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?	N/A
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 The current level of access to information enables a range of online safety research, though this research is often limited by the availability and quality of data. Independent researchers, including those from academic institutions, non-profit organisations, and think tanks, work on a variety of topics that align with the objectives of the Online Safety Act (OSA). These include, for example, harms to children, the societal impacts of social media, violence against women and girls (VAWG), safety by design, and harmful and illegal content.[1] These works use a variety of qualitative and quantitative techniques to develop new insights and safety tools, including ones designed to filter offensive and illegal content and detect grooming attempts. The relationship between researchers and platforms is asymmetrical, with researchers often facing challenges in accessing comprehensive and timely data. While the work currently being done is informing the development of evidence-based strategies to enhance online safety, improvements to data access would allow this to occur at a far more rapid pace.

[1] For example, see:
Fethi Fkih (2023). Threat Modelling and Detection Using Semantic Network for Improving Social Media Safety. International Journal of Computer Network and Information Security available online here
Ying Chen, Sencun Zhu, Yilu Zhou, and Heng Xu (2012). Detecting Offensive Language in Social Media to Protect Adolescent Online Safety. IEEE. available online here
Shiza Ali (2024). Youth, Social Media, and Online Safety: A Holistic Approach Towards Detecting and Mitigating Risks in Online Conversations. Boston University. available online here
Janneke van de Loo, Guy De Pauw, and Walter Daelemans (2016). Text-Based Age and Gender Prediction for Online Safety Monitoring. International Journal of Cyber-Security and Digital Forensics available online here

Question	Your response
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 Greater access to internal documentation, algorithm audits, and detailed user journey data would enable researchers to conduct more comprehensive and impactful studies, ultimately leading to better-informed strategies for enhancing online safety. Independent researchers currently face significant challenges in accessing certain types of information that are crucial for the study of online safety matters. A major gap is the current inability to comprehensively quantify online harms; greater access to platform data would allow researchers to triangulate against other sources of data and build a better understanding of the scale of these harms. Limited access to data and information contextualising this data makes it particularly difficult for researchers to quantify more context-dependent online harms, such as cyberbullying, misinformation, and hate speech. Researchers often lack access to the internal documentation and research held by platforms which would provide valuable insights into the platforms' current knowledge of harms and the effectiveness of their safety measures against these. Arturo Béjar's whistleblowing at Meta revealed that the platform is aware of significant online harms, such as bullying and unwanted sexual advances, particularly affecting teenagers, but has not been transparent about these issues.[2] Simply knowing what research a given company is undertaking, and on which topics, gives independent researchers much-needed context for the online environment they operate in. Having additional context provided alongside data would allow researchers to better understand the reasoning underpinning design decisions, and therefore better interpret the data that is provided to them. Researchers are currently unable to audit algorithms and processes to understand how these systems work and identify potential biases or flaws. This information would allow researchers to identify how algorithms influence user behaviour and spread harmful content and assess the extent to which platforms are complying with Ofcom's regulatory efforts. The data that researchers are currently provided with is often aggregated. Researchers need access to more detailed user journey data to analyse how users interact with platforms and identify points where safety interventions could be most effective. This would facilitate greater research into user behaviour, the spread of harmful content, and the impact of platform design on user safety.

[2] Associated Press (2023). Ex-Meta employee says his warnings of Instagram's harm to teens was ignored. The Guardian. available online here

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

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? – N The sharing of information for research into online safety related issues faces a number of significant challenges. Small to medium sized platforms may argue that providing data to researcher imposes an unreasonable burden on their business operations. This makes it difficult for researchers to investigate small-but-risky sites. At the opposite end of the scale, large platforms are able to create a hostile legal environment for researchers. Companies including Meta and X have taken legal action against researchers.[3] They may also cite commercial sensitivity to avoid granting access to data. These platforms may delay responses, refuse requests, or provide only partial data – all of which complicate the research process. While it is essential to consider what is feasible for services to deliver, it is equally important to recognise the potential value of this data for safeguarding children and young people. The decision of what data is made available lies with the platforms, and researchers often do not know precisely what data is being collected. This lack of transparency undermines research, as researchers may not be able to establish what data can be asked for; this environment effectively allows large technology companies to influence the direction of research, reducing the impact of this body of research and prejudicing the information available to the regulator. Securing data access and transfer is both technically challenging and financially burdensome for external researchers. The datasets involved in this form of research are often vast in scale and extremely complex, requiring significant resources to manage and analyse. Furthermore, different online service providers use non-interoperable or non-standardised systems, which further complicates the process of data sharing and comparison. There are barriers and complications associated with every method of data access for researchers at present. These include: • Data scraping involves using automated tools to extract publicly available data from websites. This can be legally and ethically challenging as it often violates the terms of service of the platforms. • APIs allow developers to access certain types of data, such as user posts, comments, and analytics, in compliance with the platform's terms of service. This access is often limited and is controlled by the platform, who may additionally charge for access. • Direct data requests involve formally requesting data from the platform, via formal channels and partnerships. As with API access, data access via this route is often limited and is controlled by the platform.[4] • Data donation is when users voluntarily share their data with researchers. Platforms may facilitate this by providing tools for users to download their data and share it securely. This approach is highly labour-intensive, and data

Question	Your response
	quality may be compromised as participants might change their behaviour if they know they are being observed.
Question 2a: What are the legal challenges/risks to sharing information from online services with independent researchers?	N/A
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?	N/A
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? ● To what extent do you view security as a governance issue compared to a technical infrastructure issue?	N/A

[3] Chris Vallance (2023). X Corp sues anti-hate campaigners over Twitter research. BBC News available online here
Thomas Claburn (2024). Meta accused of trying to discredit ad researchers. The Register. available online here
Victoria Elliott (2024). A Lawsuit Argues Meta is Required by Law to Let You Control Your Own Feed. WIRED. available online here
[4] University of Bath (2023). Study warns API restrictions by social media platforms threaten research. available online here

Question	Your response
Question 2d: What are the information quality challenges relating to online services sharing information with independent researchers?	Confidential? – N Platforms primarily collect data for commercial purposes, which may not align with the needs of independent researchers. Independent researchers are often less familiar with the limitations of the commercial data provided, which further complicates analysis. For example, researchers need to be able to contextualise any changes or tests that the platform was conducting during the period for which the data is provided. Where data is outdated or fragmented in this way, it is difficult to draw accurate conclusions. To rectify this, an audit of the datasets held by large online platforms would be beneficial. Such an audit would help external actors to understand what data exists, and hence how it can best be used to facilitate online safety research. Data sharing is further challenged by the physical infrastructure necessary for processing. This may include data centres, high-speed networking, and strong security measures, all of which are costly and resource-intensive to develop and maintain. Managing and integrating various systems, ensuring data security, and handling large volumes of data cause further complexities. Having insufficient infrastructure in place leads to barriers to data sharing; high-quality data is often more resource-intensive to transfer, and so infrastructure limitations can lead to a reduction in the quality of information available for research.
Question 2e: What are the financial costs to online services relating to online services sharing information with independent researchers?	N/A

Question	Your response
Question 2f: What are the financial costs to researcher trying to make use of information shared by online services?	Confidential? – N The financial costs to researchers trying to make use of data held by online services are significant. Large platforms, including X and Reddit, charge for API access to their data. For example, X has three tiers of charges: $100/month, $5000/month, and $42,000/month.[5] If a researcher wishes to challenge a decision made by a platform to provide partial or no data in response to a request, they may be able to appeal via legal or regulatory processes, but there are costs and delays associated with these, and no guarantee of success. Researchers also face financial risks relating to potential legal action if they engage in data scraping that violates the platforms' Terms of Service. Additionally, the computational resources, data analysis tools, and expertise required for such research is expensive. Given that independent, civil society, and academic researchers already operate with limited resources, the onus should be on companies to facilitate data sharing and bear the associated costs, rather than placing this burden on researchers.

[5] X's documentation on their API access is available online here

Question	Your response
Question 3: How might greater access to information for the purpose of research into online safety issues be achieved?	Confidential? – N Greater access to information for research into online safety issues can be achieved through several key measures. First, establishing infrastructure to coordinate academic and civil society data requests is essential, and will improve the situation for all parties. Coordinated data requests reduce the burden on platforms, as there will be fewer duplicated or very similar requests, while also streamlining the data access process for researchers. There should also be mechanisms to foster greater collaboration between researchers and platforms. For example, the audit of datasets currently held by platforms, described above, could contribute to a more collaborative research environment. This could additionally be facilitated by clearer legal and ethical frameworks which would reduce friction in the data access process. The creation of these frameworks should be informed or even led by partners who are experienced in this field, such as UK Research and Innovation, to ensure that data sharing is conducted responsibly. Additionally, providing financial and resource support for data sharing initiatives is crucial, as third sector and academic researchers often have limited resources. The broadest possible amount of data should be available for research purposes. This should include user interaction data, content moderation logs, and metadata that can help contextualise user behaviour and platform changes. Going forwards, it is important that proportionality should consider not just what is feasible for services to deliver, but also the potential value this information will offer for safeguarding children – if the information could have a significant impact on strengthening protections, then it is proportionate and necessary to request it. The definition of an 'independent researcher' should likewise be kept as broad as possible, to ensure that valuable research is not blocked and to further guard against regulatory capture. Thorough and collaborative vetting of researchers (please see our response to question 3e) will then be necessary to ensure the quality of research produced, while additionally ensuring that valuable research is not unnecessary blocked. To facilitate research, as far as possible data should be formatted in a standardised and interoperable way, in order to ensure that it is straightforward to analyse and appropriately contextualised. This said, in efforts to make this data more accessible, it is important breadth and depth of information is not lost in the name of standardisation. The more high-quality data that researchers have access to, the more high-quality research they will be able to produce.

Question	Your response
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?	N/A
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, what are these and what are the benefits and disadvantages of these models/arrangements?	N/A
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?	N/A
Question 3d: What are the advantages and disadvantages of this approach? ● These may include elements pertaining to financial, legal, security, technical or feasibility issues	N/A

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?	Confidential? – N Third-party organisations, such as regulatory bodies, civil society, and public sector organisations can play a crucial role in facilitating researcher access to online safety related information. Researchers who wish to access data will need to be vetted; while the platforms may suggest that they can perform this vetting, an independent third party or single authority will be necessary to ensure impartiality, consistency, and avoid conflicts of interest in order to maintain trust in the research process. Representatives from the regulator, the public sector, and the third sector could come together to perform this vetting in a way that maintains trust for all parties. Ofcom, for example, could play a significant role in evaluating the efficacy of data access systems and ensuring that different services comply with regulations. Civil society organisations may act as independent researchers themselves. This will allow them to – together with other researchers – feedback on their experiences of how well data access systems are working. Civil society organisations could additionally have an important role to play as mediators, providing a third perspective on research and helping to balance the interests of researchers and platforms; given their own experience with research, they will be able to mediate from a knowledgeable position. Having a robust, transparent mediation process in place will further build trust in the process. Third party organisations could additionally come together to consider the best approaches to the challenges that a researcher data access regime will produce. They will need to consider how best to ensure the security and privacy of the data, managing the logistics of data sharing, and maintaining the necessary infrastructure. Clear guidelines and standards for data access and use will need to be set out, and these will further require ongoing oversight and evaluation.
Question 3f: What could these third-party models look like, and what are some of the benefits and challenges associated with this approach?	N/A

Question	Your response
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 Online service providers should give researchers access to several key categories of information in order for them to study online safety matters effectively. Our response is not an exhaustive list of changes that need to be made but rather aims to illustrate some key changes that would be helpful. First, extensive data on existing online harms is crucial to understand their causes and develop mitigation strategies. For example, platforms hold usage data which shows how users are interacting with the service, content data which includes content created and shared by users, and tracking data of users' preferences. All of this can be used to investigate user's experiences, and hence their experiences of harms.[6] There is also a significant evidence gap around algorithmic profiling and content amplification, necessitating access to both the relevant user data and to the algorithms themselves. This information will allow researchers to identify how algorithms influence user behaviour and spread harmful content. The data provided by companies should be as comprehensive as possible, with platforms interpreting requests broadly, rather than narrowly as they do at present. This should include providing contextual information for decisions, such as product design notes and meeting notes, to help researchers understand the reasoning behind design choices. In terms of format, data should be clear and accessible. For online harms to children to be thoroughly researched, user data should be broken down where possible and appropriate to provide greater detail on who is most impacted by these harms. For example, breakdowns of data by age and gender will aid researchers in understanding how platforms are complying with Ofcom's age-appropriate design codes and allow them to investigate the specific impacts of design choices on children, ensuring the proper contextualisation of data. Improving independent researcher's access to data is vital. It will lead to tangible positive outcomes, including stronger safety governance, increased transparency, and greater user trust. Access to a broad range of data enables researchers to develop evidence-based recommendations for improving platform safety, ultimately resulting in services designed with user safety in mind. This aligns with Ofcom's online safety objectives and will promote a safer and more trustworthy online environment for all users.

[6] Examples of this research include:
Fethi Fkih (2023). Threat Modelling and Detection Using Semantic Network for Improving Social Media Safety. International Journal of Computer Network and Information Security available online here
Ying Chen, Sencun Zhu, Yilu Zhou, and Heng Xu (2012). Detecting Offensive Language in Social Media to Protect Adolescent Online Safety. IEEE. available online here
Shiza Ali (2024). Youth, Social Media, and Online Safety: A Holistic Approach Towards Detecting and Mitigating Risks in Online Conversations. Boston University. available online here

Janneke van de Loo, Guy De Pauw, and Walter Daelemans (2016). Text-Based Age and Gender Prediction for Online Safety Monitoring. International Journal of Cyber-Security and Digital Forensics available online here