Feedback for the European Commission on the draft Delegated Regulation on data access provided for in the Digital Services Act

Abstract

This submission provides feedback to the European Commission on its draft Delegated Regulation on data access under the Digital Services Act (DSA), focusing on the implications for online gaming platforms. While not explicitly referenced in the DSA, gaming platforms fall within its scope as "hosting services," with some qualifying as "online platforms" and potentially as "very large online platforms" (VLOPs). These platforms play dual roles as sources of entertainment and socialization, but can also provide venues for various types of harm, including dissemination of hate speech, harassment, grooming, and extremist radicalization.

The social dimension of online games blurs the boundaries between gaming and traditional social media. Features like user-generated content, matchmaking, and in-game communication channels make games arenas for both positive social interaction and significant systemic risks. However, understanding these risks is hindered by limited access to platform data. This submission identifies critical challenges and opportunities for a responsible data access regime, balancing research needs, privacy concerns, and the unique features of gaming environments.

Key systemic risks in gaming include:

- **Illegal Content**: Online games host illegal activities such as hate speech and child sexual abuse material.
- **Fundamental Rights Violations**: Online games are exploited by violent extremists, with implications for the right to life and non-discrimination. Some games also undermine players' right to privacy and autonomy through manipulative designs and extractive personal data practices.
- **Civic Discourse, Electoral Processes, and Public Security**: Games are exploited for extremist propaganda, recruitment, and disinformation. Features like user-generated content facilitate the spread of extremist hate-based ideologies, with documented cases linking gaming environments to real-world violence and radicalization.
- **Gender-Based Violence, Public Health, and Well-Being**: Identity-based harassment, doxxing, and manipulative monetization practices disproportionately harm women, LGBTQIA+ players, and children, affecting mental health, equality, and consumer protection.

To mitigate these risks and enhance accountability, independent research is essential. However, the gaming ecosystem presents unique challenges for data access. Unlike social media, gaming platforms often process ephemeral content, such as real-time communications and in-game behaviors, which is not stored long-term. This submission outlines researchers' data access needs, including:

- **Persistent Data**: User account information and user-generated spaces should be accessible via APIs to facilitate large-scale trend analysis.
- **Ephemeral Data**: Real-time text and voice communications and gameplay data are critical for understanding in-game interactions but require robust privacy safeguards and some consideration of technical and financial constraints.
- **Moderation and Enforcement Data**: Platforms should provide detailed reports on moderation actions, systemic risk assessments, and mitigation strategies.
- **Systemic risk assessment data**: Data on persuasive design practices and targeted advertising, particularly regarding children, would help evaluate economic exploitation risks.
- **Experimentation Data**: Platforms' product testing results could reveal systemic risks tied to specific design features.

The submission proposes mechanisms for ensuring secure, privacy-compliant data access, including encrypted data sharing, anonymization, and collaboration between researchers and platforms to address technical and cost-related challenges. By establishing a balanced, well-regulated data access framework, the European Commission can advance systemic risk research and mitigation in online gaming, fostering safer, more accountable digital environments.

I. Introduction

The undersigned parties are members of a multi-stakeholder working group that seeks to advance informed and constructive regulation of the online gaming industry. Our working group is made up of ten members, including five members from civil society or academia, four members from the gaming industry, and one member from a regulatory body. We also recently joined the Global Online Safety Regulators Network as official observers.

While video games are not explicitly mentioned in the Digital Services Act (DSA), gaming services fall within the scope of the regulation as "hosting services." Furthermore, certain games — specifically, online multiplayer games in which players can publicly share information with other players — qualify as "online platforms" under article 3(i) of the DSA and, as such, are subject to its transparency requirements.

For example, the popular game-creation platform, Roblox, allows users to create their own games and then disseminate them to a potentially unlimited number of other players on the platform. Roblox currently has over 30 million monthly active users in Europe, and its rapid global growth means that it is likely to cross the threshold of 45 million users in the EU to be considered a very large online platform (VLOP). Similarly, players on the popular multiplayer game Fortnite, which is owned by Epic Games and also has hundreds of millions of users worldwide, can create and publish virtual worlds, called "Islands," which are then available for other players to participate in. Certain multiplayer competitive games and massively multiplayer online role-playing games (MMORPGs) also qualify as "online platforms" to the extent that one of their principal features and attractions is to enable players to disseminate information widely among the player base.[1]

[1] For example, players in Riot Games' League of Legends, which reportedly attracts more than 30 million daily users to its regional server for Western Europe (EUW), can volunteer to participate in matchmaking and leaderboard

Such games share similarities with social media platforms in that they provide venues for social interaction and content sharing among users across borders. Indeed, contemporary online games are much more than the digital version of traditional games. They constitute social platforms through which players from all ages, nationalities and social backgrounds meet, interact, discuss via in-game channels, trade via in-game marketplaces, share ideas and build community.

While the social aspect of online games produces positive effects, it also introduces important systemic risks spanning from the dissemination of hate speech and extremist ideologies to cyber-harassment, grooming, doxxing, and stalking. These threats, which are not unique to games but afflict other types of online platforms as well, can reach far beyond the virtual environment and inflict real harm on players' mental health as well as physical safety.

Beyond individual harms, online gaming platforms face risks of collective harm at the societal level. A growing body of evidence shows that extremist actors are exploiting online games to disseminate violent ideologies, network with like-minded people, and perpetrate real-world harm. Similarly, the vast communication networks embedded within games can be used for disinformation campaigns, sometimes involving foreign interference aimed at destabilizing societies or influencing political processes.

This submission aims to bring attention to the aforementioned systemic risks related to online games and to highlight practical approaches for enabling more research on how to best protect the users of these services.

Currently, independent researchers' access to gaming platform data is extremely limited, hampering their ability to conduct large-scale quantitative studies into nature and scale of the risks. In some respects, this lack of access can be explained by competitive commercial factors incentivizing games away from transparency, which could respond well to regulatory requirements shifting the commercial landscape. But, in other respects, access to in-game communications and behavioral data comes with legitimate challenges — ranging from privacy risks to technical and resource constraints — which gaming services, researchers and Digital Services Coordinators (DSCs) would need to overcome. This submission addresses these challenges and proposes a way to manage them in pursuit of a viable and meaningful data access regime that responds to the unique features of online games.

II. Background on the gaming industry and gaming services

Online gaming is a gargantuan industry. In 2024, the global video game industry generated over $200 billion in revenue and provided entertainment to more than three billion consumers around the world. With a projected market value of over $300 billion by 2027, the video game industry is larger than the music, movie, and television industries combined.

---

tracking, which involves sharing their username and other account information with the broader community. In MMORPGs such as Blizzard's World of Warcraft or Linden Labs' Second Life, users can create and personalize "homes" and other persistent spaces, which they can make accessible to all other users on a shared regional server or even on the platform globally.

While comparable to the social media industry in terms of size and reach, online games are different from mainstream social media platforms in some important respects. These differences impact the types of data that independent researchers would need in order to understand and shed light on the impact of games on the exercise of fundamental rights, civic discourse and public security.

The most critical difference between gaming platforms and social media is that social media tends to consist of public or semi-public, permanent content, which platforms or researchers can search for and review at any time as needed. In contrast, gaming sites primarily make use of private, ephemeral content (e.g., voice chat, real-time text messaging, and in-game behaviors), which is typically processed but either not stored or stored only temporarily, due to cost and/or privacy reasons associated with long-term storage of this data. As such, it is substantially harder for researchers to gain access to this data.

Other noteworthy differences between social media and gaming platforms include games' frequent use of user-generated content, through which end users can significantly alter the in-game content, story, characters, or setting, as well as many players' use of pseudonyms and avatars. Despite these particularities of gaming platforms, they still largely function as social platforms and should therefore be considered within the scope of the DSA's data access regime.

III. Systemic risks and impacts in gaming

While online games are a source of joy and entertainment for millions of users, they are also sites where real-world harms can originate. The virtual worlds of video games, once seen only as sanctuaries providing escape, relaxation, and fun, have become breeding grounds for hate, harassment, and other forms of "toxicity." Players, particularly young players, women, people of color, and members of the LGBTQIA+ community, frequently endure toxic environments characterized by vitriol, discrimination, and threats. Beyond their impact on specific players' individual rights to non-discrimination and physical and mental health, certain gaming sites have been exploited for extremist radicalization, which in turn undermines democratic institutions and public security.

Below is a breakdown of the four categories of systemic risks (Article 34 DSA) and the ways that games can play a role in exacerbating them.

1. The dissemination of illegal content:

   Among the types of illegal content and conduct found in games are child sexual abuse material and hate speech. There is mounting evidence of child sexual abuse occurring in digital gaming spaces. In 2024, Bloomberg documented "Roblox's Pedophile Problem," outlining the systemic failure of Roblox's trust and safety systems to protect children from grooming and exploitation. It is crucial to address these risks as they undermine children's right to protection from exploitation and abuse under the United Nations Convention on the Rights of the Child (UNCRC) (Articles 19, 34, and 36), as referred to in recitals 52 and 81 of the DSA.

Hate speech is also a very common occurrence in online games, although the incidence varies across titles. Through surveys of multiplayer gamers, the Anti-Defamation League (ADL) has repeatedly noted that large numbers of players experience identity-based harassment in games (e.g., based on players' gender identity, racial identity, etc.). In the 2023 installment of its annual gamer survey, the ADL found that 75% of teens (ages 10-17) experienced some type of harassment in online multiplayer games, with more than one third of teens ages 10-17 reporting that the harassment they faced in games was identity-based. Hate speech is not only harmful but also explicitly illegal in all EU member states, with laws designed to curb the dissemination of content that incites violence, discrimination, or hatred. The EU's Framework Decision 2008/913/JHA mandates the criminalization of public incitement to violence or hatred based on race, color, religion, descent, or national or ethnic origin. While enforcement and specifics vary across countries, national laws align with this framework.

2. Negative effects for the exercise of fundamental rights:

Harmful behavior in games can negatively impact players' human rights. In the most severe cases, extremist radicalization through gaming inspires violent actions that violate individuals' right to life. The perpetrator of the Christchurch massacre in New Zealand was a regular participant in gaming chat rooms, where he frequently engaged in racially-motivated extremist ideation. Gaming, by his own admission, played a role in his radicalization and even inspired the way that he executed and broadcasted the shooting. Similar links to online gaming communities surfaced in copycat shootings at Poway, California; El Paso, Texas; Halle, Germany; and Buffalo, New York. Gaming platforms and communities played an enabling role in each of these shooters' willingness and ability to perpetrate extreme acts of offline violence, resulting in the violation of victims' right to life. In this context, the United Nations Committee on the Rights of the Child requires that "children are not recruited or used in conflicts, including armed conflicts, through the digital environment. That includes preventing, criminalizing and sanctioning the various forms of technology-facilitated solicitation and grooming of children, for example, through use of social networking platforms or chat services in online games" (General Comment No 25 (2021) §122). In other, more common, occurrences involving intimidation and doxxing, the targeted or affected individuals suffer discrimination, violations of privacy, and mental health harms.

In parallel, players increasingly face risks of economic exploitation due to wide deployment of manipulative and exploitative designs in contemporary video games. The widespread adoption of free-to-play (F2P) games has driven game providers to rely heavily on in-game purchases and targeted advertising, incentivizing the use of manipulative "dark patterns" and exploitative designs to maximize player engagement and spending. Some games — particularly those accessed through mobile phones — rely on the extensive collection of personal data to deploy highly personalized marketing strategies. These practices raise serious concerns about privacy violations but also the exploitation of players' vulnerabilities. The resulting risks include heightened susceptibility to addiction, excessive spending and play-time, and long-term psychological, social, and physical harm.

Children's rights to protection from exploitation and harmful information (UNCRC articles 17, 19, 34, and 36) are jeopardized through exposure to explicit or harmful content, risks of grooming, cyberbullying, and scams in online gaming, as well as data exploitation due to inadequate privacy and data protection safeguards. For example, Roblox, a game-creation platform that caters principally to children under 13 and is considered "the world's largest recreation zone for children,"[2] allegedly puts profits over children's safety, with "social media features [that] allow pedophiles to efficiently target hundreds of children." The UN Committee on the Rights of the Child has emphasized the need to regulate such harms, referencing the importance of public health research to combat misinformation and harmful materials. The Committee has also called for measures to prevent unhealthy engagement in digital games, including regulation of design features that undermine children's development (General Comment No. 25 (2021), §96).

3. Negative effects on civic discourse, electoral processes, and public security:

The gaming sector offers an immersive and easily accessible arena for extremist persuasion, propaganda, and recruitment. Game-creation platforms like Roblox and Minecraft provide the tools for anyone – even those with rudimentary technical skills – to create games that simulate extremist worldviews. While these platforms may discourage such uses, they can still be leveraged in this way. The use of user-created worlds or game-creation platforms to propagate extremist ideals are well-documented, and have included reenactments of Nazi and Uyghur concentration camps. One example can be seen in the long-running (now defunct) virtual slave society on Roblox, called The Senate and People of Rome, which consisted of a rigidly hierarchical society under the command of the lead player, who anointed himself "Caesar." At its height, the game involved hundreds of players occupying different roles as commoners, servants, patricians, commanders, senators, and magistrates. Members of the "Caesar's" exclusive army were instructed to "read SS manuals and listen to a far-right podcast about a school shooter." Some members insisted that they viewed the allusions to Nazi mobile death squads, the staged battles between slaves in the amphitheater, and even the virtual execution of one of the players, as simply part of a joke. But one player admitted that after "simulating life under Fascism" as a 14-year-old on The People of Rome, he had since become even "more supportive" of it. There are many other documented examples of experiences that promote extremist worldviews – including bespoke maps and gameplay scenarios where players abuse or murder ethnic minorities, and World War II simulations where players simulate Nazi Germany and enact the murder of Jewish people.

While extremism online is certainly not unique to online gaming, these spaces provide certain conditions that purveyors of extremist ideologies find attractive: their extensive reach, including among youth and children; the ease of communication that gaming platforms provide without significant oversight or accountability; the opportunity to network and build community; and the underlying normalization of toxic rhetoric, which has been associated with an increased risk of being persuaded by extremist propaganda.

[2] According to activist short-selling firm Hindenburg Research, more than half of Roblox's 79 million daily active users are children under 13.

4. Negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being:

   Hateful communication and hate-based harassment within games can lead to acute psychological impacts, with implications for victims' right to health. According to the 2022 ADL survey, 10% of surveyed adult gamers who experienced harassment while playing online multiplayer games reported having depressive or suicidal thoughts. Nearly a quarter of witnesses to, and half of direct targets of, such abuse report post-traumatic stress disorder symptomology.

   The prevalence of identity-based harassment and intimidation also affects users' right to non-discrimination. Many video games are notoriously hostile towards women — with over half of them experiencing online abuse — even though almost half of the global gamer population is female. Such gender-based violence in gaming serves to perpetuate negative stereotypes and harmful attitudes towards women and girls. Doxxing, another common form of in-game harassment which involves publicly sharing a player's personal identifying information with the intention to intimidate them, impacts as many as one in five game players. Doxxing is a particularly dangerous form of online harassment because it invites others to translate the online intimidation into real-world, physical aggression.

While there is some qualitative and quantitative evidence that gaming sites can contribute to the above systemic risks, researchers lack access to necessary in-game data to better understand the scale and nature of the harms. The following section outlines the types of data that would be needed to advance research in this area, as well as the recommended safeguards and procedures to avoid negatively impacting other important rights and interests.

IV. Data access needs for researchers to study systemic impacts

This section will outline researchers' **data access needs** for the purposes of conducting systemic risk research on gaming platforms, and propose a **process** for fulfilling those needs, including by implementing **appropriate safeguards**.

Data access needs

A. Persistent user account information through searchable application programming interfaces (APIs): While the exact data storage processes vary by gaming platform, all games store some basic information persistently — particularly relating to player accounts (usernames, passwords, historical user achievements, leaderboards, etc.). Some games — primarily on mobile platforms — also collect additional identifiers regarding a player's age, gender identity, spending habits, and other sensitive data. However, most console and PC games do not have any way to identify a user beyond an email address. This 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 gaming 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 games store data related to those 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, even if 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). Third party researchers, with very few exceptions, completely lack access to all such ephemeral data, contributing to important gaps in the understanding of social harms on gaming platforms.

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 interpersonal harms in these spaces. For example, in a rare instance of data sharing by a game company, the publisher Activision gave researchers at the California Institute of Technology (Caltech) access to communication data in order for the researchers to analyze the company's moderation pipeline and propose improvements. Through their analysis, the researchers were able to identify bottlenecks in the moderation system and suggest ways to improve the game's real-time moderation at scale. With more consistent and systematic access to in-game communication data, researchers would be able to enhance their understanding of systemic harms and propose helpful mitigation strategies.

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.[3]

[3] 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

Doing so is required under Article 13 of the EU General Data Protection Regulation (GDPR).[4] While GDPR 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,[5] DSCs should work with gaming services under Article 40(6) to develop private, secure, and cost-sensitive methods of storing and sharing limited tranches of ephemeral data for the purposes of independent research (see details in the section below on process and safeguards).

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 DSA on hosting services, including platforms, is the duty to make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period (Article 15). 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. Detailed information on their data processing practices, business models and data protection safeguards specific to children, addressing gaps not covered by the GDPR: In line with Article 28 (protection of minors), Article 34 (risk assessments), and Article 35 (mitigation of systemic risks), gaming platforms should disclose information about their practices and measures with

---

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" (it remains unclear what the services are or how data will be used); "We may use your personal data for research purposes" (it remains unclear what kind of research is involved); and "We may use your personal data to offer personalized services" (it remains unclear what personalization entails).

[4] Under the GDPR, gaming services that process gamers' personal information are already required to provide clear and detailed information about the personal data they collect, process, and store, including communication data such as voice or text chat. This is mandated under Article 13 GDPR, which requires transparency about the categories of data collected, the purposes of processing, the legal basis for processing, the retention period, and the rights of data subjects.

[5] 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 or upload content that contains your Personal Information."

respect to children specifically. This includes internal information, studies, and data revealing the known impact of profiling children for commercial purposes, the use and profitability of targeted advertising techniques, and revenue generated through child engagement (e.g., Meta's knowledge of Instagram's harm to teens and similar reports regarding TikTok).

Gaming platforms should also provide detailed information on how algorithms rank, recommend, or personalize content for children, including criteria for content display, engagement metrics, and measures to mitigate harmful outcomes. Additionally, they should share data on targeted advertising practices, such as methods for identifying child users, types of ads displayed, and instances of non-compliance with restrictions, as well as disclose the use of persuasive design techniques like gamification or rewards aimed at engaging children, along with their behavioral impacts. Such disclosures would enable researchers and regulators to better evaluate risks, design effective interventions, and implement protective measures to mitigate harms to children online.

F. Systemic risk assessment and mitigation measures data: Under Articles 34 and 35 of the DSA, platforms are required to conduct systemic risk assessments and undertake mitigation measures to address those risks. Researchers would benefit from having access to the entirety of those risk 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 related to children's safety and well-being.

G. 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.

Process and safeguards

When researchers request data access from gaming service providers under legal frameworks like the DSA, providers may raise valid concerns related to player privacy, technical and resource constraints, and the protection of business secrets. Below are some ways to address these concerns while preserving the ability of vetted researchers to study systemic risks in this sector.

Privacy Concerns:

- Anonymization and pseudonymization: Gaming service providers can anonymize or pseudonymize data, including ephemeral data, before sharing it with researchers to minimize privacy risks for players. This involves removing or replacing personally identifiable information while preserving the data's utility for research purposes.

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. However, 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.

Technical and resource constraints:

- Providing alternatives with respect to ephemeral communication data: 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. Given this distinction, it is our recommendation that Digital Services Coordinators (DSCs) either:

    a. Require server-based communications for all relevant game studios, to ensure researcher access could be achievable when necessary.
    b. Require games to disclose to their users whether their communications are peer-to-peer (and thus completely unmoderated, with no guarantees whatsoever regarding safety) or server-based.

- Negotiation and consolidation of requests regarding gameplay data: 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 to researchers. Platforms and researchers should engage in dialogue, facilitated by DSCs, to explore workable solutions that balance both parties' interests. This may involve platforms proposing alternative datasets or access methods.

In terms of the specificity of data access requests, researchers should clearly articulate the research objectives and justify the necessity and proportionality of the requested data, focusing on data directly relevant to understanding systemic risks. For instance, if the researcher requesting to know the position of the character in the game world, they might need to collaborate with the platform to answer questions like (a) how frequently should this position be assessed (every second?); (b) does the researcher need pixel-specific coordinates or would coarser locations suffice; (c) does the researcher need to know the orientation, velocity, or other aspects of the character as well; etc. Because of this complexity as well as the sheer volume of data to be collected in this category, 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 make 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.

In addition, to ensure that platforms are not overwhelmed with individual requests and can appropriately prioritize their efforts towards compliance, DSCs should field requests from vetted researchers and consolidate and prioritize 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.

Business Secrets:

- Balancing Commercial Interests with Research Objectives: The DSA prioritizes research into systemic risks over absolute commercial secrecy. Service providers should not refuse data access solely based on commercial interests. Recital 97 of the DSA underscores that commercial interests should not automatically lead to a refusal to provide access, but rather guide the modalities of access.
- Technical and Legal Measures: Platforms can employ technical measures like data clean rooms and legal tools like non-disclosure agreements to protect commercially sensitive information while allowing researchers to access necessary data.

V. Conclusion

The integration of online gaming platforms into the DSA's data access framework is essential for addressing the systemic risks they pose while preserving their benefits as social and entertainment spaces. By enabling secure, privacy-compliant access to platform data, the European Commission can empower researchers to better understand and mitigate harms, promote user safety, and uphold fundamental rights.

This balanced approach will ensure that online gaming evolves into a safer and more accountable part of the digital ecosystem.

VI. Authors of this submission (in alphabetical order)

Kaila Jarvis, Keywords Studios
Rachel Kowert, University of York
Noémie Krack, Centre for IT and IP law (CiTiP) of KU Leuven
Leah MacDermid, Keywords Studios
Ingrida Milkaite, Ghent University
Simon Monkman, Ofcom
Mariana Olaizola Rosenblat, NYU Stern Center for Business and Human Rights
Mike Pappas, Modulate
Martin Sas, Centre for IT and IP law (CiTiP) of KU Leuven