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 Independent researchers are currently able to obtain very limited information from gaming services providers to assess the prevalence and nature of harms on those platforms. Transparency practices in the online gaming industry generally lag behind mainstream social media platforms. Broadly speaking, gaming platform data consists of: ● **Persistent Data**: This includes user account information and user-generated spaces which could be accessible via APIs to facilitate large-scale trend analysis. ● **Ephemeral Data**: This includes real-time text and voice communications and gameplay data, which are critical for understanding in-game interactions but require robust privacy safeguards and some consideration of technical and financial constraints. ● Policy enforcement information: This includes data regarding games' moderation actions, strategies and efforts. Currently, very few companies make persistent data widely available to researchers. To date, only Roblox, a game-creation platform, and Steam, a digital marketplace for games, have public APIs through which researchers can conduct searches of persistent platform data. Even fewer companies provide access to ephemeral data, which is critical to studying and understanding harmful interpersonal conduct in games, including child exploitation, grooming, radicalization, and hate-based harassment. The only recent example of a major game company sharing such data with researchers is the collaboration between the publisher Activision and

	researchers at the California Institute of Technology (CalTech), which gave select researchers access to communication data in order to analyze the company's moderation pipeline and propose improvements. Additionally, most game companies do not release transparency reports with basic data about their policy enforcement actions. Among major game platforms and publishers, only Xbox, Roblox and Activision currently release any meaningful enforcement metrics on a regular or semi-regular basis.
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 Currently, the majority of research on gaming platforms is done by recording first-person accounts from users – specifically, asking them to recall experiences and note the frequency, nature, duration, etc. While surveys of this sort can be helpful, there are many shortcomings with data that rely on participant memory. Most current research in this field focuses on understanding the frequency and nature of online harms and mental health impacts of those harms on the user. The majority of research is cross-sectional in nature and relies on opportunity samples (i.e., non-representative data) of undergraduates or via social media recruitment.
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 The goldmine in terms of understanding harms in online games is **ephemeral communication data**. This includes user account information and user-generated spaces which could be accessible via APIs to facilitate large-scale trend analysis. With access to ephemeral communications and gameplay data researchers would be able to conduct robust, large-scale analyses of the prevalence, nature, and mitigation of harms in these spaces. As noted above, independent researchers' access to ephemeral communication and behavioral data in online games is currently extremely limited. A rare exception is the research collaboration between the

	publisher Activision and researchers at the California Institute of Technology (CalTech). Such collaborations are very few and far between, and provide little public transparency as to the terms of the collaborations. Game researchers also struggle to access **persistent data** – such as user account information and user-generated spaces – even though such data can be shared through searchable APIs, allowing them to track user networks and trends in iconography to, for example, help uncover terrorist networks, without compromising players' privacy. As noted above, only a few gaming platforms currently have public APIs. The lack of standardized API access hampers comparative analyses of gaming services and leads to misaligned incentives (services which are less likely to prioritize trust & safety are less likely to be transparent, and therefore also less likely to be publicly criticized due to lack of access to their in-game data). In addition, researchers lack systematic access to gaming platforms' moderation and enforcement data. This includes detailed reports on moderation actions, systemic risk assessments, and mitigation strategies. As noted above, most game companies do not release transparency reports with basic data on their policy enforcement actions. Finally, independent researchers would benefit from access to data from product experimentation results, which could reveal harms tied to specific design features of those services. Online platforms regularly conduct experiments to test the impact of their product designs on the user experience. For example, they might test the impact of different persuasive design strategies on children's engagement and spending habits. The results of such experiments can reveal information about the links between specific product choices and systemic risks impacting players and society broadly. To the extent that online gaming platforms conduct experiments, researchers should be able to request access to the data produced by such experiments, including metrics on their success or failure, with appropriate safeguards implemented to protect trade secrets and other confidential information.

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 There is limited open-access sharing of game platform data. For example, the Open Science Framework website (osf.io) allows researchers to make the data supporting their findings available after publication. See, e.g., the Unity Analytics Data shared by the University of York. While such data-sharing regimes are useful to ensure replicability, they are limited in their ability to provide new insights beyond what the researchers already studied. There are no known governance models allowing for pre-publication data sharing.
Question 1d: What technologies are typically used by providers of online services to facilitate existing information access?	Confidential? N Online services that host static user-generated data can share that data with researchers through searchable APIs. For more information on the state of research APIs and other tools for research on social media, see here. Such APIs are also relevant to online games to the extent that games store persistent data, such as user account information and user-generated digital spaces.
Question 1e: Have services and/or researchers made use of privacy-enhancing technologies to enable access?	Confidential? N The following technologies and methods can be used by gaming services to safeguard user privacy while enabling researcher access to platform data: ● Anonymisation and pseudonymisation: Service providers can anonymise or pseudonymise

	data, including ephemeral data, before sharing it with researchers to minimize privacy risks. This involves removing or replacing personally identifiable information while preserving the data's utility for research purposes. Most ephemeral data – including voice chat data, which is inherently privacy sensitive – can be pseudonymized or anonymized to protect players' privacy. This anonymization is typically done by (a) only storing the content of the communications, but not any personally identifiable data regarding the user who created the communication; (b) scanning such content to redact any identifiable information included in the content itself; and (c) when possible, in the case of voice chat, only storing transcriptions, or using voice-changing software to mask the voice of the speaker. Furthermore, this data can be protected using privacy and security best practices, such as encryption in transit and storage. ● Data aggregation: Aggregating data into larger groups can further protect individual privacy. For example, advertising databases can group users into pools of at least 100 individuals before disclosing targeting parameters. ● Restricted access and secure environments: Platforms can implement technical measures to control data access and ensure secure handling. This may involve using APIs with specific permissions, establishing data clean rooms, or creating virtual laboratory environments.

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 Access to in-game communications and behavioral data comes with legitimate challenges — ranging from privacy risks to cost barriers — which gaming services and researchers would need to overcome. <u>Privacy concerns</u>: Many gaming platforms currently avoid collecting ephemeral communication data in order to protect the privacy of their users, and may have concerns about being required to collect this data. But, as noted above, most ephemeral data can be pseudonymized or anonymized to protect players' privacy. <u>Technical and resource constraints:</u> Collecting ephemeral communication data may be harder for some games than for others. While some games utilize server-based communication systems – in which the game serves as an intermediary for the communications, and thus could, in principle, collect or analyze those communications if needed – other games utilize peer-to-peer communication systems which are not accessible to the game studio. In order to grant researchers access to peer-to-peer communications, the game would first need to update to a server-based system, or install on-device monitoring tools, both of which can pose technical and monetary challenges to studios. Furthermore, each game configures gameplay data in unique ways, so any such data collection would first require discussion and reasonable agreement regarding exactly what information the platform would collect and make available. Platforms and researchers should engage in dialogue, facilitated by authorities like DSCs, to explore workable solutions that balance both parties' interests. This may involve platforms proposing alternative datasets or access methods.
Question 2a: What are the legal challenges/risks to sharing information from online services with independent researchers?	Confidential? N Game services are subject to data privacy regulations and intellectual property protections which constrain companies' ability to share consumer and internal data

	liberally. However, there are well-known safeguards that can be implemented to ensure compliance with privacy and IP regulations.
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 Challenges with providing data access depend on the type of data requested. Key challenges include: ● The data may not currently be stored by the game service provider. Recording the data may require engineering work, material costs (for storing the data), as well as considerations of the privacy impact of any such additional data to be collected. ● The data may not have a standard format. Text data, for instance, is easy to share and analyze. Gameplay data, however, does not have a standard format. This poses two major challenges. The first is interpreting the data – if a researcher is told "the user pressed the 'A' button at this time", or even "the user's character moved three pixels to the left", it is very difficult for the researcher to make sense of this data. The second issue is comparison across titles – the lack of standards means two games might store and transmit this data in fundamentally different ways, and asking any studio to change their format to match another would involve substantial engineering work and possibly be impossible due to the design of the game. ● The data may contain sensitive PII and may not be easy to clean. Inputs from a controller can be shared so long as no PII is explicitly attached, but text or voice records might include spoken PII and require sophisticated review to ensure nothing private is being leaked.

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? – Y / N
Question 2d: What are the information quality challenges relating to online services sharing information with independent researchers?	N Some games and game platforms, such as Minecraft, Fortnite, and Roblox, allow users to create or host their own spaces, with unique names, attributes, and content, within the platform. These platforms store data related to these user-generated spaces persistently as well. Much of this data is difficult to sort through as it relates to game configurations rather than textual content, but platforms frequently also include text-based tags to indicate the type of space or experience that has been created. It is possible to enable researchers to search through this kind of persistent content based on the tags, although these tags – whether player-generated or AI-generated – can be imperfect. Another challenge is the provision of data that are too broad or vague. For example, when sharing content moderation metrics, platforms should disaggregate the data sufficiently – e.g., by type of illegal content detected and enforced against – so that researchers can derive sufficiently nuanced insights.

Question 2e: What are the financial costs to online services relating to online services sharing information with independent researchers?	Confidential? – Y / N See answer to question 2b.
Question 2f: What are the financial costs to researchers trying to make use of information shared by online services?	Confidential? – N Some platforms impose fees on researchers to access their APIs. These fees can be unduly burdensome. See, e.g., https://developer.x.com/en/products/x-api.

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 See answer to questions 3c and 3e.
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 There are no known current models or frameworks that exist to allow researchers to access sensitive information beyond direct collaborations between industry and researchers.

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?	While there is no precedent, there are frameworks that exist for sharing data collection, such as OSF (https://osf.io/). Anonymous/depersonalized data could be shared there, allowing access for researchers without having to engage in individual vetting procedures for each request. The data that could be shared there would vary depending on privacy/security concerns. For example, it may be possible to share the raw data that is utilized for their transparency reports (policy enforcement, etc.) but perhaps not likely for voice-chat data.
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 To ensure that platforms are not overwhelmed with individual requests and can appropriately prioritize their efforts towards compliance, a third-party organization could be tasked with fielding requests from vetted researchers and consolidating and prioritizing such requests into manageable tranches of data that gaming services would be able to provide utilizing a reasonable amount of resources on a time-limited basis (see question 3e). When researchers request data access from gaming service providers under legal frameworks like the OSA, providers may raise valid concerns related to privacy issues and the protection of business secrets. Below are some ways that a third-party organization could address these concerns while preserving the ability of vetted researchers to study relevant risks in this sector: ● Require researchers to articulate the research objectives and justify the necessity and proportionality of the requested data, focusing on data directly relevant to understanding online harms. For instance, a researcher seeking to analyze ephemeral gameplay data to understand the scale and nature of extremist recruitment might request access to the positions of characters in the game world. Because of the sheer volume of data to be collected here, it would be unreasonable to demand that a game platform continuously make this data available. Instead, game developers and researchers should directly collaborate to identify reasonable measures the game can take which inform the key details of interest to the researcher. For instance, rather than a researcher requesting “all position data of all players within the

	virtual world", a researcher might specify "I'm interested in understanding whether players are more likely to bring up extremist views when they know they are part of smaller or larger groups." In-game location data might be useful in this case (i.e., in order to determine group size), but it will be substantially more achievable for game developers to provide data pertaining to these sorts of targeted questions, as compared to providing full visibility into ephemeral streams of gameplay data. ● Similarly, larger data types like ephemeral audio or video data, can be expensive for game platforms to store and transmit. Requiring researchers to communicate clear time windows (e.g., "we only need data from this week") and sampling strategies (e.g., "we only need 1% of the user data") can significantly help platforms reduce their costs to ensure complying with requests can be done reasonably.
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? – N A third-party organization could help facilitate, coordinate, and streamline research data access requests to ensure those requests are manageable for industry, and cost-effective in terms of reducing duplication, and responsive to privacy and security risks. Such an organization could also serve to increase transparency into data sharing between industry and researchers.
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 The following are categories of information/data that online gaming services should enable researcher access for: A. Persistent user account content through searchable application programming interfaces (APIs): While the exact data storage processes vary by game, all games store some basic information persistently – particularly relating to player accounts (usernames, passwords, historical user achievements, leaderboards, etc.). While some games – primarily on mobile platforms – also collect additional identifiers regarding a player's age, gender identity, spending habits, and other sensitive data, most console and PC games do not have any way to identify a user beyond an email address. This basic data can be made available to researchers through searchable APIs, allowing them to track user networks and trends in iconography to, for example, help uncover terrorist networks, without compromising players' privacy (see section on safeguards for more details). B. User-generated spaces through searchable APIs: Some games and game platforms, such as Minecraft, Fortnite, and Roblox, allow users to create or host their own spaces, with unique names, attributes, and content, within the platform. These platforms store data related to these user-generated spaces persistently as well. Much of this data is difficult to sort through as it relates to game configurations rather than textual content, but platforms frequently also include text-based tags to indicate the type of space or experience that has been created. It is possible to enable researchers to search through this kind of persistent content based on the tags, although these tags – whether player-generated or AI-generated – can be imperfect. Access to this data would allow researchers to identify and assess trends regarding user-generated content at scale. Currently, researchers seeking to study problematic user-generated content – such as extremist content – on gaming platforms have to engage in a laborious process of sorting through content manually. With access to searchable APIs, researchers would be able to scale their efforts to track and analyze such content.

C. Ephemeral social and behavioral data: Better understanding of harmful interpersonal conduct in games, including child exploitation, grooming, radicalization, and hate-based harassment, requires analysis of in-game communications data (i.e., ephemeral text and voice chats exchanged among game participants) as well as interactive gameplay data (i.e., the position and movement of one player's virtual-reality avatar as it attempts to, for example, impose on another user's personal space or imitate a sexual act).

An initial hurdle for researchers is that many game services do not specify clearly in their privacy policies whether they collect, process, and store communication data such as voice or text chat.[1] Doing so is required under the UK Data Protection Act. While this Act does not require gaming services to record or store communication data if they lack the capacity, they must nevertheless disclose what data is collected, how it is processed and for what purposes (clearly explaining how a service, for example, makes "voice-related services safer"), ensuring transparency and compliance. As a preliminary matter, therefore, gaming services should be held accountable for providing this information, which would allow researchers to make better informed data access requests.

In cases where gaming services do *not* already collect or store certain communications and gameplay data,[2] a

[1] For example, Roblox states that it collects, processes, and stores voice recordings "to enable voice services and make voice-related services safer," but this explanation may not fully satisfy GDPR requirements. Under the GDPR, such statements must be specific and transparent, clearly outlining purposes like moderation or analytics, the legal basis for processing (e.g., consent, contracts or legitimate interests under Article 6), and how long data will be stored or the criteria for determining retention. Information provided under the GDPR must be in plain, clear, and simple language, avoiding complex or ambiguous phrasing. It should be concrete, definitive, and free of room for multiple interpretations, particularly regarding the purposes of and legal basis for data processing. According to the European Data Protection Board's Guidelines on Transparency (p. 8-9), poor examples include vague statements such as: "We may use your personal data to develop new services" (unclear what the services are or how data will be used); "We may use your personal data for research purposes" (unclear what kind of research is involved); and "We may use your personal data to offer personalized services" (unclear what personalization entails).

[2] For example, Roblox's privacy policy states that the company does not store physical movement information on VR platforms, nor do they store "Information required for additional features that require the use of your camera

	third-party organization could work with companies to develop private, secure, and cost-sensitive methods of storing and sharing limited tranches of ephemeral data for the purposes of independent research. D. Data regarding enforcement of Terms of Service and/or Codes of Conduct: Researchers would benefit from access to data regarding games' moderation actions, strategies and efforts. Among the obligations established by the OSA on "categorized" services is the duty to publish annual transparency reports, covering information about illegal content on the service; measures taken to comply with safety duties; use of algorithms and proactive technology; user reporting and complaints handling; staffing and training related to online safety; and cooperation with law enforcement (UK OSA, Section 74-75). In order to make these reports meaningful sources of information for researchers, policymakers and the public at large, they should contain sufficiently specific and disaggregated data regarding the number of user reports received, actioned on, appealed, and upheld or reversed within each category of harmful content that the game has set out to monitor and moderate. Furthermore, gaming platforms should be required to disclose data regarding which moderation actions were carried out using automated systems, manual human review, or both. These metrics should include efforts to identify, prioritize, and moderate harmful content targeting children specifically. E. Systemic risk assessment and mitigation measures data: Under Section 9 of the OSA, covered services must conduct a thorough illegal content risk assessment. Researchers would benefit from having access to the entirety of those assessments rather than just the public versions. When access to the entirety of the assessments is not possible, researchers should at least be able to request the underlying data as well as key details regarding the methodologies used to identify, evaluate, and address the risks, especially those specifically related to children's safety and well-being.

or upload content that contains your Personal Information." https://en.help.roblox.com/hc/en-us/articles/115004630823-Roblox-Privacy-and-Cookie-Policy

	F. Data from product experimentation results: Online platforms regularly conduct experiments to test the impact of their product designs on the user experience. For example, they might test the impact of different persuasive design strategies on children's engagement and spending habits. The results of such experiments can reveal information about the links between specific product choices and systemic risks impacting players and society broadly. To the extent that online gaming platforms conduct experiments, researchers should be able to request access to the data produced by such experiments, including metrics on their success or failure, with appropriate safeguards implemented to protect trade secrets and other confidential information.