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 The ability of independent researchers to obtain information from providers of regulated online services is highly variable and, on the whole, inadequate. The current situation can be characterised as "hit and miss," heavily contingent on the specific platform and the nature of the data sought. Over the past few years, there has been a noticeable decline in the availability of legitimate avenues for researchers to access data. Platform mechanisms that previously facilitated research, such as CrowdTangle, APIs, and firehose access, have become increasingly restricted or discontinued. This trend has forced researchers to operate in a precarious environment where they risk violating Terms of Service agreements to conduct essential research. The current landscape is one of obstruction and, at times, the use of legal avenues by platform providers to prevent access.
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?	Nil response - the ODI does not have relevant experience to contribute to this question.
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 Yes, several critical categories of information are largely inaccessible to independent researchers, hindering a comprehensive understanding of online safety issues. These include: ● Comprehensive data on the prevalence and types of online harms: Granular, unbiased data on the prevalence, nature and types of harms occurring on platforms is essential for understanding the scale and specifics of the issues. ● Data related to the efficacy of safety algorithms and processes: Independent researchers are largely unable to audit platform safety algorithms and content moderation processes effectively. This is due to the unavailability of removed content for examining false positives and the lack of effective methods to discover content that should have been removed (false negatives). This data would enable external validation of platform claims regarding safety and the effectiveness of their interventions. ● Internal platform documentation and research: Access to internal documentation, research findings, and data held by platforms themselves would provide invaluable insights into the platforms' understanding of online harms, their internal efforts to address them, and the challenges they face. It would be particularly useful for researchers to have to access internal AI policies to better understand how organisations deploy AI, including what is permitted and what is not, especially for activities such as content moderation.

	• Real-time data: Particularly important for research on current events like elections or public crises, real-time data is mostly unavailable to external researchers. • Supply chain transparency: Many content moderation activities are outsourced to third-party companies (often in other jurisdictions). It is not always possible to identify who these companies are, or the activities that take place.
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 Current data governance models employed to grant researchers access to online services' information are varied but often inadequate. Some platforms offer limited access through: • Publicly accessible information libraries or databases: However, these often lack the granularity and depth required for comprehensive research, and the quality of the data is often not sustained. • Vetting or accreditation of individuals or organisations: Some platforms employ vetting processes, but these can be opaque, inconsistent, and may not adequately address the needs of independent researchers. • Accreditation of specific use cases: This model can be overly restrictive, limiting research to pre-approved topics and potentially hindering exploratory research. Examples from the online services industry are limited, and where they exist, they often fall short of providing meaningful access. Furthermore, the ODI's research highlights the lack of clarity surrounding the definition of "public data" as a significant barrier to research. This ambiguity is sometimes exploited by platforms to limit access, creating legal and ethical uncertainties for researchers. Initiatives like the proposed Delphi survey by the ODI aim to address this by fostering consensus on what constitutes "public data" and establishing guidelines for its ethical use. This could become a potential future data governance model, complementing existing models such as those based on vetting and accreditation.
Question 1d: What technologies are typically used by providers of online services to facilitate existing information access?	Confidential? N The technologies used to facilitate information access are often rudimentary or intentionally obstructive. Some common approaches include: • Single sign-on (SSO): While SSO can streamline access, it can also be used to control and limit the data available to researchers. • Restricted APIs: These APIs often provide limited data and are subject to change or discontinuation at the platform's discretion. However, alongside these, "obstruction and lawfare" can be seen as "technologies" being used to prevent researcher access. The complexity of Terms of Service is being used to prevent researchers from being able to access data. This is concerning, given the importance of independent research to online safety.
Question 1e: Have services and/or researchers made use of privacy-enhancing technologies to enable access?	Confidential? – N Privacy-enhancing technologies (PETs) have been explored and, in some cases, employed to facilitate data access while protecting user privacy. However, their application in this context is still limited. One challenge is the potential for PETs, such as differential privacy, to introduce noise into the data, which can affect the accuracy of research findings. There are also live debates on the ethics of providing synthetic data, with some promoting its abilities to protect the privacy of data subjects, while others point to the risks of relying heavily on artificial data that is not generated by real-world events. While PETs hold promise, their

	effectiveness and applicability in the context of online safety research require further investigation and development.

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 challenges constraining information sharing for online safety research are multifaceted and significant: The challenge of access: The primary constraint is the limited access granted by platforms, especially medium-sized and smaller ones, which often cite the resource burden of providing access as a barrier. Platforms are often unwilling to share data that may be sensitive or commercially valuable. Distrust and fear of reputational damage provide further motivation to restrict access. Technical challenges: Ensuring secure data access, transfer, and storage presents considerable technical hurdles. The sheer volume and complexity of data generated by online services require sophisticated infrastructure and expertise to manage effectively. Some platforms may develop trusted research environments (or similar) to maintain control over the data to avoid directly transferring data, but these are resource-intensive to create. Financial costs: Data sharing entails significant financial costs for both platforms and researchers. These include developing and maintaining data-sharing infrastructure, ensuring data security, and covering legal and compliance costs. Data sharing technologies and infrastructure are also constantly evolving, meaning that providers need to constantly invest in keeping these up to date. However, the alternative is also expensive as researchers would rely on FOI requests, which take considerable time and resources to fulfil. Lack of standardisation: The absence of standardised data formats and interoperability across different online service providers complicates data aggregation and analysis. Legal environment and threats: The legal landscape surrounding data sharing for research is complex and, in some cases, hostile. Platforms have taken legal action against researchers and those using data scraping techniques, especially to train generative AI models, creating a chilling effect on independent research. There is also ambiguity in the application of GDPR to research activities, creating legal uncertainty. Lack of clarity on 'public data': The absence of a widely accepted definition of 'public data' and guidelines for its fair use creates legal and ethical challenges for researchers. This ambiguity is sometimes used by platforms to restrict access to data, even data that is ostensibly public. Lack of clarity over research purposes: There are challenges for some platforms as to who should be permitted to access data, whether they need institutional backing and who makes those decisions. Platforms are increasingly using ‘apply to access as registered researcher’ schemes, where researchers have to satisfy a number of requirements and have given a lot of power to the platforms to decide upon the appropriate research use cases. Unsustainable access models for smaller platforms: Providing access to data costs time and resources, and business models need to balance access and sustainability. Research integrity: The risk of undermining research integrity exists if access to data is contingent on platforms influencing research questions or methodologies.

	This can lead to biased or incomplete research that does not serve the public interest. Verification and delays: Platforms often delay responses to data requests or refuse them without adequate explanation. There is a lack of mechanisms to verify the completeness and accuracy of the data provided without additional costs or harming smaller platforms.
Question 2a: What are the legal challenges/risks to sharing information from online services with independent researchers?	Confidential? – N The legal challenges and risks are substantial, and recent research by the ODI highlights the chilling effect of lawsuits brought by platforms against researchers and web scraping companies, even when those lawsuits are ultimately unsuccessful. The legal risks associated with accessing and using data that may be considered "public," but where the boundaries of fair use are not clearly defined are particularly challenging. The ongoing debate around what constitutes "public data" adds another layer of legal complexity, as highlighted by the recent Meta vs. Bright Data case. Further legal challenges include: Unclear legal protections for researchers: In the UK, legal protections for researchers accessing and using platform data are not clearly defined. This lack of clarity creates a significant risk for researchers who may face legal challenges from platforms. Terms of Service restrictions: Platform Terms of Service often restrict common research methodologies, such as data scraping, creating legal risks for researchers who employ these techniques. The lack of standard terms and ambiguity in many Terms of Service, particularly for smaller platforms, creates further uncertainty, stifling research. Data protection implications: Sharing user data, even in anonymised or aggregated forms, raises data protection concerns under regulations like the GDPR. Navigating these regulations requires careful consideration and legal expertise. Data sharing arrangements must comply with data protection principles, including purpose limitation, data minimisation, and security. Fundamental human rights implications: Data sharing practices must respect fundamental human rights, including the right to privacy and freedom of expression. Commercial sensitivity: Platforms often cite the commercially sensitive nature of their data as a reason to restrict access. They are also concerned about the potential for research findings to negatively impact their reputation or business interests.
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? – N The technical challenges are numerous and complex: Secure infrastructure: Developing and maintaining secure and reliable data sharing infrastructure and APIs is a significant undertaking. Larger datasets may require secure computing environments, which require further resources. Moreover, handling large datasets from online services requires significant data storage and engineering capabilities. Data processing and analysis: Handling large-scale datasets and extracting meaningful insights requires specialised skills, tools, and computational resources, limiting the number of researchers accessing the information. Data quality and integrity: Ensuring data quality and integrity throughout the sharing process is crucial but challenging. The data provided may be incomplete, inconsistent, or lack adequate documentation.

	Data sharing mechanisms: There is a trade-off to be considered between data sharing mechanisms (where platforms provide data) and data access paradigms (where researchers access data directly). Each approach presents its own set of technical challenges. Ad hoc processes: Existing data access processes are often ad hoc and unreliable, with APIs subject to change or discontinuation. Data requested on a 1:1 basis may be similar to other requests, meaning a duplication of effort. Privacy-enhancing technologies (PETs): While PETs can allow access to sensitive data, their implementation at scale is expensive and technically demanding.
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?	Confidential? – N De-anonymisation risks: There is a risk of de-anonymisation when sharing data, even if it has been anonymised or aggregated. This risk is heightened when dealing with large and complex datasets. Data breaches and misuse: Preventing unauthorised access, data breaches, and misuse of sensitive information is a critical concern. Robust security protocols and infrastructure are essential. Platforms may also be concerned about reputational damage or legal liability in the event of a data breach. Security exemptions: The security exemptions in the Digital Services Act (DSA) are not clearly defined, and it is important that this is not replicated in the UK context. While security-based exemptions may be necessary in some cases, the bar for such exemptions should be high. Audit trails: Verifiable logs of data shared for research purposes are needed to create audit trails and ensure accountability.
Question 2d: What are the information quality challenges relating to online services sharing information with independent researchers?	Confidential? – N Information quality challenges relate to the reliability, accuracy, and completeness of the data. Data designed for business purposes: The data collected by platforms is primarily designed to serve their business and product goals, which may not align with the needs of researchers. For example, different formats, standards, and definitions may mean the subject and scope of the datasets are unclear. Data provided often lacks sufficient context, making it difficult for researchers to understand its meaning and significance within the broader ecosystem of the service. Data reliability: The reliability of data needs to be verified, which is currently often impossible. This lack of verification can undermine the validity of research findings. Platform changes: Researchers need to be informed about any product experiments or changes made by the platform that may affect the data provided. Outdated or fragmented data: Datasets can be outdated, fragmented, or unverifiable, making it difficult for researchers to draw accurate conclusions. Biases and limitations: Addressing potential biases and limitations in the data that may affect research findings is crucial. In some cases, there is a negative cycle whereby platforms don't do any internal analysis of the biases that exist within their datasets but also don't let researchers access the data because they are concerned that it is biased.

Question 2e: What are the financial costs to online services relating to online services sharing information with independent researchers?	Confidential? – N Infrastructure and security: Developing and maintaining data-sharing infrastructure, APIs, and security measures is costly. And so is the cost of ongoing data management and support, which includes the resources needed to standardise and anonymise datasets and service the requirements of researchers trying to access the data. Data engineering: Providing data access requires significant data engineering efforts, particularly for VLOPs, which need to develop ways to pull or query data from often siloed services. Monitoring and assessment: Investment is also needed to facilitate monitoring and assessment protocols, ethics review, feasibility assessments, and research review processes.
Question 2f: What are the financial costs to researcher trying to make use of information shared by online services?	Confidential? – N Data access fees: Researchers often need to pay for data access or services from online platforms. In particular, heavy API subscription costs (such as those imposed by X, formerly Twitter) can be prohibitive. During the pandemic, a number of telcos provided discounted access to mobility data to monitor social distancing but curtailed this access after a year. Legal and compliance costs: Ensuring data protection compliance and obtaining legal advice can be costly, particularly for smaller organisations. There is also significant financial risk associated with potential legal action if researchers use data scraping or other methods that violate platforms' Terms of Services. Standardised and accessible legal information for researchers looking to access data would help to reduce this risk and compliance costs. Data storage and analysis: There are data and cloud storage costs to researchers trying to make use of information from online platforms, especially when dealing with large datasets. Researchers also need access to expensive computational resources and data analysis tools. Testing burden: Currently, the burden of testing and research often falls on civil society and academia due to platforms' reluctance to share data. This places a significant financial strain on these organisations.

Question	Your response
Question 3: How might greater access to information for the purpose of research into online safety issues be achieved?	Confidential? – N Achieving greater access requires a multi-pronged approach: Investment in the data infrastructure: Ongoing investment in new infrastructure is needed across academia and civil society to coordinate data access requests and facilitate data sharing. Collaboration: Enhanced collaboration between stakeholders, including regulators, online service providers, researchers, and third-party organisations, is essential. Legal and ethical frameworks: Clear legal and ethical frameworks for data sharing need to be established to provide clarity and protection for all parties involved. These frameworks should also proactively address the ambiguity surrounding "public data" and establish guidelines for its fair use. They should also take into account regional differences and avoid a one-size-fits-all approach. Secure technical infrastructure: Developing secure technical infrastructure and data governance processes is crucial to ensure data security and privacy.

	Innovative models and technologies: Exploring innovative data-sharing models and privacy-enhancing technologies can help address some of the challenges associated with data access. Financial support: Providing financial and resource support for data-sharing initiatives, particularly experimental approaches and for smaller organisations and independent researchers, is essential. The costs to the researchers are significant barriers to online safety research. Trusted partners: A trusted partner with experience in managing data repositories could play a valuable role in leading the vetting and access process. UKRI could potentially fulfil this role.
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? – N The following models offer valuable lessons for online services, particularly in establishing trust, ensuring security, and balancing data access with privacy protection. They could be adapted to the online services context to facilitate secure and ethical data sharing for research purposes: Trusted Research Environments (TREs): TREs, such as those used in UK healthcare (e.g., ONS 5 Safes), provide secure environments for accessing and analysing sensitive data. They offer a high level of control and security but can be complex and expensive to implement. Data institutions: Organisations like Smart Data Research UK, Health Data Research UK, ADR UK Genomics England, and UK Biobank serve as trusted data institutions that facilitate access to sensitive data for research purposes. These models offer valuable insights into the role good data governance and stewardship can play, but there are sustainable data access challenges. UK Data Service: This service provides access to a wide range of social and economic data under controlled conditions, including some sensitive data. International models: Other countries, such as France (CASD) and Canada, have initiatives aimed at facilitating access to data for research purposes. The UK can learn from these models and emulate what elements have worked. Secure enclaves: As used by Meta, secure enclaves provide a safe computing environment for analysing sensitive data. Data trusts: Provide a framework for data sharing with independent oversight and transparent rules for access and use. Federated learning: This allows researchers to train models on decentralised datasets without directly accessing sensitive data. The ODI's research into a typology of access models, building on our Data Access Map, offers a valuable framework for understanding different approaches to accessing social media data. This typology, which includes accessing data directly from companies, platforms/apps, users, and third parties, can inform the development of new models for researcher access. For instance, it could inspire new data trust or data cooperative arrangements.
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?	Confidential? – N Some existing models within the online services industry could be expanded. API-based data access: This allows researchers to access specific datasets programmatically. The previous model used by Twitter, which allowed researchers to search its entire archive of public content, is a good example, although this capability has now been removed. International cooperation (SOMAR) may also present opportunities.

	Data collaboratives: Partnerships between online service providers and research institutions to facilitate data sharing for specific research projects (e.g. the Data Donation model). Sandboxed environments: Meta's sandbox environment for a subset of public content could be a model for other platforms. The benefits of these models include increased transparency and the potential for more robust research. Disadvantages include the limited scope of data often provided, the potential for platform influence on research, and the lack of standardisation across platforms. Research by the ODI reinforces the potential of API-based data access and highlights the need for greater clarity and standardisation in this area. The example of Twitter's previous API model, which allowed for broader access to public data, is relevant here. Furthermore, the ODI's work on building consensus around the definition of "public data" could pave the way for more widespread adoption of API-based access, as it would provide more explicit guidelines for what data can be accessed and how.
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? – N Possible new models include the Digital Services Act (DSA) model, which mandates data access for vetted researchers. This model could be implemented more broadly, though questions remain about its practical implementation
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? – N Advantages of these approaches include increased transparency, the potential for more comprehensive research, and the ability to hold platforms accountable. Disadvantages include the potential for platform influence on research, the need for robust vetting processes, and the challenges of ensuring data security and privacy.
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 Scrutinising research projects through transparency and open science mechanisms will likely require the involvement of multiple actors to ensure oversight and accountability. Regulatory bodies: Regulators, including Ofcom could mandate data access for research purposes, set standards for data sharing, oversee compliance, and play a crucial role in mediating between platforms and researchers. There needs to be a clear framework for assessing the regularity of audits and corporate regulatory capture, even if it's simply transparent data about interactions between regulators and firms. Civil society organisations: Civil society organisations can advocate for greater data access, conduct independent research, and provide expertise on online safety issues. They can also play a role in vetting researchers and ensuring ethical data use. ODI research over the last 12 years exemplifies the crucial role that civil society organisations can play in facilitating researcher access. They can act as mediators and advocates, helping to bridge the gap between platforms and the research community. Furthermore, our work highlights the importance of civil society advocacy in pushing for regulatory measures, such as the DSA, that mandate data access for research. Public sector organisations: Public sector organisations, such as UKRI, can fund research, develop data infrastructure, and facilitate data sharing agreements

	between institutions. They can also provide support and information sharing networks for organisations on data protection, preparing applications, and legal advice.
Question 3f: What could these third-party models look like, and what are some of the benefits and challenges associated with this approach?	Confidential? – N Third-party models could involve independent organisations acting as mediators and facilitating data access between platforms and researchers. Third parties could also play a crucial role in establishing ethical review boards to oversee research involving platform data, vetting researcher requests, and the research use cases. Finally, third parties could form data cooperatives where researchers and civil society organisations pool resources and expertise to negotiate data access with platforms. The benefits of such models include increased independence, greater expertise, and enhanced public trust. Challenges include the potential fragmentation of the research landscape and the need for sustainable funding.
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 Access to data encompassing user-generated content, platform curation processes, and internal platform decision-making is essential for comprehensive online safety research. This data enables researchers to investigate a range of issues, including the spread of disinformation and hate speech, the effectiveness of content moderation efforts, and the impact of algorithms on online behaviour. These categories of data are crucial for understanding the complex interplay between platform dynamics and online safety outcomes. The categories include: Data on harms: Comprehensive data on the prevalence, nature, and types of harms occurring on their platforms. Content moderation data: Information about content moderation decisions, including both automated and human review processes. Algorithm data: Data on the design and operation of algorithms that may impact online safety, such as recommendation and ranking algorithms. User data: Anonymised or aggregated user data that can help researchers understand user behaviour and the impact of online harms. Platform interventions: Data on the effectiveness of platform interventions to mitigate online harms. Internal research: Relevant internal research and documentation related to online safety issues and internal policy documents. All of these categories of information would be invaluable for understanding the root causes of online harms, evaluating the effectiveness of platform interventions, developing evidence-based policy recommendations, and holding platforms accountable for their efforts to create safer online environments. Both existing and potential harms should be included. Researchers need access to the full spectrum of data, including personally identifiable information, where justified, as this data is often critical for social research. Restrictions on data access by major social media platforms in the recent past underscores the urgency of addressing this issue. A collaborative approach, involving platforms, researchers, regulators, and civil society organisations is essential for developing and implementing sustainable solutions that ensure responsible and ethical access to data for public-interest research.