Twitter would publish datasets that they had attributed to an influence network that researchers could then analyse to better understand how foreign interference and manipulation is conducted. These kinds of transparency were extremely valuable.