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?	The status quo leaves very few avenues for researchers to obtain information from providers of regulated services to inform their research. Since the OSA received Royal Assent, the situation regarding access to data has become markedly worse. ● Meta's announcement in August 2024 that it was shutting Crowdtangle was a significant blow to the online safety research community. In light of the UK election in July and the Southport riots in August, the consequence is that in future there will be less research on Meta's platform responses to such incidents. ● Despite its research API long being a high watermark for the research community, X's decided to restrict access to its research API which had previously been free. The astronomical prices that are now being charged immediately price out most public interest researchers. ● In 2024, further news that TikTok's "Creative Center" was prohibiting searches of hashtags and trending videos demonstrates that the environment for online safety researchers has been deteriorating despite the introduction of regulation. One of the few remaining avenues available to researchers in order to gain information from regulated services is research partnerships. The most well known version of this was the ill-fated 'Social Science One' partnership which was marred in scandal. Notably, "Facebook provided a data set to a consortium of social scientists last year that had serious errors, affecting the findings in an unknown number of academic papers, the company acknowledged." Many have argued that Social Science One represents a 'systemic failure.' Furthermore, the terms of service of all major regulated services expressly prohibit the type of data collection required to conduct worthwhile online safety research. As a result open source intelligence research (OSINT) is one of the only viable data collection methods currently available to independent researchers but this is a.) labour intensive b.) expensive c.) almost impossible to scale. The limited and deteriorating scope of information sharing and online safety research has a number of consequences for the research field: ● Research that *is* conducted is less rigorous, scalable and replicable ● It is harder for academia and civil society to attract and retain research talent due to the diminishing opportunities for high quality research ● It is harder for the research community to standardise and replicate research outputs

	Crucially, the regime in the UK must account for the following: 1. When left to their own devices, regulated services have demonstrated they are not interested in providing data to public interest and online safety researchers. Of particular note, is when researchers' findings are perceived to reflect adversely on the reputation of a regulated service. 2. Article 40 of the Digital Services Act and the related delegated Acts have set-out how this can work in practice. As a result, the UK has a second mover advantage and can learn from other jurisdictions how best to design and implement such a regime. 3. Civil society and academic research are complementary and both offer different strengths. Any future framework that enables access or accredits researchers needs to account for the distinct needs, complexity and offerings of both communities. For a UK data access regime to be successful, we need online safety researchers from academia and civil society. Research will contribute to a greater ecosystem of transparency which helps better inform policymaking by legislators and the work done by Ofcom.

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?	Examples of independent researchers carrying out research into online safety matters are: ● Victims groups (VAWG, anti-racism, anti-hate) seeking to document the lived experience of different communities experiencing online harm ● Civil society groups focused on the impact social media is having on democratic integrity ● Children and young people charities seeking to improve their online experience and prevent harm ● Safety tech sector, seeking to understand how better services might protect users online Examples of topics/issues they are researching include, but are not limited to: ● The promotion of harmful content (eating disorders, pro-suicide content, illegal content, content harmful to children) ● The efficacy of ad libraries or so-called 'transparency centres' – do these services actually deliver what platforms claim (normally they are insufficient, unreliable and censored) ● Ad experiments to test whether platforms are upholding their own terms of service for advertisers using their platforms ● Terms of service violations which demonstrate that platforms are not upholding their contractual obligations to users, ie they are not doing what they say they do ● Examining the proliferation of coordinated inauthentic behaviour (CIB) and foreign interference (FIMI) material on regulated services ● Exploring how democratic processes, integrity and elections are affected or undermined by hostile actors using regulated services

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?	A robust, mandatory data access regime for accredited independent researchers would facilitate the type of research outlined above (1a) but in a standardised, more rigorous and replicable way. It would make it easier for the UK research community to retain and attract talent, while giving Ofcom and DSIT a better evidence record they could use to inform decision making. At a high level, researchers need access to: ● Full, usable databases on specific research topics which can be used for experiments and analysis ● Data relating to systems and design choices made by regulated services and the trade offs these choices have on user experience ● Data relating to the use of AI, filters and content moderation ● Critically, data must be well labelled, organised and formatted in order for it to be practically used by the research community via queries. ● Data must be delivered in a timeous manner
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.	● As previously highlighted, public and accredited research APIs have been used as a way for regulated services to share information with researchers in the past. ● The European Digital Media Observatory has done extensive work looking into the mechanics of *how* and *who* data access should be granted under Article 40 of the Digital Services Act. The related 'Delegated Regulation on data access provided for in the Digital Services Act' also provides a useful roadmap with examples of proposed data governance models. ● Many accreditation systems already exist in academia for the processing of sensitive data. These models should be considered, but will need careful modification to ensure they are inclusive of civil society's needs.

Question 1d: What technologies are typically used by providers of online services to facilitate existing information access?	● Research APIs ● Raw datasets ● Research 'partnerships' ● Searchable databases (although often flawed)

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?	● As outlined extensively above, this is an academic question given the scarcity of data and lack of avenues for access.
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?	The key technical challenges relating to sharing information from online services with independent researchers are: ● Data storage and processing is resource intensive ● Data must be stored safely in a privacy-preserving way ● The scale of the data to be shared, if not appropriately formatted, is basically unlimited. The regime should be sure not to allow platforms to flood independent researchers with datasets that are so vast they are unusable. ● In order for data to be used by independent researchers it has to be structured and classified. Researchers have no use nor interest for ALL data produced and held by regulated services. They are simply looking to access specific buckets that relate to system and design choices, user experience, amplification and other specific areas of interest.
Question 2d: What are the information quality challenges relating to online services sharing information with independent researchers?	As stated above, while the status quo results in an acute shortage of data the inverse could also be a problem: too much data that is not properly formatted or labelled would overwhelm researchers to the extent that it would be unusable. It should not be discounted that platforms may choose to do this as a deliberate tactic to further obfuscate research being conducted on their platforms. Similarly, when data is shared but crucial elements are either redacted or censored it can be hard for researchers to use. A future access to data regime should be designed to ensure that researchers are able to make specific data queries, for specific research projects which are then transferred from regulated services.

Question	Your response
Question 2e: What are the financial costs to online services relating to online services sharing information with independent researchers?	The financial costs to online services relating to sharing information with independent researchers is minuscule. For example, Meta's revenue in 2023 was $134.9 billion. Regulated services represent some of the wealthiest companies in history. Ultimately, a robust ecosystem of transparency and research will result in making platforms safer, better for users and consequently more attractive to advertisers (the source of platform revenue). In short, it will be good for share prices and business. As has been widely reported, over the past 2-3 years platforms have fired significant proportions of their 'trust and safety' teams which has left vulnerabilities in their ability to comply with laws like the OSA, but presumably has also resulted in increased profits.
Question 2f: What are the financial costs to researcher trying to make use of information shared by online services?	The financial costs to researchers trying to make use of information shared by online services is significant, particularly in light of resource scarcity in the research community. Significant cost points for researchers include: ● Staff (including competing with tech companies on compensation to attract talent) ● Secure and privacy respecting cloud storage services ● Accreditations (for example, X's research API now starts at $42,000/month) ● Legal costs associated with risk assessments and dealing with litigious platforms ● Robust data processing infrastructure

Question	Your response
Question 3: How might greater access to information for the purpose of research into online safety issues be achieved?	While Ofcom's report into researcher's access to data is a welcome step, ultimately the regulator currently does not have the statutory power to facilitate or mandate such access. HMG needs to legislate to provide such provisions. We are heartened by HMG's amendments to the Data (Use and Access) Bill which indicate an understanding that the status quo is untenable. However, we would like to see these provisions made more robust by: 1. Ensuring Ofcom has the power to mandate the transfer of specific information requested by independent, accredited researchers 2. Allowing Ofcom to levy remedial action or fines against regulated services that do not facilitate the transfer of information to researchers 3. Providing safe harbour protections for researchers engaged in online safety research in the public interest. Specifically, these protections should protect academics and civil society organisations from falling victim to nefarious litigations by platforms. 4. Enable researcher's access to data to study online safety matters relating to UK users regardless of where a researcher is located (in line with the DSA). Without the aforementioned provisions and protections, the UK is at risk of creating a narrow opening for access to data that is not fully exploited by the research community due to the chilling effect of recent actions by platforms.
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?	Every other multi-trillion pound industry has its own version of independent research and verification, whereby data is securely shared with accredited experts. Pharmaceuticals, oil and gas, automobile manufacturers, water safety and pollution. All of these sectors have independent researchers able to verify whether they are doing what they say they are. Another parallel example is economic researchers who conduct research based on stock prices, company management and board movements.

Question	Your response
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?	There is potentially a significant role for regulatory bodies and public sector organisations to play in facilitating data access to researchers. For example, Ofcom or UKRI could act as the accreditation body which vets independent researchers for suitability to gain access to information from regulated services. Civil society needs to have a seat at the table when it comes to accessing information from regulated services. As a sector, it has proven to be the canary in the coalmine over the past decade and a half, alerting governments and regulators about the emerging threats and harms to users. In order to continue to play that role, special dispensations need to be made to ensure that any accreditation process does not disqualify or disadvantage groups that have done the sort of groundbreaking research that government and media have relied on.
Question 3e: 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?	Key categories of information which should be provided by online service providers for research purposes include, but are not limited to: ● Reach, virality and engagement of posts ● How system and product changes affect reach, virality and engagement of posts ● Key metrics measured by platforms ● Proliferation of comments on posts ● Comparative data on virality and engagement based o