OliverWyman | CogCo

INSIGHTS INTO THE VIDEO SHARING PLATFORM SECTOR

CONFIDENTIALITY AND LIMITING CONDITIONS

Report qualifications, assumptions and limiting conditions

Oliver Wyman was commissioned by the Department for Digital, Culture, Media and Sport (DCMS) to conduct an assessment of the Video Sharing Platform (VSP) sector, including the current state as well as the trends and possible evolution pathways in the future. The primary audience for this report includes DCMS, Ofcom, providers of video sharing capabilities and the general public.

Oliver Wyman shall not have any liability to any third party in respect of this report or any actions taken or decisions made as a consequence of the results, advice or recommendations set forth herein. This report does not represent legal advice, which can only be provided by legal counsel and for which you should seek advice of counsel.

The findings contained in this report may contain predictions based on current data and historical trends. Any such predictions are subject to inherent risks and uncertainties. In particular, actual results could be impacted by future events which cannot be predicted or controlled, including, without limitation, changes in business strategies, the development of future products and services, changes in market and industry conditions, the outcome of contingencies, changes in management, changes in law or regulations. Oliver Wyman accepts no responsibility for actual results or future events.

The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified. No warranty is given as to the accuracy of such information. Public information and industry and statistical data are from sources Oliver Wyman deems to be reliable; however, Oliver Wyman makes no representation as to the accuracy or completeness of such information and has accepted the information without further verification. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

CONTENTS

EXECUTIVE SUMMARY

DCMS has commissioned Oliver Wyman to assess the current and future state of the Video Sharing Platform (henceforth VSP) industry, with a particular focus on implications for user safety. Throughout this report, "we" is used in reference to Oliver Wyman, as the authors of this report.

SCOPE OF STUDY & KEY FINDINGS

UK users today have access to a wide variety of video content through a range of video sharing platforms (VSPs). VSPs with the required connection to the UK are regulated by Ofcom under the VSP regime and are anticipated to be regulated under the upcoming Online Safety (OS) regime once the VSP regime is repealed by the Online Safety Act. VSPs in scope of this report cover (1) platform providers with the required connection to the UK who notified their status to Ofcom under the VSP regime at the time of writing this report, and (2) other VSPs.

In this report, we have analysed the current state of competition, innovation and growth in the VSP sector, reviewed user protection mechanisms currently deployed, and examined the possible future evolution of the sector. Throughout, we also provide our perspectives on best practices from other risk based regimes that could be applied in this sector to facilitate better user safety outcomes. Our findings are based on a combination of desk research, expert interviews, quantitative and qualitative analysis and complemented by insights from a survey of a representative group of 2,252 members of the public (of which 355 were under the age of 18), conducted for the purposes of this work in February 2022. Through the survey we investigated users' experiences of, and reactions to, encountering harmful video content online.

The global VSP sector is fast-growing and heavily concentrated with 5 top players aimed at users of all ages (YouTube, Facebook, TikTok, Twitch and Dailymotion) dominating the space, accounting for ~90% of total video views in the UK in October 2021. When using VSPs, the majority of users are regularly exposed to video content that they consider inappropriate, distressing or deliberately misleading. Under 18s most frequently report encountering harmful content more than once a week which strengthens the importance of robust safety measures aimed at protecting children online. Survey outcomes show the range of content that users recall as harmful goes beyond the harm categories typically prioritised by VSPs. The majority of users take limited or no action in response to encountering harmful content, citing uncertainty around their ability to make a difference by doing so as a key reason.

Large proportions of survey respondents report that they have not encountered many safety features on VSPs they use (e.g. complaint systems, advertising rules and requirements, reporting mechanisms). Advertising rules and regulations, and media literacy programmes, were the two safety features which the fewest respondents had encountered, and the same two features were also least likely to be recognised by them. When asked about how they perceive the effectiveness of different safety features, most respondents ranked each safety feature to be at least somewhat effective at managing harmful content. Among these, age verification and terms and conditions were the two safety features with the lowest ratings of perceived effectiveness.

Our research of the VSP sector shows that many VSPs do not yet take a systemic approach to user safety and often only address these topics in a relatively reactive way. The need to ensure fast growth and maximise revenues in turn encourages use of methods that increase user engagement (e.g. recommendation algorithms), typically exposing users to additional risks. Through our research it appears that: a) VSPs have limited focus on user protection and risk management considerations throughout the whole lifecycle of product development and b) VSP governance structures and organisational checks and balances are not robust enough to ensure an adequate focus on user protection. Given that regulation of platform providers in this space has only recently been strengthened (the Ofcom regulated UK VSP regime came into force in November 2020) and is planned to be strengthened further by the introduction of the Online Safety regime, there is a unique opportunity for a step change in how VSPs approach the area of user safety.

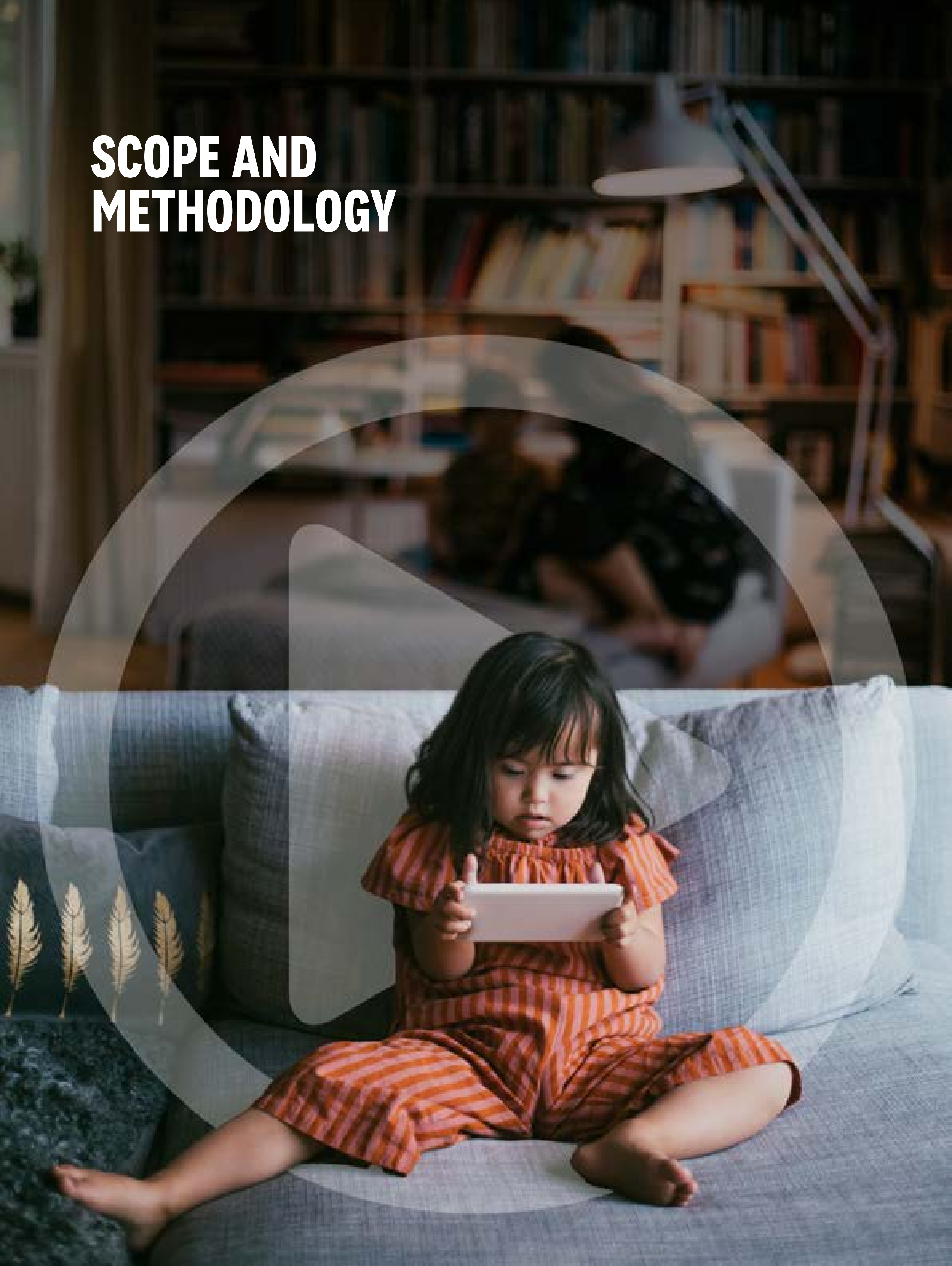
CONSIDERATIONS FOR POLICYMAKERS

Innovations and potential evolution of the VSP business models, for example continued reliance on an advertising based model, and diversification of revenue streams (e.g. by entry into adjacent sectors), are likely to further increase consumer risk in the future as user safety concerns are magnified with the growing scale and complexity of the VSP sector.

Following our research, we have listed below the key considerations for VSP platforms and for the design and implementation of upcoming and future regulatory frameworks:

- The Online Safety Bill was introduced in Parliament in March 2022. Given the fast pace of market development, Oliver Wyman expects that following the first few years of operation, the scope of the Online Safety regime may need to further evolve to account for the landscape and severity of online harm that is likely to emerge.
- Given the rapid pace of market developments, regulatory frameworks in this space should be sufficiently flexible to allow supervision of the sector to be risk-based. Furthermore, they should also be structured in a way that is technology agnostic where possible (i.e. unbiased towards use of a specific technology and thus less prone to becoming obsolete as the market continues to change). This approach will facilitate implementation in a space as dynamic as the VSP sector.
- Regulators in this space will need to ensure that any safety measures deployed, and metrics used to evaluate the effectiveness of regulation, will need to be built adequately to accommodate the emergence and widespread adoption of new forms of video content and user interactions online (e.g. livestreaming and immersive real time digital environments where harms to users can materialise instantaneously).
- As VSP business models continue to evolve and platforms experiment with further functionalities and revenue streams, new overlaps are likely to arise between regulation of online safety and further regulatory areas such as data protection, competition and financial services. This may necessitate further close cooperation between regulators, including the Information Commissioner's Office (ICO), Ofcom as the current UK established VSP and the future Online Safety regulator, the Advertising Standards Authority (ASA) in its role as a self regulator of the UK’s advertising industry and the Financial Conduct Authority (FCA) as the financial services conduct regulator. As a first step, we recommend further strengthening the cooperation between these bodies in the Digital Regulation Cooperation Forum (DRCF).

SCOPE AND METHODOLOGY



REGULATORY CONTEXT

In recent years, the scope of the European Union's regulatory framework that applies to audiovisual media, the Audiovisual Media Services Directive (AVMSD), has been extended to include Video Sharing Platforms (VSPs). The UK's Audiovisual Media Services (AVMS) Regulations 2020 transposed the EU's revised 2018 Audiovisual Media Services Directive and were laid in Parliament on 30th September 2020. Those Regulations came into force on 1st November 2020 and for the first time introduced rules for VSPs.[1] Ofcom currently regulates VSPs with the required connection to the UK, through a systems based (not content based) regulatory framework. VSPs that are established in an EU country fall under the jurisdiction of that nation's domestic VSP regulations.[2] At the time of writing this report, there are 18 UK established VSP platform providers regulated by Ofcom under the VSP regime, including TikTok, Snap and OnlyFans.

Since its introduction, the VSP regime requires all online video services with the required connection to the UK that allow users to upload and share videos with the public to: (1) notify Ofcom and, (2) comply with rules around protecting users, especially under 18's, from the risk of viewing harmful material in videos. Under the VSP regime, platform providers are required to:

- Protect all users from videos that are likely to incite violence or hatred against particular groups, and videos which include content which would be considered a criminal offence under laws relating to terrorism, child sexual abuse material, racism and xenophobia.
- Protect under 18s from videos containing pornography, extreme content and other material which might impair their physical, mental or moral development.[3]

In parallel, as part of the further enhancement of the UK's framework for digital regulation, the UK government introduced to parliament the Online Safety Bill in March 2022 which sets out a regulatory framework aimed at tackling harmful content online.[4] The regulatory

[1] www.ofcom.org.uk

[2] www.ofcom.org.uk/online safety/information for industry/vsp regulation/guidance who to notify to ofcom

[3] www.ofcom.org.uk

[4] www.bills.parliament.uk

framework will place a duty of care towards users on a range of online service providers who facilitate uploading and consumption of user generated content (UGC). In comparison to the VSP regime, the scope of the Online Safety regime encompasses other types of UGC beyond video, as well as search engine providers. Whilst the VSP regime focuses on VSPs with a required connection to the UK, the Online Safety regime will also include online service providers of UGC beyond video with links to the UK (e.g. through a sizable UK user base). The current VSP framework is expected to be superseded by the Online Safety regulatory framework.

In this context, DCMS has commissioned Oliver Wyman to assess the current and future state of the VSP industry, with a particular focus on implications for user safety.

DEFINITION OF A VIDEO-SHARING PLATFORM

For the purposes of this report, a Video Sharing Platform (VSP) is defined as an online service which allows users to upload and share videos with members of the general public. The provider of the service controls the organisation but not the selection of videos on the platform. This includes platforms for which facilitating user sharing of video content is:

- either the principal purpose of the service (or a dissociable section of the service); or
- an essential functionality of the service as a whole (i.e. where the provision of videos contributes significantly to the commercial and functional value of their service).

In this context, a platform provider that allows users to view content which is exclusively not user generated (e.g. journalistic media, on demand video streaming such as Netflix or Amazon Prime) are considered not in scope. Further, peer to peer sharing of video content facilitated by the service (e.g. sharing of external video links via a messaging app) is also considered out of scope.

In order to capture all platforms relevant for the future Online Safety regulation, the VSP definition used throughout this report goes beyond the VSPs with a required connection to the UK regulated by Ofcom under the VSP regime. Consequently, VSPs in scope of this report cover:

- VSPs with a required connection to the UK who notified their status to Ofcom under the VSP regime at the time of writing this report,
- other VSPs.

Throughout this report we use the terms ‘Video sharing platforms (VSPs)’ and "VSP sector" to refer to both of these groups combined. When making statements about about platform providers who notified their status to Ofcom under the VSP regime, we will refer to them explicitly.

SCOPE OF THIS REPORT

Throughout this report, "we" is used in reference to Oliver Wyman, as the authors of this report.

In this report, we investigate the VSP sector by focusing on two key areas:

- The current state of the VSP sector — we assess competition, innovation, and historical growth in the sector, methods used by VSPs to target and engage their users and their implications for user safety, as well as the current VSP approach to assessing the risk of harm to users and prioritising user safety actions.
- The future state of the VSP sector in the short and medium term — we analyse user, VSP and external trends which are likely to shape the future of the VSP industry and the possible high level evolution pathways for the sector.

The UK VSP regime will be superseded by the upcoming Online Safety regulatory framework that puts even further emphasis on risk. Therefore, throughout this report, we also provide our perspectives on best practices from other risk based regimes that could be applied in this sector to facilitate better user safety outcomes.

METHODOLOGY

Our findings are based on a combination of desk research, expert interviews, quantitative and qualitative analysis, and outcomes of a user experience survey we conducted for the purposes of this work in February 2022. Two data sources that we wanted to highlight in particular are:

- Viewership data for top 100 VSPs used by UK-based consumers which we used to inform the assessment of the current state of competition and growth in the VSP sector, including both platform providers that notified Ofcom under the VSP regime, as well as other VSPs. For this analysis we used Comscore Video Metrix Multi Platform (VMX MP) data that covers online consumption of video content by users in the UK. Entities included in the dataset represent top 100 VSPs used in the UK by reach (i.e. number of viewers estimated to have viewed video content on that specific platform in the given time period). Our analysis focuses on the time period between January 2020 and October 2021. The dataset includes desktop viewing for all VSPs and also viewing via mobile devices for a select number of platforms (YouTube, Twitch and Dailymotion) for which it was available. The video views metric reflects the total number of streams or progressive downloads initiated by viewers over a given month, where progressive downloads represent videos downloaded from the host website to a device for watching at a later time (rather than streamed directly).
- Behavioural user experience survey conducted by Oliver Wyman and CogCo for the purposes of this work in February 2022 on a sample of 2252 UK users of VSPs, including 355 respondents aged 18 or less. In context of the emphasis on protection of children online present in the upcoming Online Safety regime and the current VSP regime, we pay special attention to differences in user experience between under 18s and over 18s throughout the analysis of survey outcomes. To this end, additional effort was expended to capture a larger sample of respondents under 18. The survey focuses on investigating participants' experiences of harmful video content and the actions they chose to take afterwards, as well as general VSPs usage and perspectives on the importance and effectiveness of VSP safety measures. As part of the survey, survey respondents are asked to recall and describe (in an open ended question) one specific instance of encountering video content that they considered to be either distressing, inappropriate, or intentionally misleading. Responses to the open ended question were manually reviewed and categorised post collection. Throughout this procedure, categories assigned by different individuals were compared on randomly selected subsets of the data to ensure consistency. Please see appendix B for further detail on the survey flow and the categories of harmful content uses.

Please note that throughout this report MN and BN are used to represent millions and billions, respectively.

CURRENT STATE OF COMPETITION, INNOVATION, AND GROWTH IN THE VSP SECTOR

CURRENT STATE OF COMPETITION AND GROWTH

We begin our assessment of the landscape of VSPs in scope of this report by considering two key dimensions of platforms to initially segment the market: 1) VSP scale and 2) the target platform audience. We consider both of these dimensions to be proxies for estimating the potential level of risk associated with using VSPs. Firstly, the risk of using a platform increases proportionally to the VSP's reach and total user base. Secondly, the risk of users' safety being compromised when using platforms aimed at different audiences will increase if VSPs fail to implement effective protection measures relative to their target audience (e.g. age verification measures for VSPs targeting over 18s). In our analysis of viewership trends and competition in the sector, we consider the following segmentation (see Exhibit 1).

Exhibit 1: Segmentation of the VSP landscape

Target Audience	VSPs aimed at all ages	VSPs aimed at over 18s
Objectives	Facilitate a safe experience for all users	Facilitate a safe experience for those who legally can access Prevent under 18s from accessing platforms
Key Levers	Appropriate labelling of sensitive or age inappropriate content	Robust age verification and age assurance measures
	Effective mechanisms for detection and removal of harmful content	

Source: Oliver Wyman analysis

VIEWERSHIP TRENDS BY SEGMENT

The VSP industry is a growing, highly concentrated space with a small number of platforms dominating the industry. Between the beginning of 2020 and the time of writing this report, the number of videos watched by UK users on VSPs each month has been increasing, however the average time spent watching videos per user per week increased only moderately and experienced fluctuations associated with UK lockdown restrictions (see Exhibits 5 and 6). Platforms aimed at users of all ages have shown strong growth whilst platforms with adult content experienced a decline in videos viewed each month (see Exhibit 5).

Please note that for the purposes of our analysis, we define monthly reach as the number of viewers who are estimated to have viewed video content on that specific platform over the whole month.

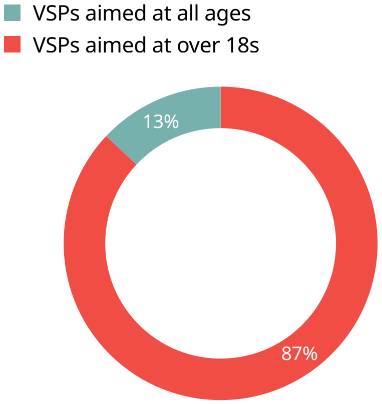
UK users are watching more video content on VSPs each year. In total, UK users watched an estimated ~245 BN videos in 2021, an increase of 13% compared to 2020, as displayed in Exhibit 3. In October 2021 alone UK users watched 21.6 BN videos across the top 100 VSPs, a vast majority of these using platforms aimed at all ages (e.g. YouTube, Facebook, TikTok, Instagram, Twitch and others), as shown on exhibit 8. Whilst the majority of VSPs accessible to UK users are sites with adult entertainment (pornographic) video content (which represent 87% of the platforms in our data sample), it is the VSPs aimed at all ages that dominate the market with over 90% of total annual video views in 2021, as illustrated on Exhibits 2 and 3.

The segment of VSPs aimed at all ages has grown their reach between 2020 and 2021 (see Exhibit 4); this also coincided with an increase in videos watched per user each month (a typical user watched 252 videos per month on platforms for all ages in October 2021, 15% more compared to January 2020, as shown on Exhibit 5). Total number of videos watched reached an estimated ~228 BN in 2021, an increase of 14% compared to 2020. In addition to a strong growth of the segment since 2020, we also observe that in aggregate, the VSP segment aimed at all ages has experienced more fluctuations across all metrics considered, compared to the adult entertainment VSPs as illustrated on Exhibits 4 and 5.

On average, a UK user spent 3.5 hours per week watching video content on VSPs in October 2021 (see Exhibit 6). The data includes only time spent watching videos as opposed to any other engagement of the user on the platform, such as reading and sharing comments, browsing, or using the VSP for any other purpose. The average number of hours spent watching videos per week per user in the UK across both VSP segments has fluctuated between 3.4h and 4.1h in the two-year period, increasing in the early months of the pandemic (April–July 2020)

Exhibit 2: Dataset segmentation

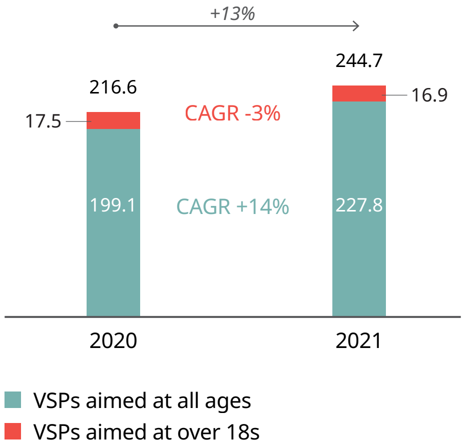
UK top 100 VSPs used by UK-based consumers



Source: Comscore VMX MP, OW custom defined list of entities (over 18s), January 2020–October 2021, United Kingdom

Exhibit 3: Total annual video views by VSP segment in the UK

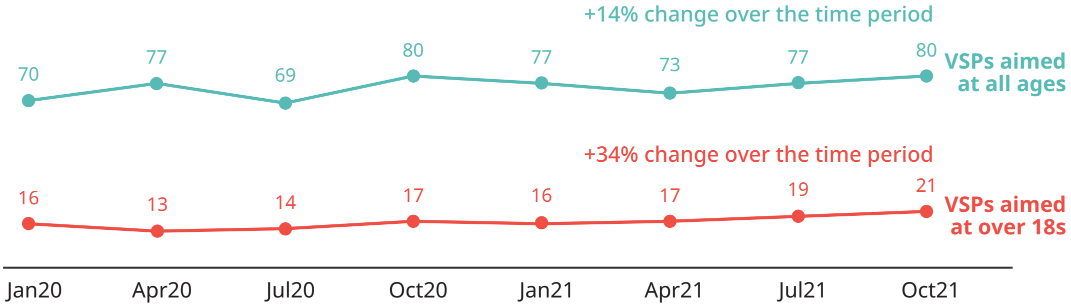
January 2020–October 2021, BN



Source: Comscore VMX MP, OW custom defined list of entities, total video views (over 18s), January 2020–October 2021, United Kingdom

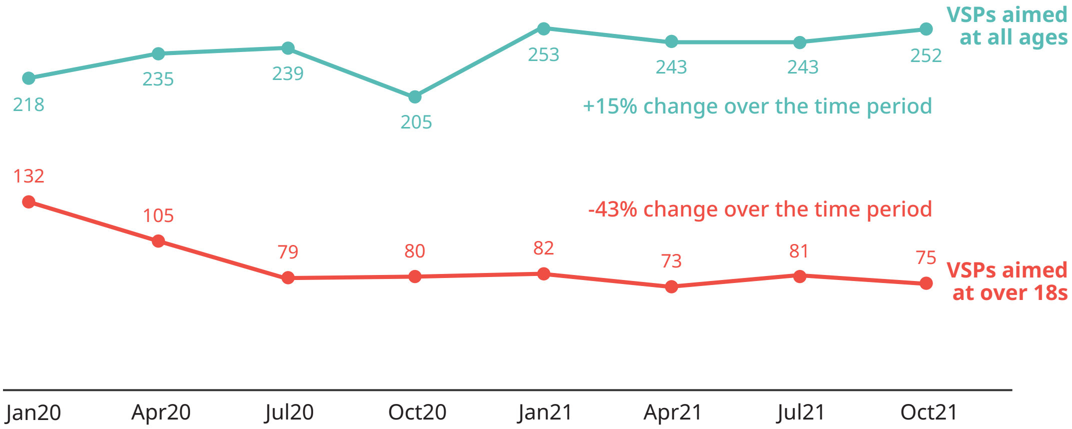
as well as in the winter and spring of 2021, when the UK was under lockdown. Overall, the average number of hours spent watching videos per week per user experienced a slight decrease, with users spending 3% less time watching videos in October 2021 compared to January 2020 (3.5h compared to 3.6h per week, as illustrated on Exhibit 6). Consistently, ~95% of time users spent consuming video content was on platforms targeting all ages.

Exhibit 4: Total monthly reach by segment, MN



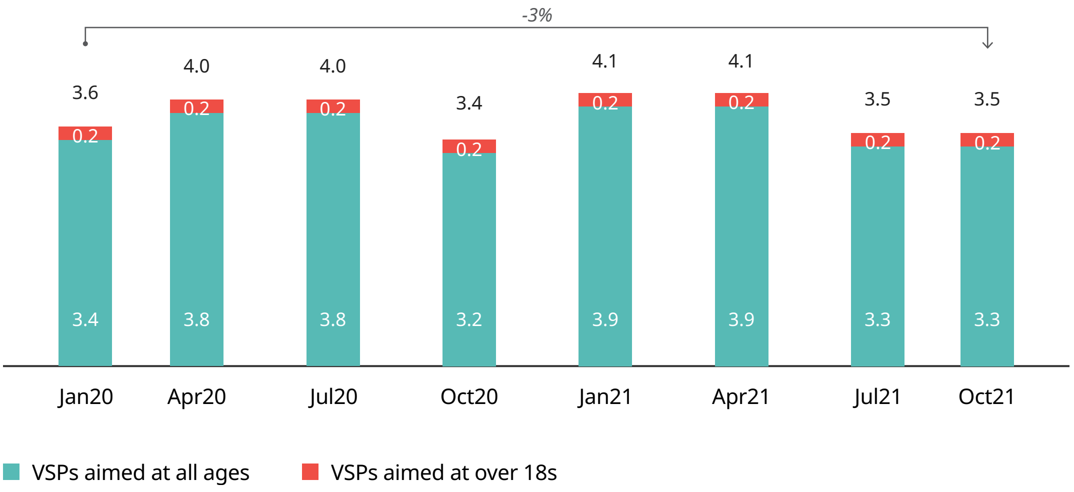
Source: Comscore VMX MP, OW custom defined list of entities, total reach (over 18s), January 2020–October 2021, United Kingdom

Exhibit 5: Total monthly video views per user by segment



Source: Comscore VMX MP, OW custom defined list of entities, total reach (over 18s), total videos viewed (over 18s), January 2020–October 2021, United Kingdom

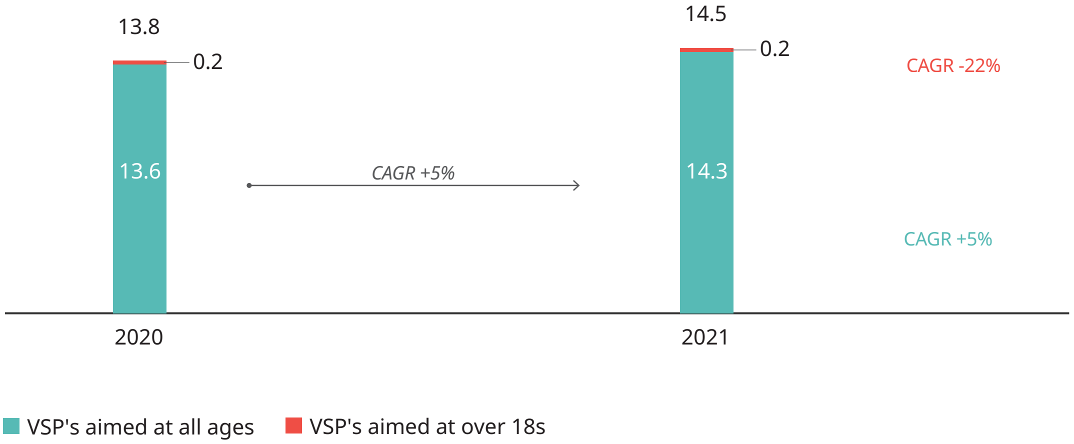
Exhibit 6: Average hours spent watching videos per week per user in the UK



Note that the calculations have been made assuming an average 4.3 weeks in a month

Source: Comscore VMX MP, OW custom defined list of entities, total minutes spent watching videos (over 18s), January 2020–October 2021, United Kingdom

Exhibit 7: Total hours spent watching videos annually in the UK by VSP segment, BN



Source: Comscore VMX MP, OW custom defined list of entities, total minutes spent watching videos (over 18s), January 2020–October 2021, United Kingdom

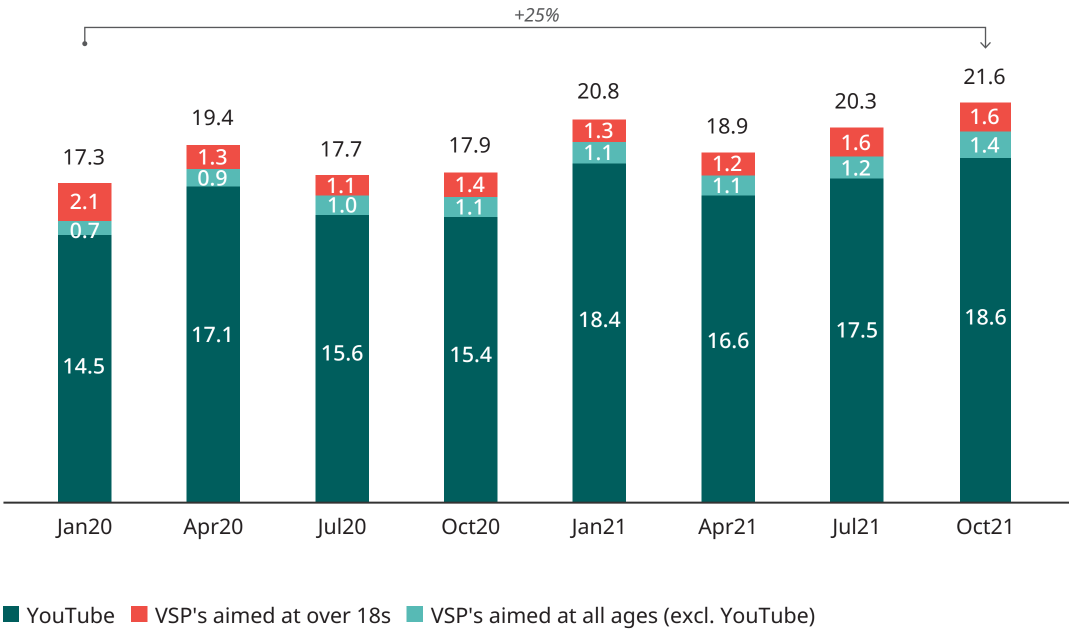
In 2021 users watched fewer videos on VSPs with adult entertainment content compared to 2020, despite the total reach expanding in that period (see Exhibits 4 and 5). In the month of October 2021, 21 MN users were watching video content on VSPs aimed at over 18s, 4 MN more than in October the previous year (see Exhibit 4). The total number of videos viewed on adult entertainment VSPs contracted from ~17.5 BN in 2020 to ~16.9 BN in 2021 (a 3% decrease) as illustrated previously on Exhibit 3, and the average user viewed 132 videos in January 2020, compared to only 75 in October 2021 (a significant 43% decrease), as shown on Exhibit 5.

COMPETITION AND PLATFORM-SPECIFIC TRENDS

The UK VSP sector is heavily concentrated with the majority of video consumption taking place on a small number of platforms. At the time of writing, YouTube, Facebook, TikTok, Instagram and Twitch are the most commonly used VSPs aimed at all ages.

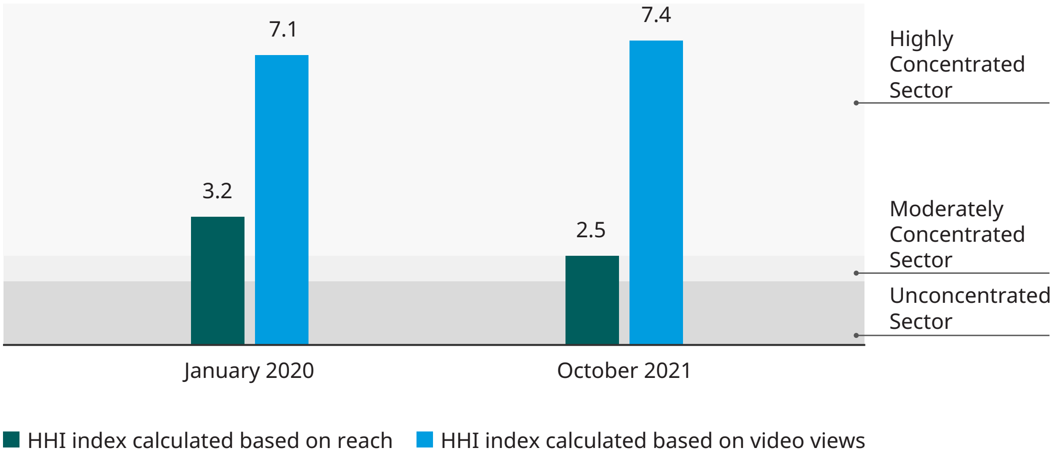
We evaluated market concentration of the sector by calculating the Herfindahl-Hirschman Index (HHI) (see Exhibits 9, 10 and glossary of key terms). HHI measures the size of firms relative to the size of the industry they are in and provides an indication of the level of competition in a market. The HHI is calculated by adding up squared market shares of industry participants, therefore, the higher the outcome, the more concentrated the industry. Typically, an industry with a HHI of less than 1,500 is considered to have low concentration, an outcome between 1,500 and 2,500 moderate concentration and HHI above 2,500 represents a high degree of concentration. We calculated HHI using the total reach of a platform (representing the number of users watching videos on the platform) and total video views. Our analysis showed that the UK VSP sector HHI in October 2021 was 2,500 and 7,400 (based on platform reach and video views respectively), implying a very strong degree of market concentration.

Exhibit 8: Total monthly video views in the UK by VSP segment, BN



Source: Comscore VMX MP, OW custom defined list of entities, total video views (over 18s), January 2020–October 2021, United Kingdom

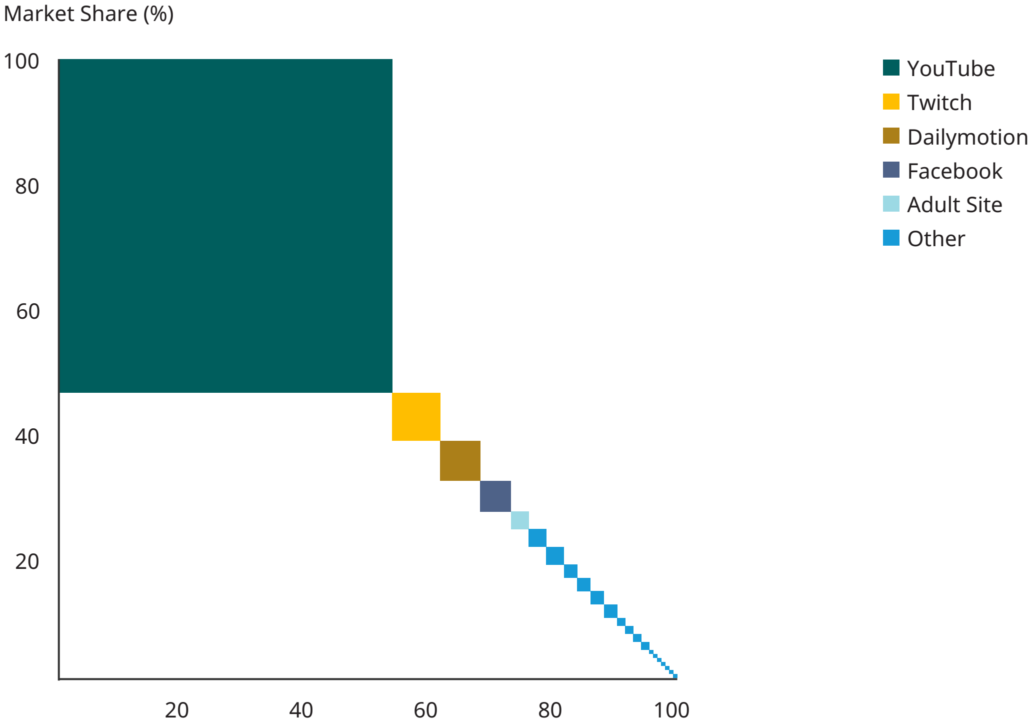
Exhibit 9: Herfindahl — Hirschman Index (HHI) of industry concentration, (thousands)



Source: Comscore VMX MP, OW custom defined list of entities, total video views (over 18s), total reach (over 18s), January 2020–October 2021, United Kingdom

Exhibit 10: Herfindahl — Hirschman Index (HHI) of industry concentration

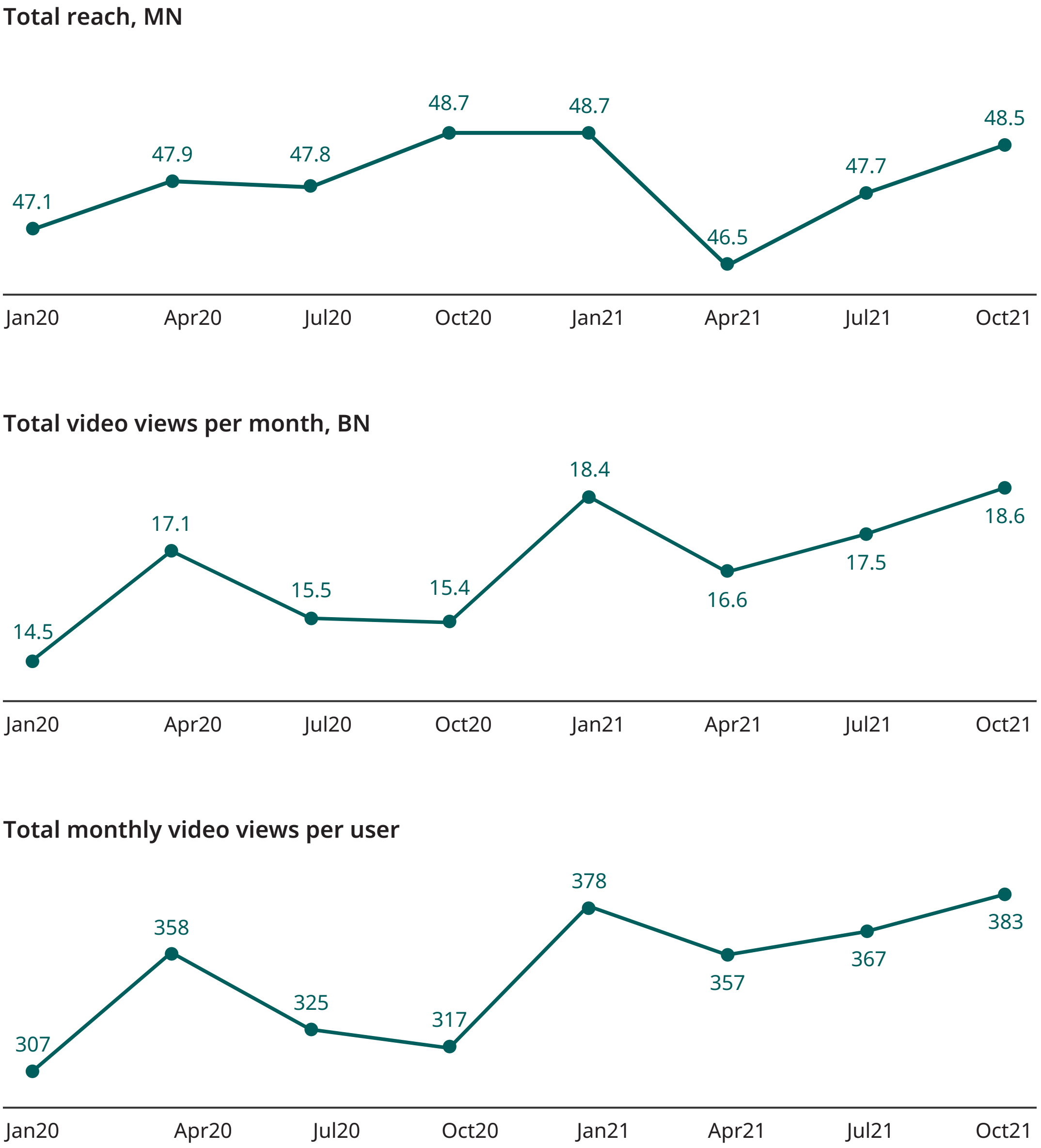
Illustration, HHI calculated based on platform reach, October 2021



Source: Comscore VMX MP, OW custom defined list of entities, total reach (over 18s), January 2020–October 2021, United Kingdom

Exhibit 11: YouTube: total reach, monthly video views and video views per user

January 2020–October 2021



Total reach, MN

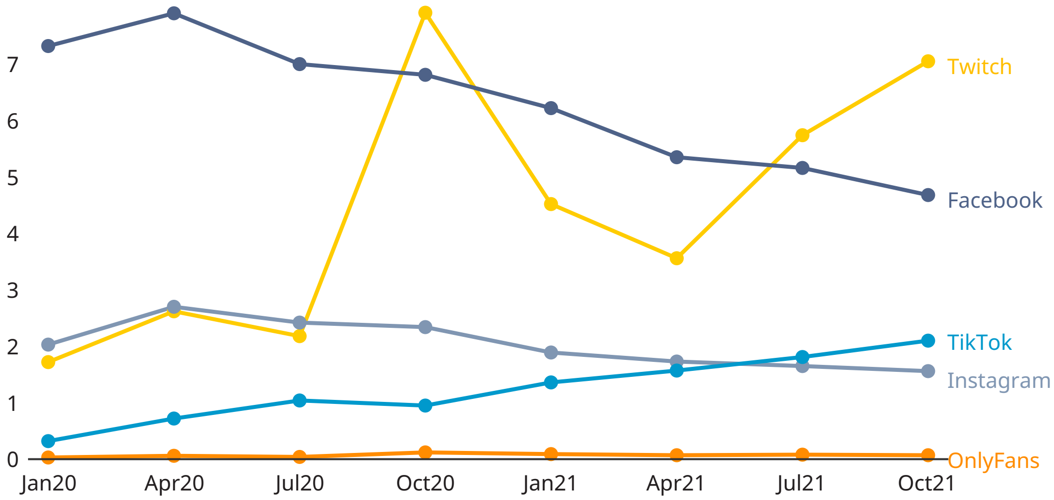
Total video views per month, BN

Total monthly video views per user

Source: Comscore VMX MP, OW custom defined list of entities, total reach (over 18s), total video views (over 18s), January 2020–October 2021, United Kingdom

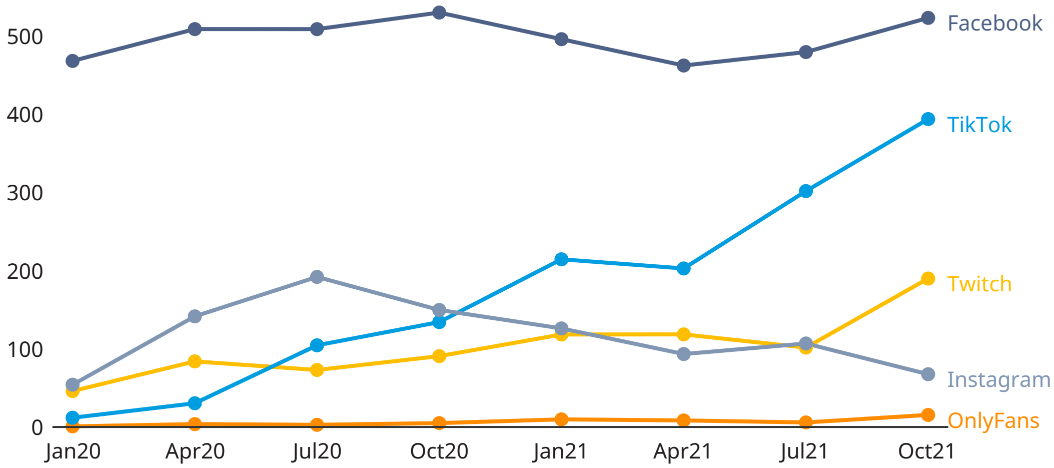
Our analysis shows that among the all-ages platforms, YouTube continues to dominate the VSP space (see Exhibit 8). UK users watched 18.6 BN videos using the platform in October 2021 alone, a 21% increase versus October 2020 (see Exhibit 11). However, over that period of time the total reach of the platform remained stable (~48 BN monthly UK users); consequently, each YouTube user watched 25% more videos per month in October 2021 (383) than they did at the beginning of 2020 (307).

Exhibit 12: Total monthly reach of selected VSP platforms, MN



Source: Comscore VMX MP, OW custom defined list of entities, total reach (over 18s), January 2020–October 2021, United Kingdom

Exhibit 13: Total video views of selected VSP platforms, MN

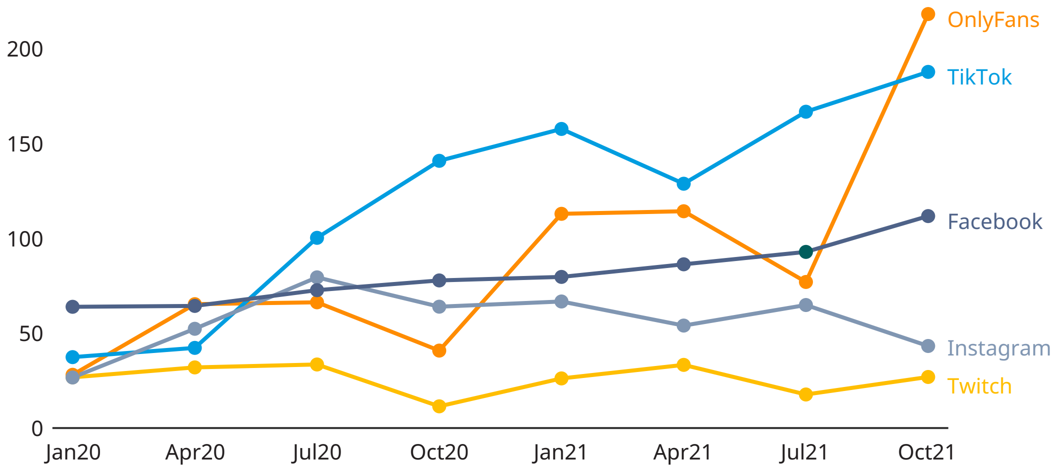


Source: Comscore VMX MP, OW custom defined list of entities, total video views (over 18s), January 2020–October 2021, United Kingdom

While YouTube has been successfully engaging their existing user base to watch more content, other platforms have in that same time period expanded their reach compared to the beginning of 2020 and saw an increase in the amount of video content watched per user. In particular, two recent market entrants (OnlyFans and TikTok) have gained scale in recent years, offering less common formats of video content (short-form video and subscription-based content).

- The total number of videos watched on TikTok reached 0.4 BN in October 2021, more than 30 times the figure from January 2020 (see Exhibit 13). Alongside a strong growth in the platform's user base, this illustrates the rapid rise in popularity of the platform, following its entrance into the UK market in 2017.[1] It was estimated that in 2020, ~21% of social network users in the UK were also TikTok users.[2]
- OnlyFans, a VSP launched in 2016 that offers users access to subscription-based content mostly aimed at over 18s, has also continued growing in popularity since the beginning of 2020.[3] Exhibits 12 and 13 show that both reach and total video views on the platform experienced a steady growth and we observe a large jump in total monthly videos viewed per user, reaching 218 in October 2021, compared to ~20 in January 2020 (see Exhibit 14).

Exhibit 14: Total monthly video views per user on selected VSP platforms



Source: Comscore VMX MP, OW custom defined list of entities, total reach (over 18s), total video views (over 18s), January 2020–October 2021, United Kingdom

[1] Statista

[2] www.emarketer.com

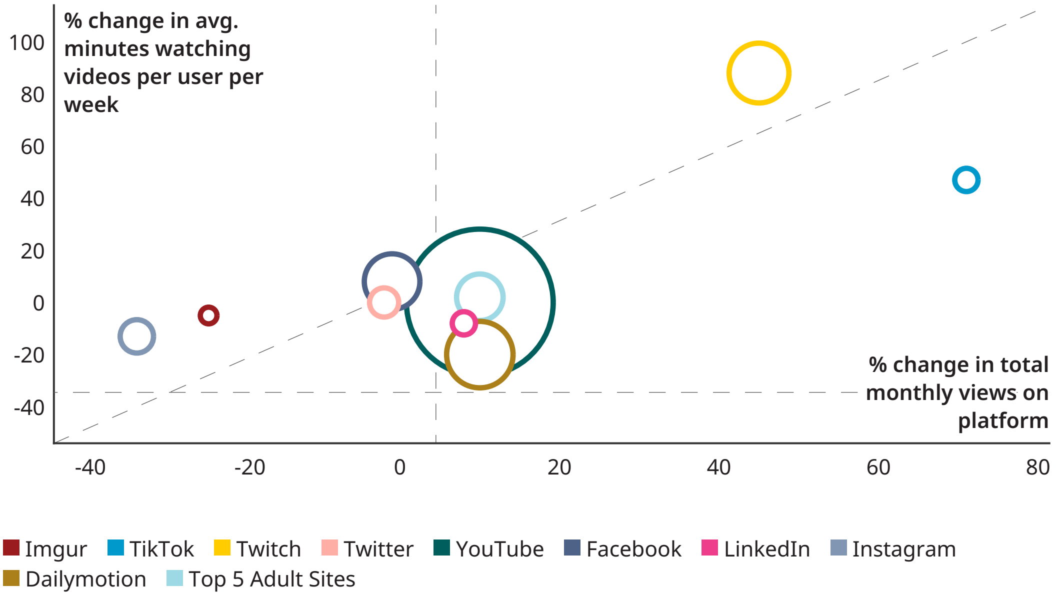
[3] www.onlyfans.com

Meanwhile, other established platforms for which video content has not been the primary focus, have seen more video consumption. Users of Facebook and Instagram have been watching 60-75% more video content each month on the platforms in October 2021 compared to January 2020 (see Exhibit 14). However, in the same time period, their monthly reach of video content (i.e. number of viewers who are estimated to have viewed video content on a specific platform over the course of a given month) has decreased by 23% (Instagram) and 36% (Facebook) which might imply that users may be selecting other platforms for their video content consumption (see Exhibit 12).

Our analysis also shows that **Twitch, a livestreaming service that focuses on video game livestreaming, has become more popular since the start of 2020**, with a greater reach and users watching four times more videos each month in October 2021 compared to January 2020, as displayed on Exhibits 12 and 13. This further illustrates the rise in popularity of livestreaming, a functionality now offered by an increasing number of VSPs.

Exhibit 15: Trends among selected platforms

Area of each bubble represents the relative reach of the VSP



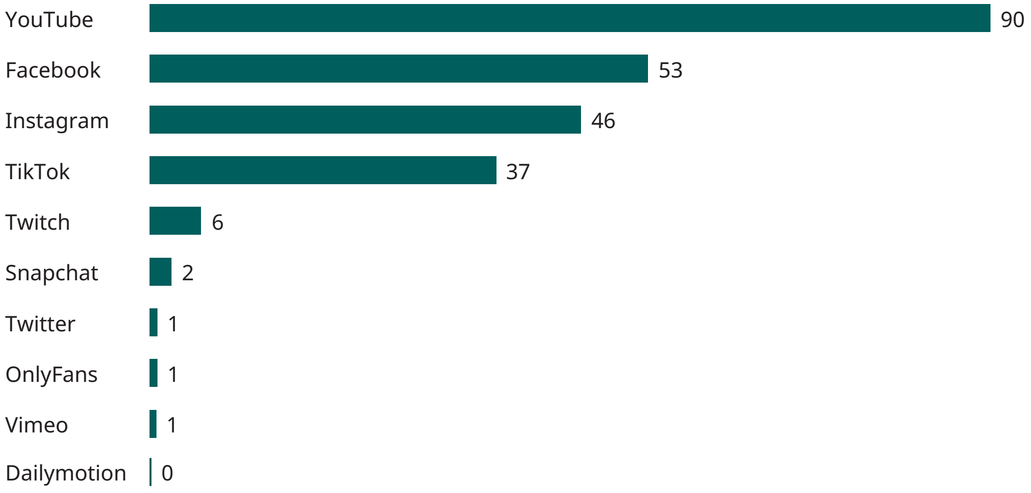
Source: VMX MP, OW custom defined list of entities, total video views (over 18s), total minutes spent watching videos (over 18s), total reach (over 18s), January 2020–October 2021, United Kingdom

A comparison of the trends in total monthly views on a platform and average minutes spent watching videos per user per week (between October 2020 and October 2021) show which VSPs have moved towards shorter videos over time, as illustrated on Exhibit 15. VSPs close to the diagonal dashed blue line on the chart experienced little change to the length of a typical video. However, a typical video watched on those below the line (e.g. TikTok, Dailymotion, LinkedIn) became shorter. In comparison, others (e.g. Twitch) saw users watch longer videos over time providing further evidence on the increased prominence of livestreaming long-form content.

Results of our user experience survey reinforce the above findings and provide further insights into preferences for different age groups (see Exhibits 16 and 17). 90% of all respondents reported using YouTube regularly, regardless of age. After YouTube, we observe notable differences between the VSPs used by respondents depending on their age group. Facebook and TikTok in particular show the biggest differences when comparing users under and over 18 years old. TikTok ranks second among under 18s (used by 76%), while only 30% of over 18 respondents reported using it. In comparison, Facebook is more likely to be used by over 18 respondents, of whom 57% reported regularly using the VSP, compared to only 31% of under 18s using it regularly. Instagram remains third most frequently selected by respondents from both age groups, with around half of respondents reporting using it. Snapchat, Twitter, OnlyFans, Vimeo and Dailymotion were other platforms highlighted by users, albeit less frequently.

Exhibit 16: Popularity of selected VSPs among survey respondents, full sample

Percentage of respondents that report watching selected VSPs

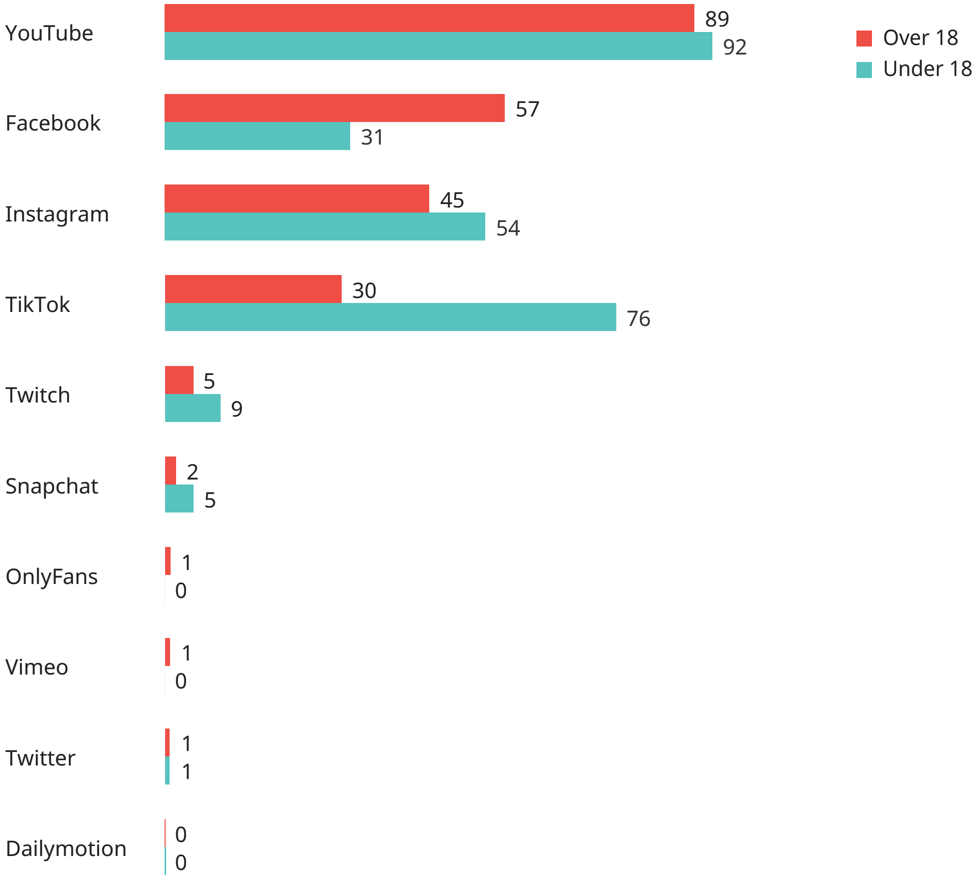


Note: Respondents were able to select multiple options.

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

Exhibit 17: Popularity of selected VSPs among survey respondents, by age group

Percentage of respondents that report watching selected VSPs



Note: Respondents were able to select multiple options.

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

INNOVATION IN THE VSP SPACE

Based on our research, we identified three key areas of innovation in the VSP space:

(1) Growth of livestreaming

(2) Emergence of new methods in personalisation of video content

(3) Rise of immersive digital environments

Additionally, we expect other innovations which have already been widely adopted to continue shaping the VSP industry going forward (e.g. the rise of short-form videos and tailored, data-powered advertising). We discuss them in more detail in our assessment of the future state of the VSP industry.

GROWTH OF LIVESTREAMING CONTENT

In recent years there has been a continued growth in livestreaming content online, accompanied by multiple VSPs incorporating innovative livestreaming features into their platforms. Twitch increased its global monthly active user base between January 2019 and January 2021 from 40 MN to 90 MN monthly active users, and saw an increase in the number of hours watched worldwide from 3.1 BN in Q1 2020 to 5.8 BN in Q3 2021.[1,2] In the United Kingdom, the total number of videos watched on TikTok grew significantly since the start of 2020, reaching 0.4 BN in October 2021 (see Exhibit 13).

While still nascent, we observe innovative use of artificial intelligence (AI) (e.g., in livestreaming channels broadcasting primarily AI-generated videos), virtual influencers and virtual live streamers. These are digitally rendered humans who act out fictional narratives and can be used to showcase products. Virtual avatars cost less than regular influencers, can appear in many places at once, and can act as spokespeople to communicate a brand’s views on topics such as diversity and inclusion or sustainability. Lil Miquela, a CGI model, has over 3 MN Instagram followers and charges a fee of $8,500 per sponsored post for brands including Calvin Klein and Prada.[3]

[1] www.forbes.com

[2] Statista

[3] www.forbes.com

Compared to "traditional" video broadcasting, livestreaming attracts viewers by offering a dynamic and engaging format for a community of content creators and users to interact in real time. However, it also poses challenges for user safety, as it requires real-time and predictive user safety measures to keep up with the real-time nature of the content. There have been historical instances of livestreaming of extremely harmful content, such as the 2019 Christchurch terrorist attack, when platforms struggled to contain and remove the video content before it reached users, as it was shared and re-uploaded. This illustrates the need for implementation of rigorous moderation techniques across VSPs, adequate for live content. Speed of detection and response is crucial to mitigating user safety risks in a livestreaming context. For greater effectiveness, the time from the start of a livestream to potential detection, and from detection to required action would need to be significantly shortened. Popularisation of live video content on VSPs is likely to require additional expenditure on safety measures, posing challenges to VSPs of different sizes. Implementing adequate protections for users can be expensive for smaller players that don’t benefit from economies of scale, whilst large platforms are likely to face challenges in scaling up their detection and moderations tools as the volume of user traffic continues to grow.

Implications for a regulatory environment: The nature of livestreaming as a medium and the potential of harms to users materialising instantaneously brings about a unique set of challenges for the design and implementation of the regulatory framework. Firstly, risk assessments that platforms prepare (mandatory in the Online Safety framework and recommended in the VSP regime) could explicitly cover the potential risks resulting from livestreaming, and the preventative and mitigating measures introduced. Secondly, the same degree of rigour should be applied when designing, implementing, and monitoring safety measures to moderate livestreamed and non-livestreamed content. This can help avoid the potential exploitation where actors seeking to inflict harm could re-broadcast harmful content in the form of a livestream seeking to avoid safety measures. Lastly, in measuring the effectiveness of safety measures in place, metrics that are put in place could also be made consistent between livestreamed and non-livestreamed content to permit building a comprehensive and consistent picture of harm across different modes of video sharing.

NEW METHODS OF PERSONALISATION

New methods for personalising video content are increasingly growing in prominence in the VSP space as ongoing technological advancements are enabling content to be tailor-made for each user or user groups.

Creation of synthetic media (video, audio and images) involves production and manipulation of existing media by artificial intelligence and machine learning systems to produce new content. For example, a person can be included in a video of a situation they did not participate in — this is also referred to as **deepfakes** (also see glossary of key terms). Synthetic media is most commonly present in adult entertainment (especially in the creation of pornographic videos), but it is also a commonly used tool to enable the spread of disinformation. Fabricated videos have been historically used to falsely represent celebrities or politicians expressing polarising views.

Personalisation of content shown to users is increasingly being used in marketing and advertising. Our research found that live video shopping and AI-based image recognition technology is transforming how brands market products to consumers. In China, popular apps such as WhatNot facilitate live shopping experiences where users can run live video-based auctions.[4] YouTube's AI system also enables users to tag objects seen in videos (e.g. a particular brand of kitchenware), which it then can advertise to viewers.[5] Some brands are creating synthetic media to hyper-personalise adverts featuring a consumer wearing or using a product, or dubbing content to be in a consumer’s local language, dialect or accent.[6,7] In 2019, the Dalí Museum in St. Petersburg, Florida collaborated with an advertising agency to create a digital version of Salvador Dalí. Visitors could engage in conversation and take photos with him.[8] In the fashion world, Gucci recently used an AI face-swap technology to enable customers to virtually try on pieces from its new collection.[9] Balenciaga created deepfakes as part of its Spring 2022 fashion show, and Zalando’s 2018 campaign with Cara Delevingne used deepfake technology to create hyperlocal ads.[10,11] While still a nascent innovation, the use of synthetic personalised advertising could change the future of marketing through the emergence of new advertisement formats leveraging data on user behaviour and preferences gathered by VSPs.

These new methods raise significant user safety concerns around privacy, data sharing and consent because the technology allows for the creation of potentially controversial videos without permission (a synthetic media advert could show a user a video whose cast looks identical to a user’ friends and family).[12] Additionally, concerns surrounding use of innovative content personalisation techniques as a tool for disinformation and pornography, are magnified as the technology improves. Young users are particularly vulnerable to the consequences of encountering convincing synthetic videos featuring well known individuals commenting on social and political issues.[13]

[4] www.techcrunch.com

[5] www.taggermedia.com

[6] www.forbes.com

[7] www.ft.com

[8] www.theverge.com

[9] www.hypebeast.com

[10] www.glamourmagazine.co.uk

[11] www.voguebusiness.com

[12] www.medium.com

[13] www.ft.com

Implications for a regulatory environment: Content personalisation is underpinned by data collection, synthesis and analysis on an unprecedented scale. To adequately protect users online from harm resulting from excessive personalisation, continued close cooperation is needed between statutory and non-statutory regulatory organisations whose remits touch upon this area, especially: Information Commissioner's Office (ICO) as the data privacy regulator, Ofcom as the VSP and the future Online Safety regulator and the Advertising Standards Authority (ASA) in its role as a self-regulator of the UK's advertising industry.

RISE OF IMMERSIVE DIGITAL ENVIRONMENTS AND FURTHER DECENTRALISATION (E.G., WEB3)

Finally, we note two interconnected innovations: (1) the rise of **shared immersive digital environments** where technology allows the blending of virtual and physical realities, and (2) a trend towards **decentralisation** across different aspects of the internet, including VSPs. In comparison to an internet landscape controlled by a handful of platforms, the concept of a decentralised World Wide Web refers to a state of the internet where users have ownership of data, infrastructure and governance. This is also referred to as Web3 (also see glossary of key terms).[14] However, we recognise that despite parallel developments in both innovations, to an extent they remain at odds with each other due to existing technological constraints. Shared immersive digital environments require a degree of centralisation or at least linkages between platforms to facilitate user interactions and movement of digital assets at scale.

(a) Immersive digital environments

By allowing users to incorporate technology into additional dimensions of their daily lives, environments like the metaverse (also see glossary of key terms) have the potential to drive user engagement to the next level through features such as enabling users to interact with each other in a virtual environment, create, buy and sell virtual goods.[15] There is a growing interest from investors and platform providers in developing immersive digital environments which offer new ways for platforms to gather user data and leverage it for advertising and building customer engagement. Some of the examples include:

- Meta's $50 million investment in building products to operate in the metaverse, as well as its rebrand under the name "Meta" signals the platform provider's belief in the metaverse as the future for social media.[16]
- Microsoft is in the process of integrating its mixed reality system "Mesh" into Microsoft Teams, with the aim of incorporating digital avatars into video conferencing as a next step.[17]

[14] www.onlinegrad.syracuse.edu

[15] www.newscientist.com

[16] www.about.fb.com

[17] www.news.microsoft.com

- Octi enables users to create and share video content set in virtual spaces and incorporates virtual items created by non-fungible tokens (NFTs) uploaded to the platform.[18,19]
- Online video platform Roblox allows users to create their own immersive worlds for other users to inhabit using VR technology.[20] In November 2021, Nike partnered with Roblox to create the "Nikeland" virtual sports arena for players to compete in as a new form of experiential advertising.[21]

While the topic of the metaverse only entered broad public discourse in 2021 and is still some time away from full implementation, many potential harms are already beginning to illustrate that moderating content in real-time 3D spaces requires new safety mechanisms to protect users from harms. The scale and complexity of these immersive digital environments magnify existing online safety challenges. Given the prominence of video content in digital immersive environments, VSPs will, along with gaming platforms, continue to be key players in its evolution and consequently could consider adapting their user protection mechanisms to keep pace with the emergence of new forms of hybrid video content.

(b) Decentralisation

There are two main aspects through which decentralisation is starting to impact the VSP sector: emergence of VSPs that rely on a decentralised model and usage or provision of decentralised services (e.g. cryptocurrencies, tokens). However, we note that at the time of writing this report, existing cryptocurrency systems often are not fully decentralised given concentration of mining resources (mining refers to the process of verifying transactions by network participants who are in exchange rewarded with newly generated cryptocurrency units).[22]

The continued push by VSPs to integrate more innovative features, including new forms of payments, into their platforms could further increase the safety risk to users. For instance, a VSP which allows users to pay content creators in cryptocurrency could cause harm if users are not made fully aware of the risks of dealing in cryptocurrencies. It may also limit access to content for under 18 users who are not allowed to register with some crypto exchanges. Similarly, targeting users, especially children, with options to purchase special in-app features can be seen as exploitative. In 2020, the EU started addressing the activity of selling gaming "loot boxes", where users purchase a box without knowing the

[18] www.octi.com

[19] www.businessinsider.in

[20] www.cnbc.com

[21] www.news.nike.com

[22] www.investopedia.com

contents, as they were viewed as a form of gambling.[23] There are several recent examples of cryptocurrency scams called "rug pulls", conducted by social media influencers, which further illustrate the scale of the issue. In a "rug pull" scam, a new crypto token is created, listed on a decentralised exchange and promoted to the influencer's audience. After new demand for the token inflates the price, the influencer sells their stake and extracts as much value as possible before the price drops to zero. In January 2022, a YouTuber admitted to extracting more than $500,000 from the supply of a crypto coin they launched and promoted to fans in this way.[24] "Rug pulls" accounted for 37% of all cryptocurrency scam revenue in 2021, compared to just 1% in 2020.[25]

Our research shows that whilst at the time of writing this report only a handful of video sharing platforms are built according to a decentralised model, it is a growing space. The concept of users and content creators being able to monetise the sharing and watching of content directly without being controlled by or benefiting an external platform lies at the core of a decentralised video sharing service. The lack of censorship over content appeals to users and content creators. Examples of decentralised video service providers include LBRY's Odyssee, Theta and Livepeer which we describe in more detail in a case study below.[26,27]

[23] www.europarl.europa.eu

[24] www.protos.com

[25] www.uk.news.yahoo.com

[26] www.odysee.com

[27] www.theta.tv

CASE STUDY 1

Livepeer, founded in 2017, is one of the biggest decentralised video streaming networks. It operates as a Platform as a Service and is hosted on the Ethereum blockchain.[1]

- Livepeer's infrastructure can be used by developers or existing VSPs to build in live or on demand video streaming capabilities into their offering. It provides a cost effective alternative to high existing infrastructure costs related to transcoding and streaming videos.[2]
- Livepeer relies on users taking on different roles in contributing to the running of the network. Users are then rewarded for their participation by earning a share of the fees paid by broadcasters. The payments are in the form of cryptocurrency or tokens. For example, users can help secure the network and participate in the transcoding and distribution of videos on the platform by contributing their computers' resources. There are 4.2k users securing the Livepeer network at the time of writing this report.[3]

[1] www.livepeer.org

[2] www.makeuseof.com

[3] www.livepeer.org

In the context of user safety in a decentralised model, we expect strong emphasis on user-generated safety features and community governance, such as flagging and reporting harmful content by users. The potential challenges brought about by decentralisation go beyond direct harm to users, also covering the broader concept of responsibility and ownership over content and activity on the platform. For instance, a Decentralised Autonomous Organisation (DAO) running a VSP based on a distributed ledger technology, would exercise a lower level of direct control over the platform.

The move towards decentralisation could also be a factor pushing VSPs to further diversify their current ad-based and subscription-based revenue models, e.g. if decentralised forms of video sharing are adopted more widely disrupting the incumbents. This could result in content creators being able to engage more directly, and profit from, their users relying less on major platforms like VSPs to connect with their audiences.

Implications for a regulatory environment: This and other aspects of technological innovation strengthen the principle that regulation and guidance in this space should be formulated in a way that is, as far as possible, agnostic to technology and business models, facilitating implementation in a space as dynamic as the VSP sector.

Furthermore, the interconnected nature of the metaverse and Web3 is likely to create areas of overlap between regulation of online safety and other regulatory areas, e.g. data protection, competition and financial services. This puts additional emphasis on the importance of regulatory cooperation mechanisms such as the recently set up Digital Regulation Cooperation Forum (DRCF) between Ofcom, Information Commissioner's Office (ICO), Competition and Markets Authority (CMA) and the Financial Conduct Authority (FCA). These overlaps and the fast pace of technological change will also impact the nature of digital media literacy initiatives needed to educate the public and children on safe behaviours online, potentially also incorporating financial literacy.

METHODS FOR TARGETING AND ENGAGING USERS

VSPs leverage a range of methods to target users at each stage of their interaction with the platform, each raising their own user safety considerations. In this report, we structure them through a lens of the user journey that begins with an acquisition of a new user (see Exhibit 18). VSPs have a strong incentive to convert one-off to repeated users as it helps maximise the time users spend engaging with platform's contents and makes a VSP more appealing for advertisers. In this section we outline the methods used by VSPs to acquire and convert users and emphasise the importance and risks associated with engagement algorithms, one of the most powerful tools used by VSPs to drive ongoing user engagement.

Exhibit 18: Outline of the user conversion journey

	USER ACQUISITION	〉	**INITIAL USER ENGAGEMENT**	〉	**ONGOING USER ENGAGEMENT**
Tools and techniques available to VSPs to target and lock in users	Cross-platform user acquisition Evolution of new VSP features and content Marketing strategy Global expansion		Thumbnails Prompts/Labelling content as sensitive or inappropriate Search function (suggestions, interaction with the algorithm) Auto-play function when scrolling		*All tools used for initial user engagement* Engagement-based recommendation algorithms (likes/dislikes, subscriptions and similar features) Activity tracking: scrolling, lingering, re-watching Auto-play after previous video ends

	ONE-OFF USER	〉	**REPEATED USER**
User conversion journey	User's sporadic interaction with the VSP Potential lack of user awareness of platform's content (thus higher level of risk) VSP does not have data on the user preferences so likely to show a wide range of content Labelling of potentially harmful content may have the opposite to intended effect (especially on younger users)		User aware of platform's content Enticement to engage with VSP may not be needed VSP can design a customised list of suggested content to watch based on previous engagement data

Source: Oliver Wyman analysis

USER ACQUISITION AND CONVERSION

VSPs employ a variety of methods to acquire new users. These include:

- **Cross-platform user acquisition** (for example through direct partnerships with other websites, or more commonly through embedded videos shared on websites which can draw users back to a VSP) can pose harm to unsuspecting users who may follow a link to a VSP without realising the type of content available on the platform.
- **Evolution of new VSP features and content** can help grow and retain the user base. Examples include in-house content, introduction of livestreaming functionalities (described in detail in a section on innovation in the VSP space) and developing versions of VSPs for children, such as Instagram for Kids and YouTube Kids.[1] The latter raises concerns about the capacity of VSPs to guarantee children's safety, as kid-specific platforms can also be a draw for actors actively seeking to spread harmful content to children.[2]
- **Marketing strategies,** such as integrated advertising (e.g. through sponsored videos) and exclusivity deals with content creators helps VSPs attract content-generating users, who in turn can draw their audiences to the platform. This can pose additional risks if users follow influencers from one comparatively safer platform to another, less protected VSP.
- **Global expansion,** for example through creating localised versions of platforms to access specific markets or acquiring competitors to secure their technology and user base. It can bring both opportunities as new entrants into the VSP market can bring new technologies and features which are attractive to users, however there is a risk that smaller, growing VSPs may lack the resources to develop adequate user safety systems.

The more effective a VSP is in converting one-off users to repeated users, the more revenue it can potentially earn from advertising, subscriptions, and in-app purchases. This strong incentive has immediate implications for the design of methods VSP deploy to encourage content consumption and content creation. At their core, many VSPs are designed to create a **network effect** (a phenomenon whereby a good or service increases in value when it is used by a larger number of people - also see glossary of key terms) among users by facilitating social interactions through comments, likes, and shares to generate engagement. Some VSPs use **"loyalty schemes"** to encourage content consumption. For example, in Twitch's Channel Points system users can accumulate points through watching streaks of channel streams which then unlock unique emojis, privileges, or ways to interact with livestreamers.[3]

[1] www.vox.com

[2] www.wsj.com

[3] www.help.twitch.tv

Many VSPs attract content creators by offering different options to **monetise their content**, most commonly through advertising revenues (whereby creators receive a cut of funds generated by their video) and fan funding where users pay creators directly (either on a subscription basis or through "tipping"). These options may be available only to creators who have reached a certain threshold of subscribers or views, and in some cases can be revoked if creators are found to have violated community guidelines or have posted harmful or unsafe content.

Ongoing user engagement is crucial for platforms to achieve sufficient scale and thus appeal more to advertisers. The following section describes data-driven recommendation engines and algorithms which are key tools for driving user engagement available to VSPs today.

ENGAGEMENT-BASED ALGORITHMS

In their current form, recommendation algorithms present one of the biggest safety risks to users, in particular children and other vulnerable groups, for several reasons:

- **Algorithms are addictive by design.** Their primary goal is maximising the total user time spent on the VSP, which can lead to more daily active users and a more commercially successful platform. However, it is also likely to have adverse effects on users, especially children. Studies show a relationship between time spent on social media (including VSPs) and perceived social isolation, depression, and other mental health issues.[4] A 2017 study by the American Journal of Epidemiology found that higher social media use correlated with self-reported declines in mental and physical health and life satisfaction.[5]
- **Engagement-based algorithms learn by analysing user consumption patterns.** VSPs increasingly track an ever-growing range of activity data based on how a user re-watches, scrolls, pauses, hovers over, cuts short, or shares a content piece. They also track users' engagement with content creators based on if a user views their profile, follows a creator, and engages with their videos. These data points, along with data on user demographics, are used by machine learning algorithms to provide more targeted video recommendations. The size of a user base drives both the complexity and effectiveness of VSP engagement-based algorithms, which gives large-scale VSPs a significant competitive advantage over their smaller counterparts because of access to vast amounts of user data. However, there are safety concerns associated with VSPs storing and processing large amounts of user data.
- **Algorithms are becoming increasingly better at identifying users' niche interests because of two key factors:** (1) it helps to capture users' attention for longer and (2) it enables targeted advertising, which in turn can boost VSP advertising revenues. Algorithms are designed to suggest content to users based on collated data of past viewing patterns. As a result, they can drive users into "rabbit holes" of content by repeatedly suggesting videos on a certain, niche topic. There are ample documented cases of long streaks of eating disorder-related or sexually explicit content being recommended to users (including minors).[6]

[4] Kimball, H. & Cohen, Y. (2019). Children's Mental Health Report: Social Media, Gaming and Mental Health. New York: Child Mind Institute

[5] www.academic.oup.com

[6] www.mashable.com

- **Algorithms designed to recommend videos with higher view and engagement rates often suggest more provocative or extreme content.** A 2021 report by Mozilla found that 71% of all videos reported as harmful by the volunteers were suggested to them through the recommendation engine.[7] Facebook's 2018 internal report found that 64% of the people who joined extremist groups on the platform did so after being steered by the algorithm.[8] Some VSPs have taken steps to reduce the spread of legal but potentially harmful content by removing certain topics from recommendation algorithms. Instagram, for example, has limited recommendations of content involving self-harm, suicide, and eating disorders, among other topics.[9] However, there is a need to address the use and core design of algorithms by platforms more broadly to effectively protect vulnerable users from exposure to harmful subjects.

Given how effective recommendation algorithms are at increasing user time spent on platforms, we expect algorithms to remain a focus for VSPs and a growing safety risk in the future. VSPs differ in how much of the content they show to users comes from the recommendation algorithm — the higher the proportion of that content, the higher the potential safety risk to users. One of the ways to mitigate this is a further increase in transparency to the public and the regulators about the design and impact of the algorithms used.

[7] www.assets.mofoprod.net

[8] www.wsj.com

[9] www.facebook.com/help

APPROACH TO ASSESSING THE RISK OF HARM ON VSPS AND PRIORITISING USER SAFETY ACTIONS

CURRENT VSP APPROACH TO USER SAFETY

Through our research, we found that VSPs regularly need to balance between continuous fast growth and revenue maximisation and doing so in a responsible way that minimises harm to users. That may at times lead to skewed incentives where mechanisms to prevent online harms are only implemented **reactively**, either in response to devastating external events (see case studies below), legal risk or increased regulatory pressure. Existing VSP governance structures and business models often fail to place user safety and well-being at the core of their processes, limiting their capacity to adequately protect users.[1] While VSPs often successfully deploy individual user safety measures, which we discuss later in this section, what is not yet more prevalent in the sector is a comprehensive, systemic approach to proactive identification and mitigation of risks to user safety.

The future introduction of a risk-based Online Safety regulatory framework that puts additional emphasis on preventative systemic checks and balances is a unique opportunity for a step-change in the overall process of how VSPs (especially those not regulated under the existing VSP regime) approach the management of the risk of harm to users.

In recent years, there are many instances when only a devastating external event triggered more decisive responses from VSPs, partially to address external pressures from the media or the public (see case studies below).

[1] www.datasociety.net

CASE STUDY 2

In 2017, 14 year old Molly Russell committed suicide in after viewing graphic content linked to anxiety, depression, self harm and suicide on a VSP platform. The tragic incident sparked a public outrage and an investigation into the consequences of the VSP's algorithms on children's mental health. It also resulted in some VSPs taking action through:

Commitment to identifying and removing graphic content related to self harm and suicide (including drawings, cartoons and memes)

Introducing restrictions on content promoting suicide and self harm (incl. pledges to exclude it from being recommended by the algorithm, alongside a number of other content categories such as misinformation and violence)

One of the root causes of the current state of user safety in the VSP space is **insufficient embedding of user protection and risk management considerations throughout the whole lifecycle of product development**, driven also by the setup of internal governance structures.

At present, responsibility for users' safety and wellbeing is commonly delegated to 'trust and safety' teams. While the introduction of these teams is a step in the right direction, for now they rarely have sufficient influence and authority to impact the decisions made by product managers or engineers.[2] Further empowerment of these teams and their involvement throughout the product lifecycle could facilitate the development of new features in a manner that better mitigates unintended, harmful consequences for users. The challenge is even higher for smaller VSPs that may lack the resources to have any staff responsible for managing trust and safety considerations.

Despite existing protection measures, the majority of users continue to experience online harm on VSPs. According to the Ofcom Pilot Online Harms Survey 2020/21, 76% of users report having been exposed to at least one type of harm online at the time of responding. The harms include both (1) harmful materials (videos, posts, pictures and other content) encountered by users and (2) harmful interactions, such as messages or bullying, also referred to as contact harms.[3]

[2] www.datasociety.net

[3] www.ofcom.org.uk

CASE STUDY 3

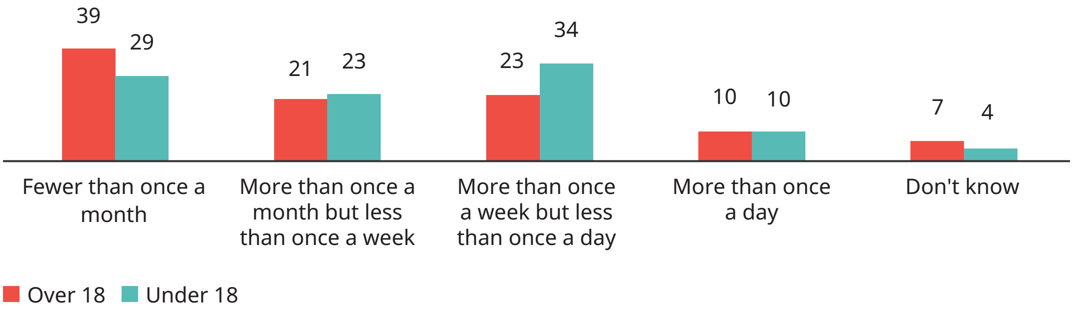
In 2019, a gunman killed 51 people in a shooting in two mosques in Christchurch, New Zealand. The attacker livestreamed the massacre via a VSP and videos of it spread online. The incident sparked a public outrage and questioning of detection systems used by VSPs to identify and eliminate graphic violent content. In response:

Some VSPs addressed the issue by **re training AI video detection systems** to more accurately identify violent content and reduce the detection time (crucial in the context of livestreaming)

VSPs, other tech platform providers and governments around the world pledged to eliminate terrorist and violent extremist content online as part of supporting **The Christchurch Call to Action**.[4] Through the initiative, the Global Internet Forum to Counter Terrorism (GIFCT) which was originally set up as an industry led initiative, has become an independent entity

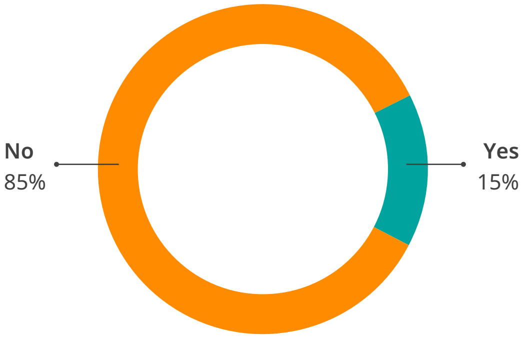
[4] https://www.christchurchcall.com/

Exhibit 19: Frequency of encountering harmful video content by survey respondents, by age group, Percentage



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

Exhibit 20: Percentage of respondents that experienced an inappropriate, distressing, or deliberately misleading interaction on a VSP, full sample



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

In the survey conducted for the purpose of this report, we asked participants how often they encounter the above two types of online harms on VSPs: (1) harmful video content and (2) harmful interactions with other users. We found that:

- Frequency of encountering harmful video content appear to vary by age (see Exhibit 19). The most common response by over 18s is encountering such content fewer than once a month (indicated by 39%), compared to more than once a week among under 18s (34%). Whilst the differences between age groups are very small and insufficient to draw meaningful conclusions, they illustrate the importance of robust safety measures aimed at protecting children online.
- More than 80% of survey respondents reported no experience of inappropriate, distressing or deliberately misleading interactions with other users on VSPs (also referred to as **contact harms**), as illustrated by Exhibit 20. Despite only a fifth of respondents recalling harmful interactions, younger users more commonly reported having experienced such interactions, which points towards a problem of children's safety being compromised beyond harmful content.

ENHANCING A SYSTEMATIC APPROACH TO USER SAFETY

The Online Safety regulatory framework that VSPs are expected to be a part of under the future Online Safety Act will be a proportional and risk-based regime. As such, organisations in scope of the framework will be required to complete risk self-assessments and be subject to supervisory and enforcement regulatory activities applied subject to risk-based principles. As part of the current VSP regime, Ofcom encourages VSP providers to conduct risk assessments to determine the level of risk to users on their service.

In other UK and international sectors where risk-based regulation was adapted, it often led to the regulators developing a broad suite of risk management capabilities (e.g. risk taxonomy, risk scoring, measuring effectiveness of mitigations) and applying them to in-scope organisations. In response, supervised organisations often develop risk management structures mirroring those applied by the regulator — thus allowing them to satisfy the regulatory requirements more easily. Most prominent examples in the UK include financial services and energy sectors.

These precedents from other risk-based regimes outline a unique opportunity for firms in the VSP sector to be on the front foot with regards to implementing robust risk management structures that could later facilitate compliance with the Online Safety regulatory framework.

In this section of the report, we discuss key individual safety measures currently deployed by VSPs and assess how these can be structured to facilitate better user safety outcomes. We lay out one possible framework that incorporates considerations on proactively managing risks to user safety online. In this approach, the main elements cover:

(A) Identification and prioritisation of risks.

(B) Implementation of user safety measures.

(C) Monitoring, reviewing and reporting on the effectiveness of the measures used.

(D) Building the risk management structures and capabilities to enable the entire process.

We also note that this approach typically works in an iterative fashion with steps (A)-(C) repeated in a cycle and enabled by (D), which facilitates accounting for the evolving nature of potential risks (as illustrated on Exhibit 21).

Exhibit 21: A possible structure of a cycle of activities to manage risks to users online

	A IDENTIFY & PRIORITISE RISK	B IMPLEMENT SAFETY MEASURES	C MONITOR, REVIEW AND REPORT
Description	Internally agree on a definition of harmful content and write policies and guidelines accordingly	Select and adopt appropriate measures to mitigate user safety risk	Measure effectiveness of protecting user safety and report progress externally
Key areas of focus	Selection of categories of harmful content relevant for the VSP to explicitly include in policies (General terms and conditions, acceptable use policies and community guidelines) Conducting a risk self-assessment (e.g. in response to externally set regulations and standards)	Age verification and estimation Management of harmful content by the platform (in particular content detection moderation and removal) Empowering users to maintain their own safety by providing them with adequate tools (e.g. user flagging and reporting, user blocking, parental controls) Protecting vulnerable groups (especially children) Enforcement of internal policies (e.g. through keeping team members and senior executives accountable for the safety of users; this could include linking KPIs and bonuses to user safety outcomes)	Choice of adequate metrics for progress tracking and regular transparency reporting

D RISK MANAGEMENT STRUCTURES AND CAPABILITIES ENABLING THE PROCESS

The degree of adaptation of a risk-based approach should be proportionate to a VSP's size and resources

Source: Oliver Wyman analysis

In the subsections below, we discuss individual measures currently deployed by VSPs in areas (A)-(C) and outline possible ways in which they could be further joined in and then describe in (D) the risk management structure that could facilitate this process.

(A) Identify and prioritise risk

With the evolving nature of online harms, there is a growing need for VSPs to define and prioritise risks based on their user base and write internal policies and community guidelines based on their individual risk taxonomies. In addition to illegal content (e.g. terrorism and Child Sexual Exploitation and Abuse (CSEA) content), this requires consideration of a wider range of harms, as there are many forms of legal but harmful content to be addressed.

Our research shows that the current VSP approach for identifying and categorising harms primarily depends on the type of content shared on the platform, the target audience and user base composition, and any relevant regulatory requirements. However, we acknowledge that findings primarily based on publicly available information may offer only limited insights into the internal VSP processes.

We found that the most common categories of content that is explicitly called out by VSPs as forbidden include:

- **Sexually explicit content and safety of minors** (including adult nudity, pornography and sexually explicit content, trafficking, solicitation, child endangerment and sexual exploitation),
- **Hate and extremist content** (including terrorist propaganda and recruitment, violence and violent extremism, organised hate, hateful speech and conduct),
- **Unlawful behaviour** (e.g. illegal and regulated goods),
- **Graphic content** (e.g. suicide, self-harm and dangerous acts, violent and graphic content),
- **Misleading content** (including spam and scams, impersonation, misinformation and disinformation).

Large, established VSPs with a global reach tend to have extensive lists of categories compared to smaller players, highlighting a gap in the existing approach of different platforms. Outcomes of the survey we conducted for this report show the range of content users recall as harmful goes beyond the categories most commonly prioritised by VSPs and also highlight the various ways in which users encounter harmful video content (see section on additional findings from the user experience survey).

Identified harms are often codified in VSP policies and guidelines. For users, this can be in the form of externally facing community guidelines, acceptable use policies, and terms and conditions; whilst for the VSP, in the form of their internal trust and safety policies.

At the time of writing of this report, a small number of established VSPs (e.g. Twitch, Facebook) published materials outlining internal processes that aim to ensure their policies and risk categories are reviewed on a regular basis.[1, 2] Inputs into this process may come from focus groups of VSP employees or external stakeholders: creators, academics,

[1] www.safety.twitch.tv

[2] www.transparency.fb.com

NGO members or the outcomes of regularly published voluntary transparency reports. Going forward, as consumption and sharing of video content continues growing and new categories of risk emerge, VSPs can benefit from introducing voluntary internal risk assessments as a mechanism to regularly revise and update the types of risk their safety measures aim to minimise.

(B) Implement safety measures

Safety measures deployed by VSPs incorporate a wide swath of activities intended to minimise users' risk of harm. Effective mitigation of online harms requires VSPs to select and implement measures of sufficient scope to address the wide range of risks that users can face when using the platform. Our research shows that VSPs vary in their choice of safety measures implemented. In this section we outline some of the key categories of safety measures used by VSPs and provide detailed insights into users' perspectives of safety features encountered on VSPs, based on outcomes of our user survey.

Age verification and estimation is one of the most common approaches used to protect children from exposure to harmful content. Robust age verification and age assurance measures are critical to prevent underage users from accessing age-restricted platforms or content. However, despite advancements in age verification and assurance technologies, many VSPs still rely on basic self-certification processes which can be easily bypassed and provide limited protection for underage users.[3] For example, more sophisticated age estimation techniques can analyse biometric data (such as facial images or voice data) or behavioural data (touch-screen usage, tapping habits, vocabulary, or text-based analysis) to assess a user's age. Some existing solutions, such as the Yoti App, are connecting age verification and estimation methods with the concept of Digital Identity (virtual form of personal identification through which people can legally prove who they are, an alternative to physical credentials - also see glossary of key terms).[4]

As many VSPs attract teens and young adult users, there are growing concerns around the **protection of underage users**. For pre-teen users, VSPs must win over parents by promising age-appropriate content and emphasising how platforms facilitate learning. As a result of growing external pressure on VSPs to step up when it comes to protecting children from online harms, some VSPs have started introducing additional safety measures. These include:

- Creating dedicated platforms for children (e.g. YouTube Kids, LEGO VIDIYO),
- Additional default privacy settings for children accounts,
- Reducing access of minor's data to advertisers to limit or ban targeting children based on interests or browsing history,

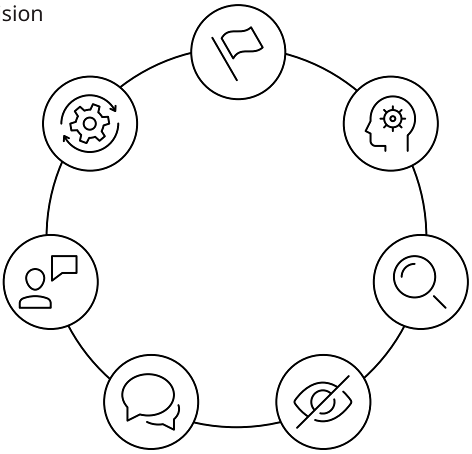
[3] www.ieeexplore.ieee.org

[4] www.yoti.com

- Disabling auto-play for underage users,
- Making safety resources aimed at children and teenagers (e.g. on the topic of eating disorders) available on platforms,
- Proactively identifying adult accounts that could engage in harmful interactions with younger users and taking actions to prevent it (for example by eliminating or blocking that accounts' interactions with minors on the platform).

However, our research shows that recommendation algorithms continue to pose a great risk of directing underage users to inappropriate or harmful content, as referenced in section on engagement-based algorithms. [5, 6]

Exhibit 22: Illustrative journey of a user flag



1. Creation
User reports content they believe is harmful

2. Consideration
User report is reviewed automatically or routed to a human moderator based on the type of content

3. Investigation
Content is investigated, resulting in a decision on whether it is kept or removed

4. Removal
If removed, the user who posted the flagged content is warned or banned from the VSP

5. Dispute
Users whose content was flagged may have the opportunity to dispute the decision to exclude them from the VSP, but the content is likely to remain removed

6. Communication
Users who flagged harmful content may be informed of a if their flagging resulted in content removal or a ban, but will not be told of other outcomes or given the opportunity to dispute decisions

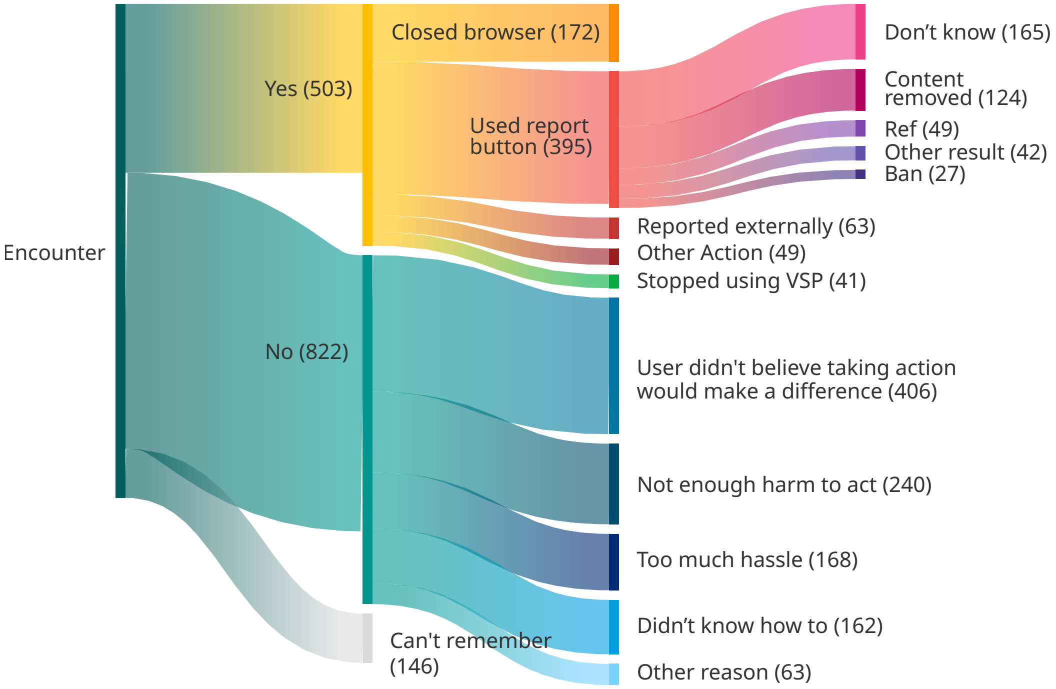
7. Refinement
When machine learning algorithms are used, the moderation decision may be fed into the system as a data point to improve the automated filtering system

Source: Oliver Wyman analysis

[5] www.wsj.com

[6] www.wsj.com

Exhibit 23: User reactions to encountering harmful content on VSPs



Ban: Account removed
Ref: Referred to advice on staying safe

Note: users were able to select multiple responses following the initial question whether they took action

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

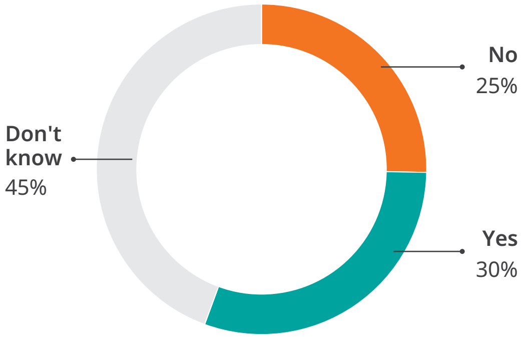
VSPs manage harmful content on the platform through methods geared towards its detection, moderation and removal. **Content moderation** incorporates human-led, machine-led, and "human in the loop" tools. Increasingly, systems leverage a "human in the loop" approach where automated machine learning (ML) software can review content at scale and with speed, while humans can review ML decisions and resolve nuanced questions of harm. Automated moderation tools are typically used for content filtering, including natural language processing and detection of illegal content through hash databases (also see glossary of key terms). In database management systems, hashing is a technique to directly search the location of desired data in a database without having to go through of its elements. From a database of known illegal images and video files, unique IDs or hashes are created to represent each image, which can then be used to identify other instances of those images. Hashing databases are used in detecting Child Sexual Exploitation and Abuse material (CSEA) and other types of illegal content.

Other automated moderating tools include restrictions on who can share content (e.g. requiring users to watch a video before sharing it, limiting comments to users who have watched a livestream for a period of time etc.).

Many VSPs have sought to empower users to maintain their own safety by providing them with a range of tools, such as options for blocking other users, parental control mechanisms and functionalities that allow all users to **flag and report potentially harmful content** (see Exhibit 22). The latter is a collective protection mechanism, through which users can protect others by reporting a piece of content they have encountered and believe to be harmful. Human-led moderation is typically employed to review user flags, decide on contextually or culturally specific content (e.g. sarcasm), and apply community guidelines in unclear situations (e.g. images of nudity used for breast cancer awareness). Users represent an important stakeholder in the content moderation process, but only if systems can effectively react to user flags.

Exhibit 24: Respondents' beliefs on other users reporting harmful content

Do you believe other users report harmful content?

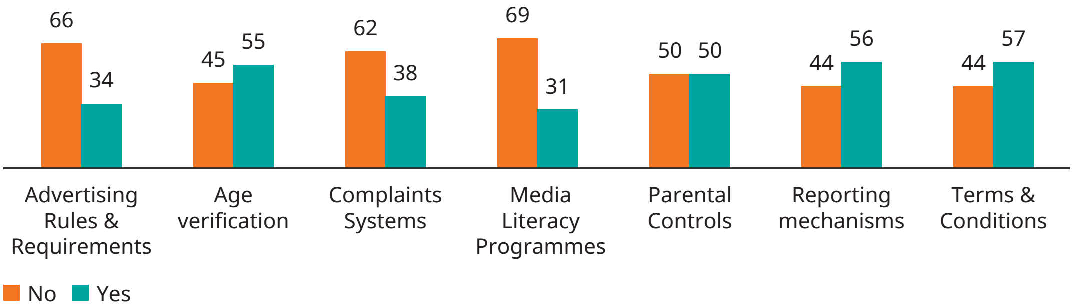


Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

Some VSPs additionally allow certain users or user groups to issue higher level flags, such as YouTube's Trusted Flagger Programme.[7] Typically in such cases NGOs, academics, and other reputable organisations are given special authority to detect and raise alarm about harmful content. Other VSPs leave content creators a choice as to the selection of manual and automated moderation tools they can implement to moderate user comments and engagement in their content.[8]

Exhibit 25: Safety features encountered by respondents on VSPs, Percentage

Have you previously encountered [safety feature] on a VSP?



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

[7] www.support.google.com

[8] www.help.twitch.tv

Our research found that existing user flagging processes often fall short of protecting users from harm due to a lack of transparency and timeliness in responding to reports from users.

- Among the survey participants who reported encountering harmful content, most respondents (822, ~55%) did not take any action in response (see Exhibit 23). The most cited reasons were a belief that they would not be able to make any difference (406, ~49%), or the opinion that the content they encountered was not harmful enough to cause them to take action (240, ~29%). We observe close to no effect of age on reasons not to take action in response to viewing harmful content, when comparing different age groups.
- A small group of all respondents (146, ~10%) could not remember how they reacted to the encounter of harmful content and were not asked any further questions. Those who reported taking action were given a list of five options to select from: clicking the report button, reporting to other authorities outside of the VSP, stopping using the VSP, closed app or browser and other. Of the respondents who took action, using the report button was the most common response (395, ~78%), followed by closing the VSP/browser (172, ~34%). Rarely, respondents would report the content to external authorities beyond the VSP (63, ~12%), or choose to stop using the VSP entirely (41, ~8%).
- We further asked users who indicated having reported the harmful content, about the outcome of their action, providing five options: site removed content, referred to advice on staying safe, user account shut down, do not know and other. The majority of users who clicked the report button did not know the outcome or resolution of their report (165, ~42%). On the other hand, 124 (~31%) of respondents believed their report contributed to the removal of the harmful video, and a small minority were referred to other materials on staying safe (49, ~12%) or believe they contributed to the banning of the user who posted the video (27, ~7%).
- When asked about their perception of other users' reaction to seeing harmful content, 45% of users did not know if others would report harmful content if they encountered it. A further ~25% do not believe others report harmful content (see Exhibit 24).

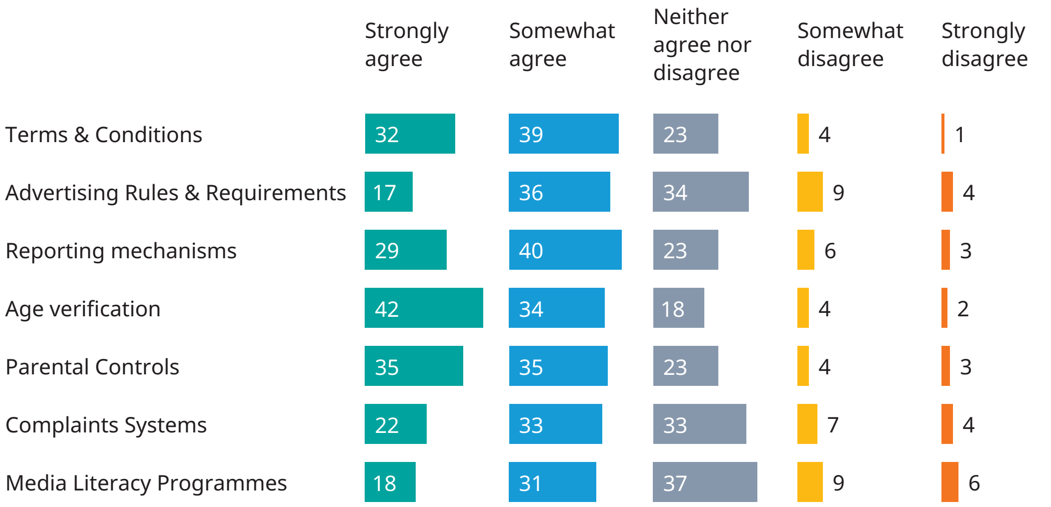
Survey findings suggest high variety in how users respond to video content they consider harmful and may imply a potential need for greater digital media literacy efforts geared towards VSP users to empower them in effectively protecting themselves online. For example, better educated users may be able to better recognise and use available safety measures (e.g. parental controls, flagging harmful content, etc.).

Lack of certainty in being able to make a difference by taking action when encountering harmful content and lack of transparency as to the outcomes of action when it is being taken may discourage some users from acting altogether.

One of the ways to increase transparency in the user flag process is to keep the reporting user apprised of the progress of the review process and the outcome of the review. Users could also be informed about the appeals process should they dispute the outcome. Additionally, to improve the overall effectiveness of user flagging, the time between flagging of content and its subsequent review by a moderator should be minimised.

Exhibit 26: Respondents’ views on being able to recognise selected safety features if they encountered them on VSPs, Percentage

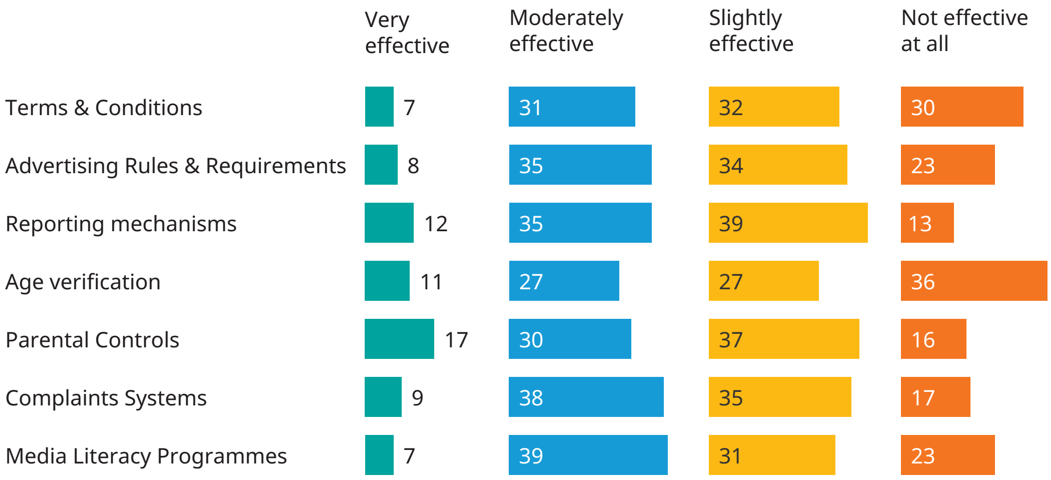
Do you agree with the following statement: I would be able to recognise [safety feature] if I encountered it while using a VSP.



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

Exhibit 27: Respondents’ views on effectiveness of selected safety features in managing the presence of harmful content on VSPs, Percentage

How effective do you believe [safety feature] is in managing the presence of harmful content on VSPs?



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

The user experience survey provides further perspectives on users' perception of selected safety features available on VSPs, including their perceived effectiveness. Despite large proportions of respondents reporting they had not encountered many safety features listed in the survey, most also agreed they would be able to recognise each of the safety features if they encountered it on a VSP.

Advertising rules and regulations, and media literacy programmes, were the two safety features which the fewest respondents had encountered (with 66% and 69% of respondents reporting no previous encounter with each feature, respectively), as shown in Exhibit 25. The same two features were also least likely to be recognised by respondents. In comparison, the most frequently encountered safety features were age verification, reporting mechanisms and terms and conditions (see Exhibit 26).

Most respondents also indicated each safety feature to be at least somewhat effective at managing harmful content (see Exhibit 27). Age verification and terms and conditions scored the lowest ratings of self-reported belief in efficacy. In comparison, parental controls and reporting mechanisms scored highest with the largest proportion of users believing they were moderately or very effective. Given these effectiveness ratings are based entirely on users' own beliefs, they are not necessarily reflective of the real efficacy of these safety features when deployed in the real world.

Finally, in order for the safety policies and measures implemented by a VSP to be effectively deployed across the platform, there is a need for internal enforcement mechanisms. This could be done for example through keeping senior executives and key decision makers within the VSP accountable for the safety of users or partially linking Key Performance Indicators (KPIs) and bonuses to user safety outcomes.

(C) Monitor, review and report

In addition to defining risks and introducing measures aimed at mitigating these, there is a need for regular monitoring of VSP effectiveness and progress in protecting user safety online. Outcomes of internal monitoring efforts can then serve as evidence for ongoing reviews of existing user safety measures, help identify gaps and motivate the need to implement adequate changes. In addition to sharing the results of monitoring internally, publishing external reports on progress year-on-year can increase transparency and accountability of VSPs when it comes to user safety efforts.

Our research shows that some VSPs (e.g. YouTube, Facebook, Twitch) issue regular voluntary transparency reports which are available to the public. A 2021 industry survey of technology platform providers estimated that ~50% of companies publish transparency reports.[9] However, this is likely to be much less common among VSPs given that transparency reporting is just beginning to be introduced among large and established platforms, while it remains a rare occurrence among smaller VSPs. Recent initiatives to issue public transparency reports have increased visibility of VSPs' efforts to protect user safety.

As laid out in guidance for Video Sharing Platforms regulated under the UK's VSP regime, Ofcom intends to publish reports, the first of which will be in the autumn of 2022, with the aim of providing transparency on (1) industry's progress in protecting users, and (2) progress made by Ofcom against published priorities.[10]

At the time of writing this report there were no regulatory guidelines or standards relating to transparency reporting. Consequently, when reports are published, the information disclosed is entirely at the discretion of the VSP. Examples of information shared in published VSP transparency reports include:

- Statistics on content removal and account termination (including breakdowns by removal reason, geography),
- Statistics on content removal appeals and account reinstatements,
- Violative View Rate (metric that represents the percentage of videos including harmful content viewed on the VSP over a set period of time),
- Source of first detection (e.g. automated flagging, user reporting, individual trusted flaggers, NGOs, government agencies),
- Information on legal and law enforcement requests,
- Description and rationale behind changes to the community guidelines and policies.

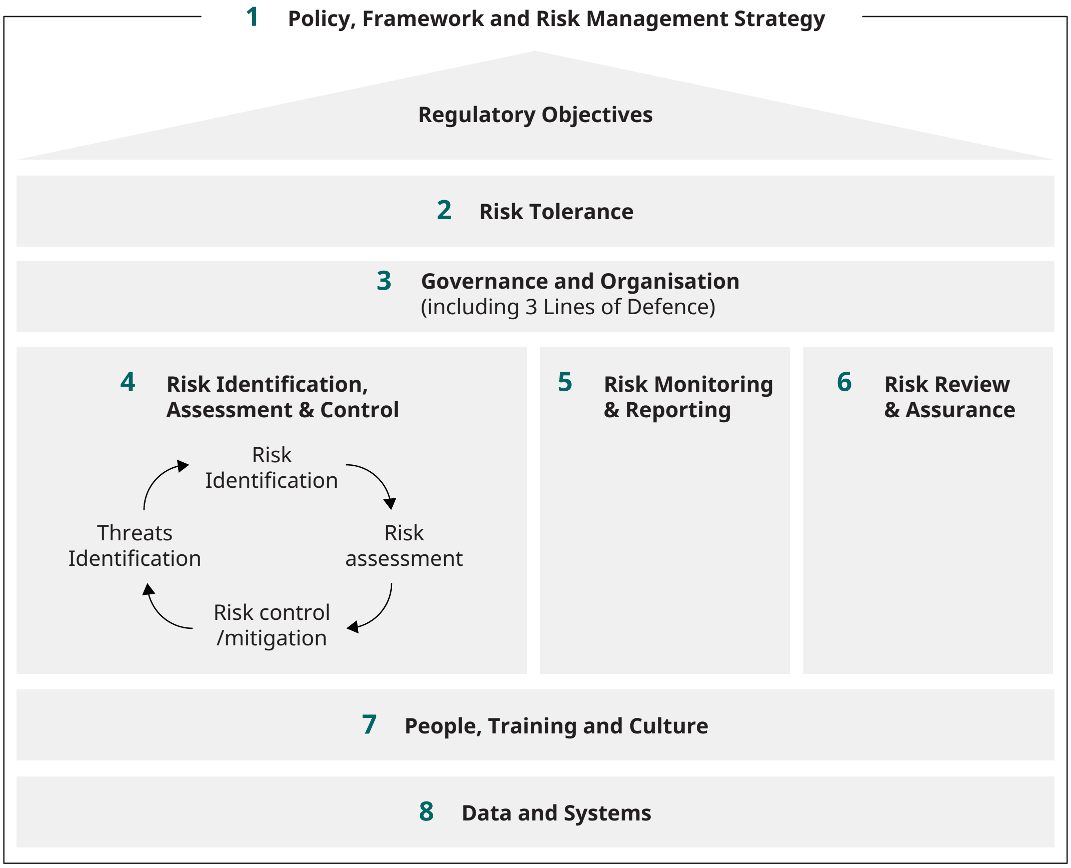
While transparency reports increase the visibility of VSPs' actions in the context of user safety, in their current form they provide an incomplete picture, with little to no opportunity to compare outcomes across platforms. Allowing independent researchers and third parties access to the underlying data behind transparency reports could provide an additional way to validate assertions.

Monitoring and reporting of the effectiveness of VSP safety measures can have the most significant impact if done consistently by VSPs which then use the results to inform decisions about further improvements needed to the existing methods. Going forward, if adopted widely, voluntary transparency reports could become a source of information for the regulator and feed into the process of monitoring the VSP sector's progress. In this context, standardisation of the reported metrics across VSPs could facilitate better comparisons.

[9] www.weprotect.org

[10] www.ofcom.org.uk

Exhibit 28: Overview of an example risk management framework used by organisations in risk-based regulatory regimes



1 Policy, Framework and Risk Management Strategy

Regulatory Objectives

2 Risk Tolerance

3 Governance and Organisation (including 3 Lines of Defence)

4 Risk Identification, Assessment & Control

5 Risk Monitoring & Reporting

6 Risk Review & Assurance

7 People, Training and Culture

8 Data and Systems

1. Risk frameworks are at **various levels of maturity** across risk-based organisations and vary significantly by sector

   Some organisations have developed detailed procedures/ toolkits documenting practical measures for framework implementation

2. Most risk-based organisations have **qualitative** Risk Assessment statements for major risks, but these are sometimes limited in their practical application

   There are a few risk-based organisations that have **calibrated thresholds / risk tolerance** to monitor risks and enable prompt mitigation actions

3. Level of **formalisation** varies across risk-based organisations, clarity is often lacking around responsibilities & accountabilities in both 1st or 2nd Line of Defence

   Most risk-based organisations have a **centralised risk function** (often very lean)

   Increasing number of organisations have appointed a **Chief Risk Officer** or equivalent

4. Most risk-based organisations classify **risks into broad categories** and have identified their top risks for prioritisation

   Risk & control assessments processes are commonly applied

5. Most risk committees at benchmarked organisations monitor risk quarterly (or with higher frequency)

   Some have a **clearly defined list of Key Risk** Indicators and reporting templates for major risk categories

6. Most risk-based organisations have a formalised review processes, consisting of both regular, **management and independent reviews** (2nd/3rd Lines of Defence)

7. Many risk-based organisations have **small risk teams** with limited resources and are working to expand their time size & capabilities

   Most are focusing on **improving their risk mindset and culture**

8. Most risk-based organisations use spreadsheet based **risk registers** to support the risk identification and management processes, a few have implemented a **centralised risk & compliance system**

Source: Oliver Wyman analysis

(D) Building risk management structures and capabilities to enable the process

Elements outlined in steps (A)-(C) can be further strengthened by the set-up of a broader, comprehensive risk management framework by firms in the VSP sector.

As outlined at the beginning of the section, regulators in other risk-based regimes often develop risk management frameworks (e.g. risk taxonomy, risk scoring). In-scope organisations in these regimes often develop internal frameworks that mirror the framework applied by the regulator to minimise the risk to their statutory objectives. Successful frameworks often share several common features:

Firstly, the risk management strategy is driven by and has full buy-in of senior management, providing an additional catalyst at all layers of the organisation and assurance of a common direction.

Secondly, the risk tolerance is consciously set ahead of time and proactive decisions are made about the level and types of risks accepted, as opposed to an ex-post default acceptance after the risks have already materialised.

Exhibit 29: Potential high-level steps taken by organisations in other risk-based regulatory regimes to set up a risk management framework

Framework component design	**Risk tolerance setting**	**Risk management operations**	**Target operating model**	**Ongoing engagement and review**
Review regulatory expectations (many firms will choose to mirror their risk management structure to regulators) Review risk mgmt. approaches of peers If part of a broader organisation, determine extent to which risk management frameworks will be standardised/ integrated If evolving pre-existing risk framework, make strategic choice on future direction	Establish or evolve risk tolerances, as required Define risk tolerance level for each objective/ priority area Assess relevance of any emerging legislation / policy changes on risk tolerance statement and thresholds	Decide how operational aspects of risk management need to evolve as a result, including: • Risk assessment methodology • Risk monitoring & reporting • Risk review and assurance Identify supporting infrastructure modifications needed to enable the changes (e.g. internal systems, data interface with supervised organisations)	Identify deparment/ team structure changes needed Adjust the governance structure & reporting processes where required Identify capabilities required, and - if required - conduct a gap analysis compared to the current state Communicate changes internally to firmly embed risk management culture in the organisation	Continue to engage with the industry and regulator to stay on top of emerging risks Conduct regular horizon scans to ensure risk tolerance thresholds are appropriate Conduct regular internal reviews to test risk strategy embeddedness

Source: Oliver Wyman analysis

Thirdly, the robust processes outlined in the previous section are underpinned by strong risk management capabilities and the infrastructure necessary to collect meaningful data and track progress in mitigation.

Lastly, a strong risk culture defined as the behavioural norms of a firm's personnel with regards to risks presented by strategy execution and business operations. For organisations in sectors that are undergoing risk-based regulatory changes, embedding such a culture helps to prevent harm to consumers or users and builds additional safeguards that go beyond the codified processes.

At present, these processes and capabilities in the VSP sector are only nascent. There are however several high-level steps that have been taken by organisations in other sectors where risk-based regulatory regimes have been set up (illustrated on Exhibit 29).

To stay on the front foot ahead of the introduction of the future Online Safety framework, VSPs could start exploring the possibility of taking similar steps to better prepare for the implementation of the upcoming regulatory regime.

FUTURE EVOLUTION OF THE VSP SECTOR AND IMPACT OF TRENDS ON USER SAFETY

The VSP industry has grown significantly in recent years and we expect it to continue to dynamically evolve in the future. **We frame our analysis of the future state of the sector by considering how VSP business models and their revenue streams are likely to evolve going forward in response to different industry trends.** Based on our analysis, we identify four high-level future scenarios for the VSP sector and assess the implications of each of them for user safety and the wider regulatory environment.

VSP REVENUE STREAMS

Our research shows that currently VSPs rely on three main sources of revenue (also see Exhibit 30): advertisement-based revenue, subscriptions revenue and revenue from other sources (such as in-app purchases), all dependent on user numbers and user engagement patterns. Evolution of VSP business models has been historically shaped by the objective to maximise profitability which resulted in the prominence of ad-based revenues for the largest, most successful platforms. Over time, we expect VSPs to adapt their business models as user priorities and behaviour patterns change.

Exhibit 30: Overview of VSP revenue streams

Advertisement-based revenue

- Most common revenue source for large-scale VSPs where VSP earns money for displaying advertisements to users and subsequent desirable user actions (e.g. purchases of an advertised product) that can be attributed to users encountering the advertisement
- Growing trend towards targeted advertising using algorithms and promoting featured content

Subscription-based revenue

- Subscription-based business models are popular among a variety of VSPs, very prominent for adult content platforms
- Comes in two main forms:
  - One to many subscription (users gain access to a library of content from multiple creators)
  - One to one subscription (users subscribe to select the creator they subscribe to)

Other revenue streams, such as:

- In-App purchases, for example:
  - Virtual currencies through which users can directly support content creators
  - Premium memberships that allows for ad-free viewing
- E-Commerce (e.g. through affiliations with merchants)
- Revenue streams for adjacent offerings

Source: Oliver Wyman analysis

TRENDS IN THE VSP INDUSTRY

We begin our analysis of potential future pathways for the VSP sector by identifying current trends shaping the industry across three key categories: VSP trends, user trends and external trends (see Exhibit 31). We acknowledge the interconnectedness of different trend categories and subcategories of trends resulting from the existence of feedback loops between them (e.g. between external circumstances, user behaviours and VSP business strategies and design choices).

Exhibit 31: Categorisation of VSP sector trends

VSP TRENDS

1 Business strategy and platform content
2 Technical design
3 Governance, compliance and operations

USER TRENDS

4 User preferences and priorities
5 Usage patterns and engagement

EXTERNAL TRENDS

6 Competitive landscape
7 Technology and innovation
8 Regulatory environment

Source: Oliver Wyman analysis

Each of the trends may impact user safety online directly (e.g. tendency for everything to be filmed increasing scale of user exposure to harmful content and endangering user privacy) or also indirectly through its influence on VSP decisions that affect user safety. Our research shows that given VSPs' predominantly reactive approach to user safety, it is likely that factors and trends which may carry reputational and / or legal risks for a VSP may remain the primary catalyst for action when it comes to improving existing safety measures or implementing new ones.

We expect trends with a high potential impact on user safety and VSP business models to be most instrumental in shaping the VSP industry landscape in the future. Exhibit 32 lists the key trends we identified within each category.

Exhibit 32: List of VSP sector trends (non-exhaustive)

	Category	Sub-category and trends
VSP trends	Business strategy	Entrance of VSPs into adjacent sectors, such as gaming, e-commerce functionalities built directly in to VSP interface (e.g. Instagram shops), Virtual Reality and Augmented Reality experiences
		Entrance of VSPs into nonadjacent sectors, e.g. payments, insurance, other financial services
		Enablers of growth in advertising revenue: • Cross-platform linkages, e.g. data integration across platforms for targeting advertising campaigns • More extreme data monetisation practices • Evolution of advertising models by enabling a more targeted approach
		Content monetisation beyond advertising: • Further expansion of UGC and VSP produced content being available on a subscription basis • Introduction of direct user to creator payments (of which VSP may take a cut), such as subscriptions (e.g. Patreon, Onlyfans) and tipping (e.g. Twitch) • Platform-specific virtual currencies (e.g. TikTok coins, Twitch Bits)
	Platform content	Proliferation of new formats of video content: • Short-form videos (<30 seconds) e.g. TikTok, Instagram Reels, YouTube Shorts • Silent video i.e. using captions, gestures, conveying ideas without sound • Growth in highly-edited, graphics-heavy videos • Segmented video formats for a variety of devices (e.g. vertical for handheld devices, square for Instagram)
	Technical design	Advances in algorithm use and capabilities: • Increased use of highly-personalised video recommendations in an infinite-scroll feed • Growing share of total content available to the user from the recommendation engine
		Leveraging user data: • Improved user activity tracking practices by AI and machine learning-based systems • Integration of third party data flows to improve recommendation mechanisms
		Continued application of behavioural insights at design level to nudge desired user behaviours
	Governance, compliance operations	Introduction of new methods of managing and monitoring safety risks (in particular among large VSPs), e.g. transparency reporting, creation of "safety teams", increased usage of Safety Tech / sophisticated AI techniques to moderate harmful content
User trends	User preferences and priorities	Growing video use beyond entertainment: • Continued use of video platforms to support learning / educational content • Rise in the amount of disinformation being spread online • Tendency for everything to be filmed, driving the popularity of livestreaming • Live video shopping
		User preference for easier-to-consume content: • Growth in share of video content on social media relative to text/images • Videos are tending towards shorter formats (e.g. TikTok, Instagram Reels, YouTube Shorts) • Familiar, remixed content from other creators e.g. reaction videos • Standardised storylines where different creators use the same backing music and theme
		Growing consumer interest in monetisation (e.g. subscription-based content consumption)

	Category	Sub-category and trends
User trends	Usage patterns and engagement	Lowering of access barriers: • Increased access to video platforms due to the prevalence of portable personal devices • Decreasing age of digital engagement, resulting in younger generations able to access platforms
External trends	Competitive landscape	Strong competitive pressure among the VSPs • Industry consolidation through acquisitions of VSPs by broader social media platform providers • Tendency for successful new entrants into the VSP space to be acquired by larger platforms
	Technology and innovation	Shift in the structure and uses of the internet: • Increased number of platforms developing technologies to participate in the metaverse • Decentralisation of the internet, increased prevalence of consumer-owned and consumer-controlled content • Increased user adoption of cryptocurrencies, motivating potential new uses in the VSP space
		Increase in digital traffic enabled by the rollout of 5G
		Rise in number of fake accounts/bots being set-up
	Regulatory environment	Tightening of the regulatory environment: • Growing regulatory scrutiny of VSP providers • Increasing focus on advertising on VSPs as a potential source of online harm • Increased reputational risk for VSPs linked to poor safety practices

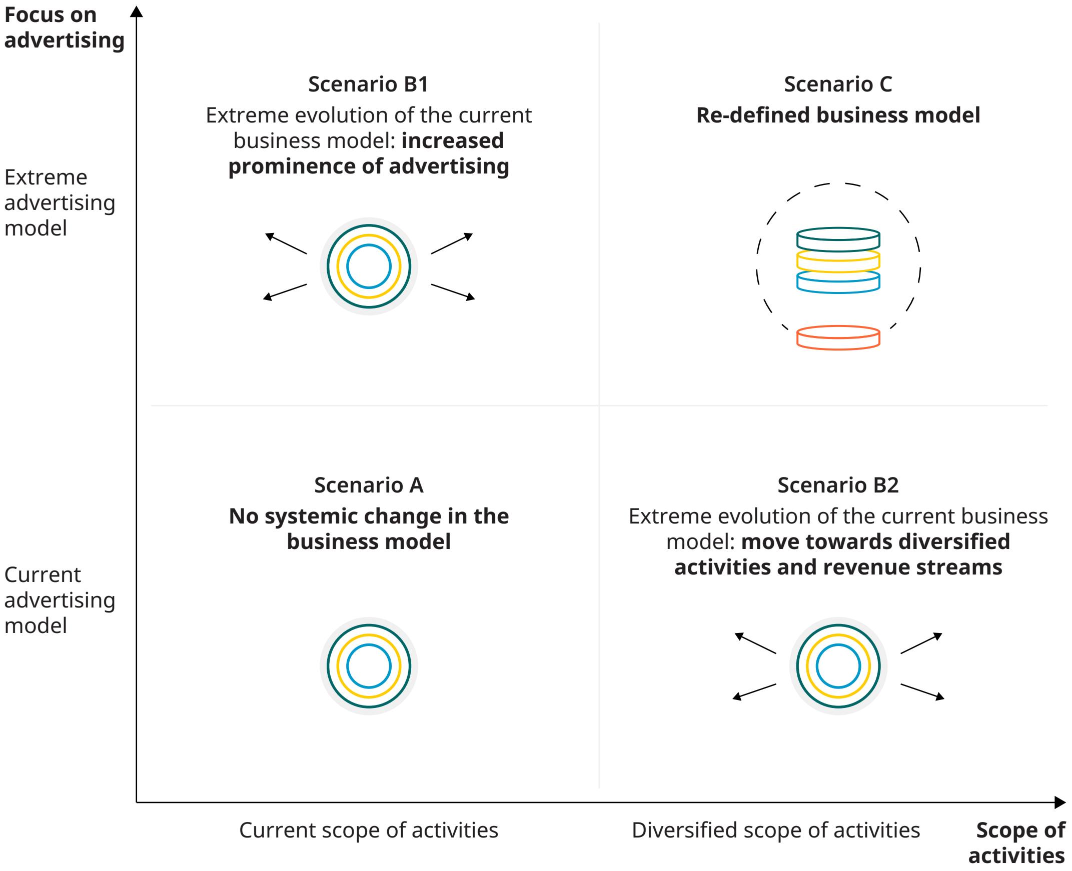
Source: Oliver Wyman analysis

HIGH-LEVEL FUTURE STATE SCENARIOS FOR THE VSP SECTOR AND THEIR IMPLICATIONS

Based on the analysis of industry trends, we identified four potential high-level future scenarios for the sector, using the lens of changes to VSP business models. Going forward we expect that changes to VSP business models may happen across two key dimensions: extent of focus on advertising and scope of VSP activities, as illustrated in Exhibit 33. Each of the scenarios that subsequently arise are dependent on specific trend enablers which would need to continue and grow in significance for the scenario to materialise.

In the remainder of this section, we discuss each scenario in turn and evaluate its potential implications for user safety and the regulatory environment.

Exhibit 33: Potential high-level future state scenarios for the VSP sector



Focus on advertising

Extreme advertising model

Current advertising model

Scenario B1
Extreme evolution of the current business model: **increased prominence of advertising**

Scenario C
Re-defined business model

Scenario A
No systemic change in the business model

Scenario B2
Extreme evolution of the current business model: **move towards diversified activities and revenue streams**

Current scope of activities

Diversified scope of activities

Scope of activities

Source: Oliver Wyman analysis

SCENARIO A

No systemic change in business model

In this scenario, we expect key VSP revenue streams to remain broadly unchanged, with the scope of VSP activities and their appetite for advertising remaining comparable to the current state. However, existing user safety concerns are likely to be magnified by the growing consumption of videos beyond entertainment purposes (e.g. to support learning, live video shopping or regular livestreaming) and as continued growth of total annual videos viewed across all platforms generates more exposure to harmful content (including the growing volume of content shared in real time).

Provided the trends of decreasing age of digital engagement and overall lowering of barriers to access online content (e.g. due to the prevalence of portable personal devices) continue, the total pool of users is likely to grow further, highlighting an increased need for VSPs to implement effective safety measures to ensure an adequate level of protection against harmful content.

Implications for a regulatory environment: In this context, a tightening of the regulatory environment is likely to have the biggest potential to impact on user safety through raising the legal and reputational risk for VSPs which are linked to poor safety practices. Additionally, as user safety concerns are magnified proportionally to the growing scale of the VSP sector, this creates a need for regulators in this space to develop capabilities to monitor the effectiveness of measures implemented by VSPs and, in turn, the effectiveness of the regulatory regime. Based on the review of the collected information, regulatory activity can be adjusted and further monitored, creating a beneficial feedback loop.

Pathways towards an extreme evolution of the current business model

As competition in the growing market intensifies, VSPs are likely to experiment with new ways of attracting users and locking them in, which might lead to one of the other two scenarios materialising: either an extreme evolution of the existing business model or a fundamental re-defining of it.

The impact on user safety in the case of an extreme evolution of the current VSP business model will likely depend on the revenue streams on which the VSPs choose to focus. In this section we consider two possibilities in detail: increased prominence of advertising-based revenue streams and a greater move towards revenue diversification. It is worth noting that whilst not all VSPs may choose the same pathway when evolving their business model, we expect larger players to set the precedence for the industry.

SCENARIO B1

Increased prominence of advertising

Advertising, at the time of writing this report the largest revenue source for most VSPs, may become an even greater focus for platforms going forward if platforms decide to double-down on advertising while maintaining their current scope of activities. Key trends that can further enable this include cross-platform linkages (e.g. data integration across platforms for the purposes of targeting advertising campaigns), more extreme data monetisation practices and advances in algorithm use and capabilities. Large VSPs are already at the forefront of the evolution of hyper-targeted advertising, enabled by recent technological advances in AI and machine-based recommendation engines and fuelled by improved user activity tracking practices.

In this scenario user data becomes crucial, giving large VSPs that can gather and process it a competitive advantage. Techniques such as leveraging data synergies across platforms for targeting advertising campaigns are likely to raise the issues of privacy (user consent for data sharing), data ownership and secure data storage. The severity of the risk increases as new forms of data may be gathered by VSPs in the future, such as facial expressions and eye movements of users participating in shared immersive digital environments.

To maximise the advertising exposure of consumers, more sophisticated algorithms will be needed to keep users engaged and we expect VSPs to continue investing in algorithm and data processing capabilities to maximise the personalisation potential. However, this carries significant user safety risks, as outlined in this section about engagement-based algorithms and may prove challenging for the regulator to effectively supervise given VSP's historical reluctance to be transparent about their algorithms.

SCENARIO B2

Move towards diversified activities and revenue streams

Through our research, we observe a trend for VSPs entering adjacent revenue-generating sectors (such as gaming, e-commerce, Augmented Reality or Virtual Reality experiences) and integrating a growing range of content monetisation methods beyond advertising into their platforms. Moreover, users' appetite for consuming content available on a subscription-only basis and supporting creators via direct payments has been growing in recent years.

In addition to these trends, there may be other, regulation-driven trends which could encourage VSPs to significantly diversify their scope of activities compared to today, thus potentially enabling this scenario to materialise. Firstly, the appeal of advertising may be limited by externally imposed limitations on the use of algorithms by platforms which would impair VSP's abilities to facilitate personalised advertising. Secondly, this could be the case if VSPs were made responsible for the harms caused by advertising content on their platforms and thus compelled to restrict advertising. The EU's Digital Markets Act which intends to impose new obligations on big platforms with significant market power (called "Gatekeepers") could contribute to the tightening of regulatory pressure, for example through new provisions for use of data for the purpose of delivering targeted advertising.[1]

Diversified revenue streams could include in-platform purchases, adjacent revenue streams, subscriptions, use of virtual currencies. There may be significant user safety risks associated, especially as the experience of making payments and transactions via VSPs becomes more seamless for users. These emerging risks necessitate extra safety measures geared towards adolescents and children who may be vulnerable to making payments without a full understanding of the consequences. Additionally, there is a wider need to educate users about digital currencies and crypto assets available for use on VSPs.

Finally, as VSPs add on a variety of additional revenue-generating functionalities (e.g. linked to e-commerce or gaming), these can pose a risk of exposing users to additional harms.

Implications for a regulatory environment: The increase in scale and complexity of user safety risks in scenarios B1 and B2 would likely place particular importance on active use of full supervisory and enforcement powers by regulators in this space to effectively protect users. Regardless of the direction the extreme evolution of VSPs business models may take, new overlaps are likely to arise between regulation of online safety and further regulatory areas, necessitating cooperation with other regulators, such as the Advertising Standards Authority (ASA) and the Competition and Markets Authority (CMA).

SCENARIO C
Re-definition of VSP business model

Far-reaching future industry changes linked to shifts in the structure and uses of the internet (such as widespread participation in the metaverse and rise of decentralised video sharing platforms) may motivate VSPs to drastically re-define their business model in the future. This could involve introducing new, currently unknown revenue streams or drastically transforming VSP's existing value proposition to the user (value proposition is a combination of benefits that the product or service can bring to the consumer). Our research shows that as social media platform providers enter non-adjacent sectors (e.g. financial services) and the web is becoming more decentralised, new possibilities emerge for VSPs when it comes to monetisation and user engagement.

Whilst the precise impact on user safety is hard to define, we can expect risks associated with the need for VSPs to adequately re-define or re-purpose their existing user safety measures such that they can effectively protect users from harms they can encounter when using platforms in new ways.

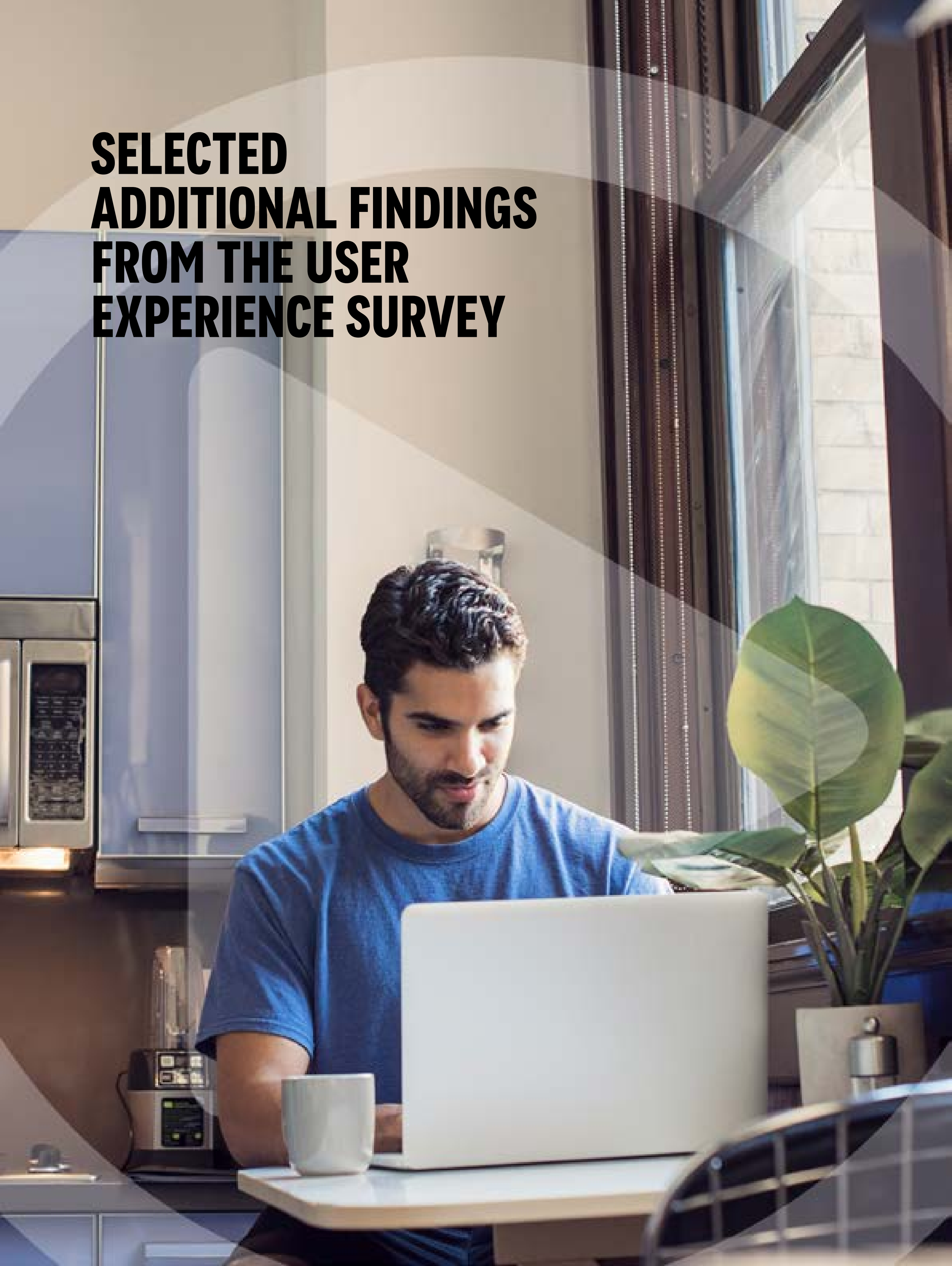
[1] www.consilium.europa.eu

Implications for a regulatory environment: Given that the structure of the business model of supervised platform providers is often one of the root causes of risks in a risk-based regulatory framework, risk-based regulators often develop tools to aid in building a better understanding of potential business model changes.

One of such tools is horizon scanning, which in this space, could be achieved through a regular analysis and assessment of VSP business models and their impact on user safety (e.g. through review of patent applications filed by VSPs or examining mergers and acquisitions (M&A) activity).

In its extreme case, this scenario may even require new regulatory powers if existing powers prove to be insufficient to effectively supervise VSPs under the new business model (e.g. potentially impacting the conversation on the future powers of the Digital Markets Unit). Finally, similarly to scenario B, engagement between regulators that cover scope of the re-defined VSP business model may be required.

SELECTED ADDITIONAL FINDINGS FROM THE USER EXPERIENCE SURVEY



In this section we outline key insights from a user experience survey which was conducted for the purposes of this report in February 2022 on a sample of 2252 UK users of VSPs, including 355 respondents aged 18 or less. The survey's primary focus is on investigating participants' experience of harmful video content on VSPs, through recalling one instance when they encountered content they considered to be inappropriate, distressing, or deliberately misleading. In addition, the survey also provides insights into usage patterns and frequency as well as perspectives on the importance and effectiveness of VSP safety measures. In context of the emphasis on protection of children online present in the upcoming Online Safety regime and current VSP regime, we pay special attention to differences in user experience between under 18s and over 18s throughout the analysis of survey outcomes.

THE KEY FINDINGS WE IDENTIFIED BASED ON THE SURVEY ARE:

1 An overwhelming majority of users agree that they would be able to recognise inappropriate, distressing or deliberately misleading video content on a VSP platform. Frequency of encountering such content differs by age: the most common response by over 18s is encountering it less than once a month, compared to more than once a week among under 18s. This illustrates the importance of robust safety measures aimed at protecting children online.

2 Types of inappropriate, distressing or deliberately misleading video content that users recall having encountered differ depending on whether users describe the instance unprompted or do so after being prompted with a list of possible categories. Irrespective of seeing the list, respondents most frequently recalled instances of fake news and disinformation as an example of harmful content encountered. Violent and disturbing content and inappropriate sexual / pornographic content were other two categories commonly recalled by those who did not see the list.

3 Some harm types frequently described could not be captured in a straightforward way by the existing list of categories. These include examples of content that users considered harmful because of the context in which they encountered it, e.g. through unwanted redirects / suggestions to other (often sexual, distressing or gambling related) materials, unexpected material designed to be misleading and therefore harmful for unsuspecting viewers or videos repeatedly suggested by an algorithm.

4 Most users take no action in response to encountering harmful content. Among those who do, most click the report button — but the majority of users who clicked the report button did not know the outcome or resolution of their report. Our findings point to the uncertainty around the impact of actions taken as one of the key drivers behind users' inaction, implying that improved VSP reporting and transparent communication of results of user flags could empower users to take action more often when encountering harmful content. Furthermore, wider media literacy initiatives could reinforce this.

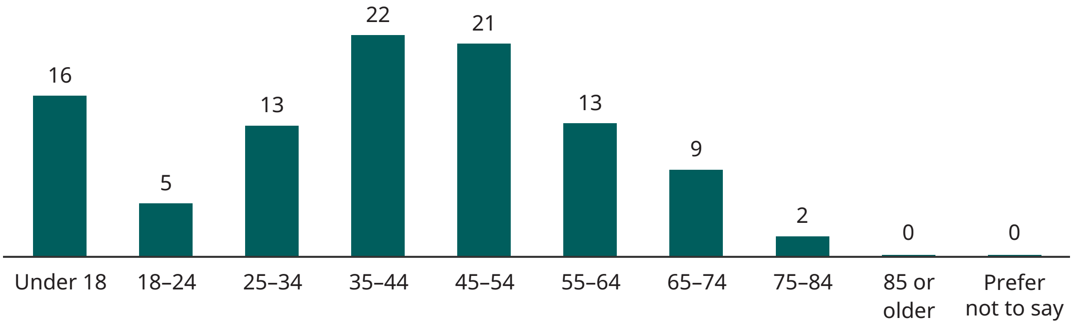
5 Despite large proportions of respondents reporting they have not encountered many safety features listed in the survey (e.g. complaint systems, advertising rules and requirements, reporting mechanisms), most also agreed they would be able to recognise each safety feature if they encountered it on a VSP (see Exhibits 25 and 26). Advertising rules and regulations, and media literacy programmes, were the two safety features which the fewest respondents had encountered, and the same two features were also least likely to be recognised by respondents. Most respondents also felt that every safety feature was at least somewhat effective at managing harmful content, with age verification and terms and conditions being the two safety features with the lowest ratings of perceived effectiveness (see Exhibit 27).

SURVEY DEMOGRAPHICS

Efforts were made to gather a sample representative of the general population demographics of gender, age, and region. These participants were invited to take part in the survey through a panel provider. Despite these efforts, the sample recruited was somewhat imbalanced towards women who comprised 62% of the final sample (see Exhibit 35). There was still considered to be a sufficient number of men to draw reliable statistics and interpretations.

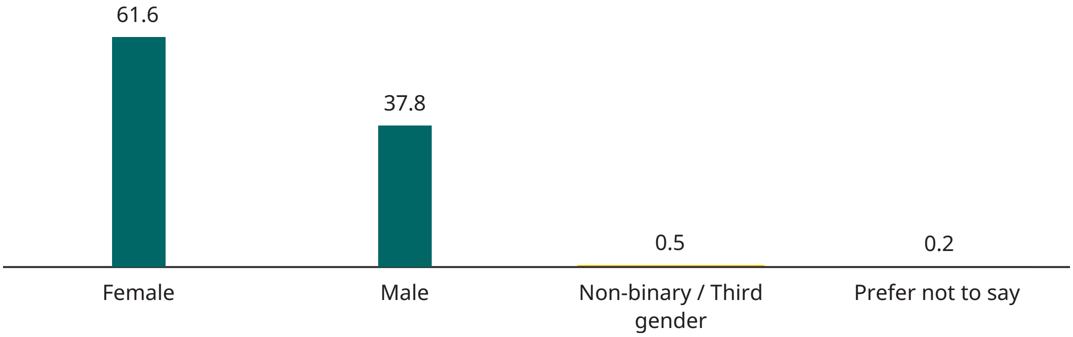
Exhibit 34 shows that the age distribution of respondents was normally distributed around the 35-54 age group, with 486 (22%) aged 35-44, and 468 (21%) aged 45-54. Additional effort was expended to capture a larger sample of respondents under 18, and the total size of this sample was 355 (15%).

Exhibit 34: Age distribution of survey respondents, Percentage



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

Exhibit 35: Gender distribution of survey respondents, Percentage

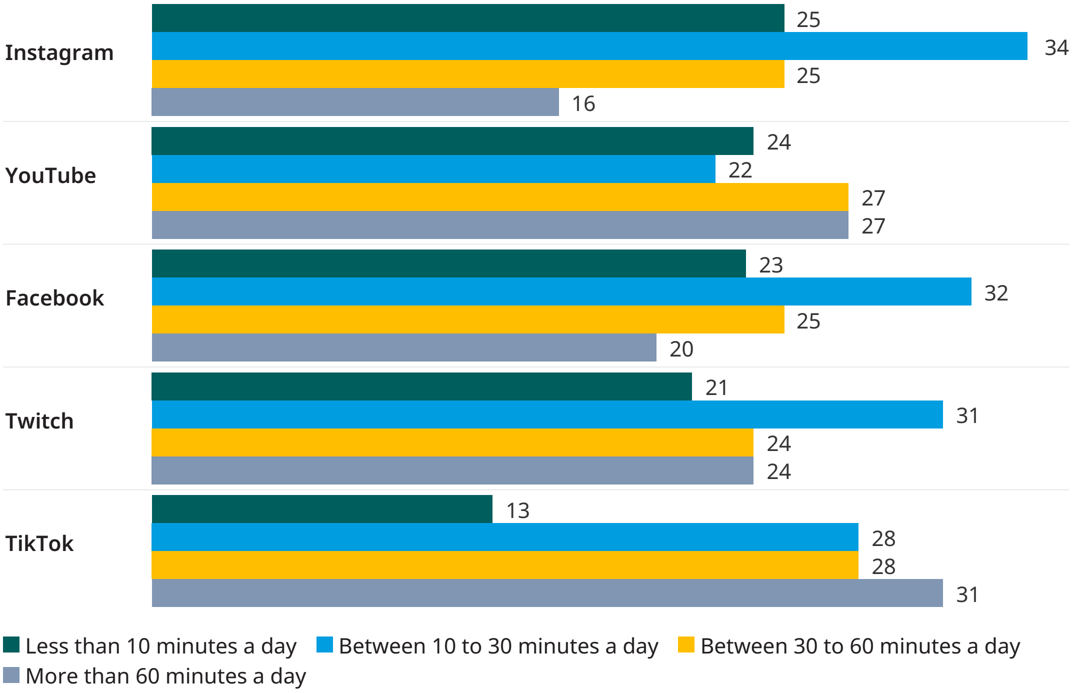


Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

USAGE OF VSPS

Respondents' self-reported time spent watching video content varied between one another, as well as between VSPs, which indicates a healthy sample of a mix of different types of users, e.g. power users (those who are more likely to use platforms' advanced functionalities than the average user), casual users, and those in between. For each VSP they indicated using, respondents were asked about the average time spent watching videos on that platform per day. Exhibit 36 shows that between ~15% and ~30% reported spending more than 60 minutes per day watching content (values vary by VSPs), which exceeds the findings of a previous study done by Ofcom.[1] Instagram users were most likely to report spending between 10 to 30 minutes per day watching videos, compared to TikTok's users most commonly reporting spending more than 60 minutes per day.

Exhibit 36: Time spent watching video content on selected platforms, full sample, Percentage



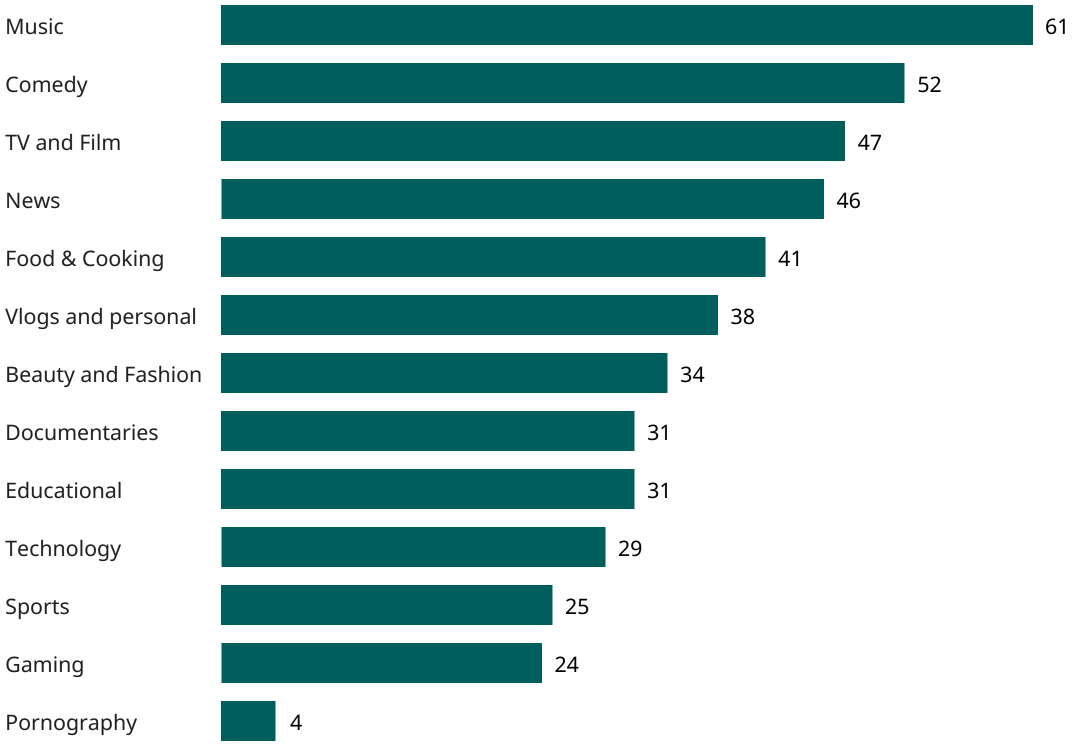
Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

[1] www.ofcom.org.uk

Music videos are the most frequently watched type of video content among all respondents, regardless of their age group (see Exhibits 37 and 38). We observe some genres of video content with very strong age driven skews, in line with expectations. Gaming content is very popular among under 18s (56% of respondents under 18s report watching gaming content) but ranks relatively low for over 18s (18%). Vlogging and personal content appears popular in both age groups, albeit with a higher proportion of under 18s watching (51% of under 18s compared to 35% of over 18s. Three video genres are significantly more popular among over 18s than under 18s: food and cooking content, news videos and documentaries.

Finally, we note that the proportion of respondents who report watching pornography may not be representative, especially for underage respondents who likely did not select this response due to the presence of their guardians when filling the survey and other social factors.

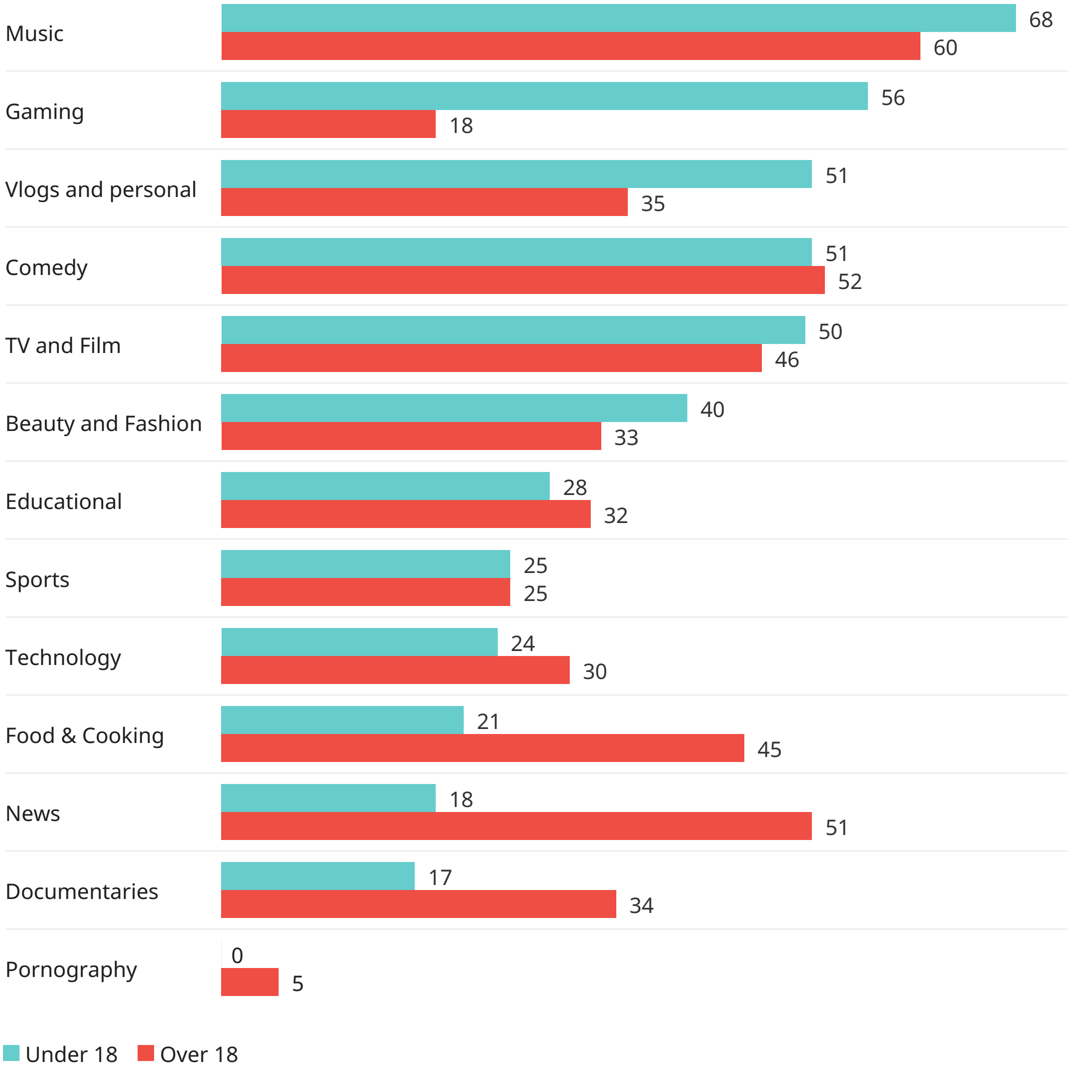
Exhibit 37: Genres of video content users report watching on video-sharing platforms, full sample, Percentage



Note that respondents were able to select more than one genre of video

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

Exhibit 38: Genres of video content users report watching on video-sharing platforms, by age group, Percentage



Note that respondents were able to select more than one genre of video

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

USER EXPERIENCE OF HARMFUL VIDEO CONTENT

(1) Identifying harmful content

Respondents generally believe that they would be able to identify inappropriate, distressing, or deliberately misleading content. The overwhelming majority of respondents agreed with the statement that they would be able to identify such content if they encountered it (see Exhibit 39).

(2) Encountering harmful content

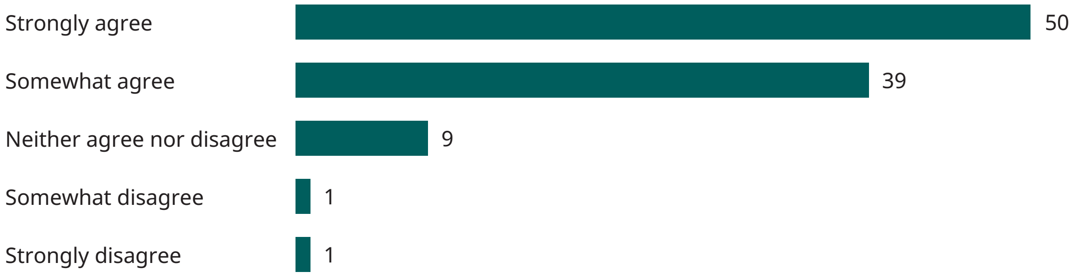
The majority of respondents (55% of the full sample, for both under and over 18 age groups), when first asked, reported that they have not encountered video content that was inappropriate, distressing, or deliberately misleading on VSPs (see Exhibit 40). It is possible that some differences between age groups may be observable when normalising for time spent watching videos on VSPs, as it could be expected that more time online may lead to an increase in the probability of experiencing an instance of harmful content.

Overall, respondents were slightly more likely to report not having encountered such content if asked without being prompted with a list of pre-selected categories of potentially harmful content.

There are several possible explanations for the higher number of "No" responses. It is possible that the breadth of "harmful content" is not entirely captured by the all-but-name

Exhibit 39: Respondents’ view on their ability to identify video content that they consider inappropriate, distressing, or deliberately misleading, Percentage

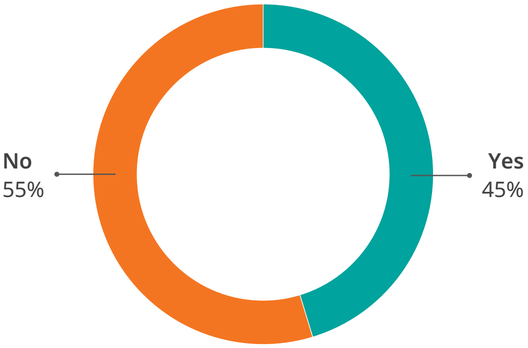
Do you agree with the following statement: I feel that I would be able to identify video content that is inappropriate, distressing or deliberately misleading, if I encountered it on a VSP.



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

definition used in the survey (*"content that is inappropriate, distressing or deliberately misleading"*). Evidence for this can be found when examining the number of items indicated to be encountered by respondents from the list of harmful content categories, which was displayed to the respondents who selected a "No" response. When prompted with the list, only 22% of respondents selected no items at all. Furthermore, it also appears that older respondents were more likely to indicate no prior encounter with harmful content, with the proportion of respondents answering "No" increasing with age.

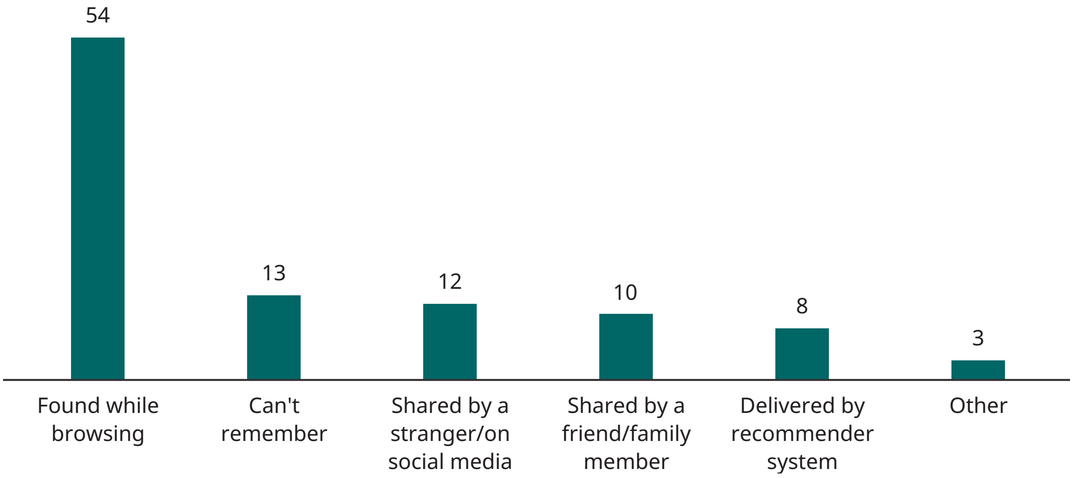
Exhibit 40: Percentage of respondents that report having personally encountered inappropriate, distressing, or deliberately misleading video content, full sample



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

We asked respondents how they encountered the piece of harmful content which they have described in the open-ended question. The majority of users (54%) report encountering harmful content while browsing, with other options being less common. A small but considerable proportion of users report encountering harmful content in ways that are driven by modern developments in VSP technology, such as recommendation systems (8%) which are autonomously driven by an algorithm, as illustrated in Exhibit 41.

Exhibit 41: Ways of encountering harmful content on VSPs, full sample, Percentage
How did you encounter the example of harmful video content which you described?



Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

(3) Recalling a specific instance of experiencing harmful content

In the survey, user understanding and perceptions of harmful content were investigated through focusing on **one specific experience of harmful video content** which the user was asked to recall through an open-ended question approach. Users who could not initially recall an instance were prompted with a list of categories and then again asked for a specific recollection. The list of categories was adapted from categories used in a previous report on User experience of potential online harms within VSPs' published by Ofcom.[1] See Appendix B for details on the flow of the survey.

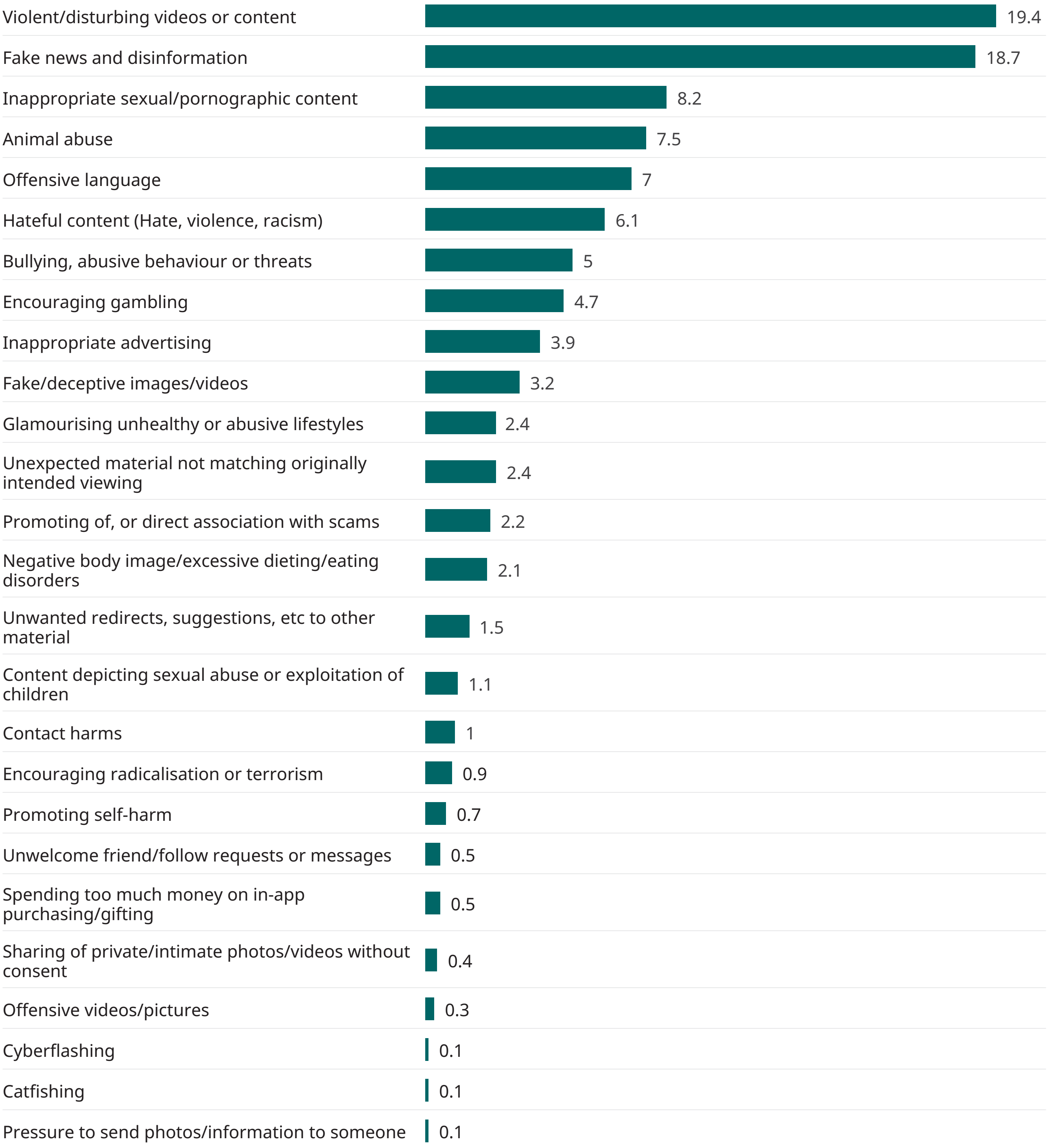
Results of the open-ended survey responses were manually categorised post-collection. In that process we made several observations:

- **Some harm types frequently described in the responses to the open-ended question could not be captured in a straightforward way by the original list of categories.** In order to capture these nuances, we defined and added new categories during the coding procedure in which respondents' qualitative responses were categorised. For example, a large proportion of recalled content that could also be described as violent or distressing pertained specifically to animal abuse, warranting its own category. Other notable categories added include unwanted redirects / suggestions to other material and unexpected material not matching originally intended viewing.
- Respondents also shared details on **how** they came across the harmful video content in addition to **what** the video consisted of. Users recalled instances of:
  - Encountering content that was deliberately designed to be misleading and therefore harmful for unsuspecting viewers (e.g. snippets of inappropriate videos "hidden" in videos on neutral topics, videos of a violent nature, or containing inappropriate language disguised as children's cartoons, materials designed to trick viewers into viewing sexual content),
  - Unwanted video contents, pop-ups and adverts were perceived by users as harmful, regardless of whether they considered the content of the advert to be of an inappropriate nature,
  - Examples of otherwise benign content being suggested to users repeatedly by a recommendation algorithm. Instances where this was recalled as a harmful experience illustrate the previously discussed "rabbit holes" of content (i.e. long streaks of videos centered on a theme recommended to users) which users may be drawn into.

Exhibit 42 shows that across the full sample, two types of harmful content (violent and disturbing content, and fake news and disinformation) were recalled in the open-ended question at least twice as often as the next most frequent category (inappropriate sexual / pornographic content). It is possible that there are underlying mechanisms driving the higher recall rate of these categories, relative to the frequency at which they were recalled when selected from the full list. An example are strong negative emotions surrounding such experiences, which make them more likely to be remembered and recalled by respondents.

[1] www.ofcom.org.uk

Exhibit 42: Categories of harmful content recalled by survey participants in a qualitative response, full sample, Percentage

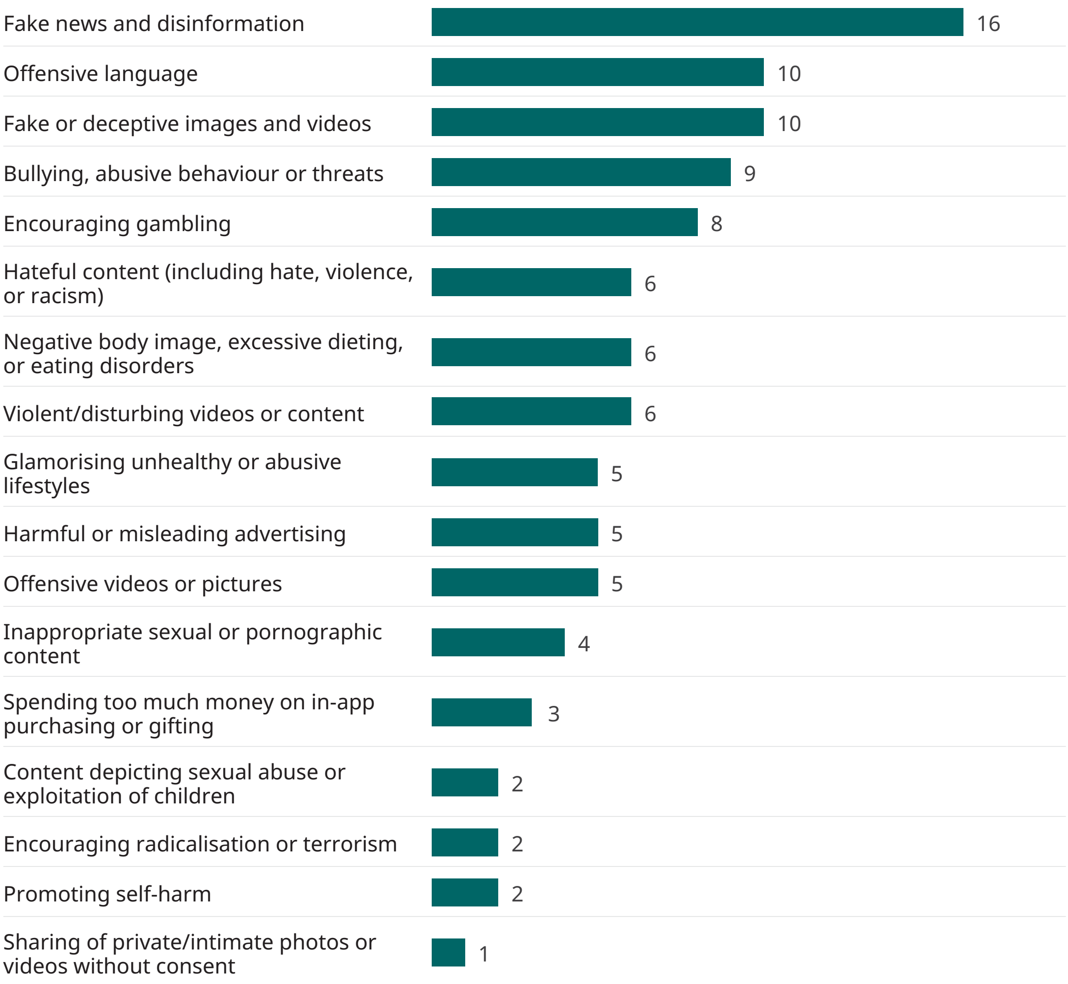


Note: Results of the open-ended survey responses were manually categorised post-collection.

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

Comparison of open-question responses with items selected by participants from the list of harmful content categories implies that the extreme types of harmful content may be less frequently encountered by respondents than some other categories, while noting their severity and lasting impact on users (see Exhibit 43).

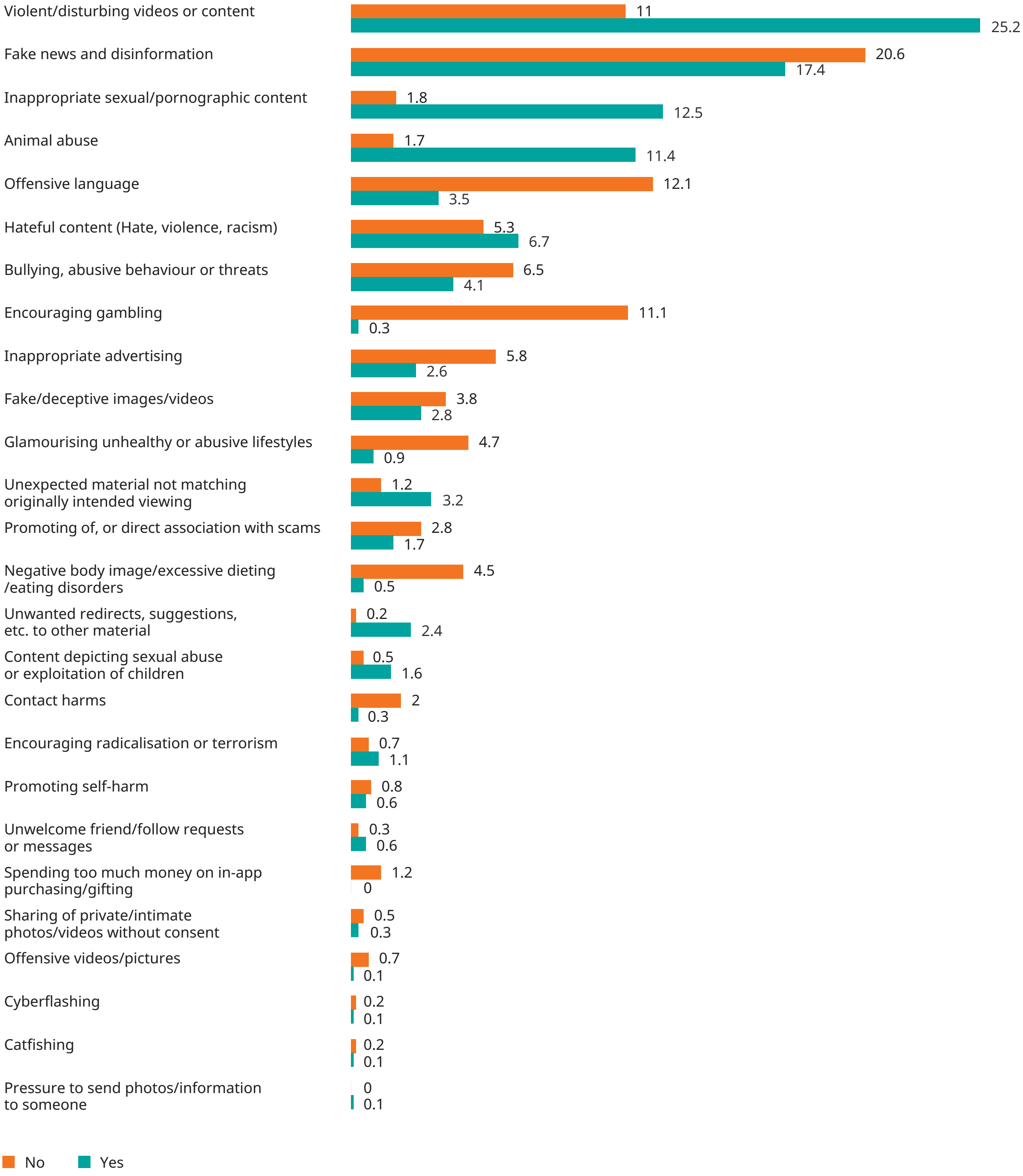
Exhibit 43: Categories of harmful content that survey respondents reported to have encountered, full sample, Percentage



Note: Respondents able to select multiple categories from a list

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

Exhibit 44: Categories of harmful content recalled by survey participants in a qualitative response, by response to the question if they previously encountered harmful content, Percentage



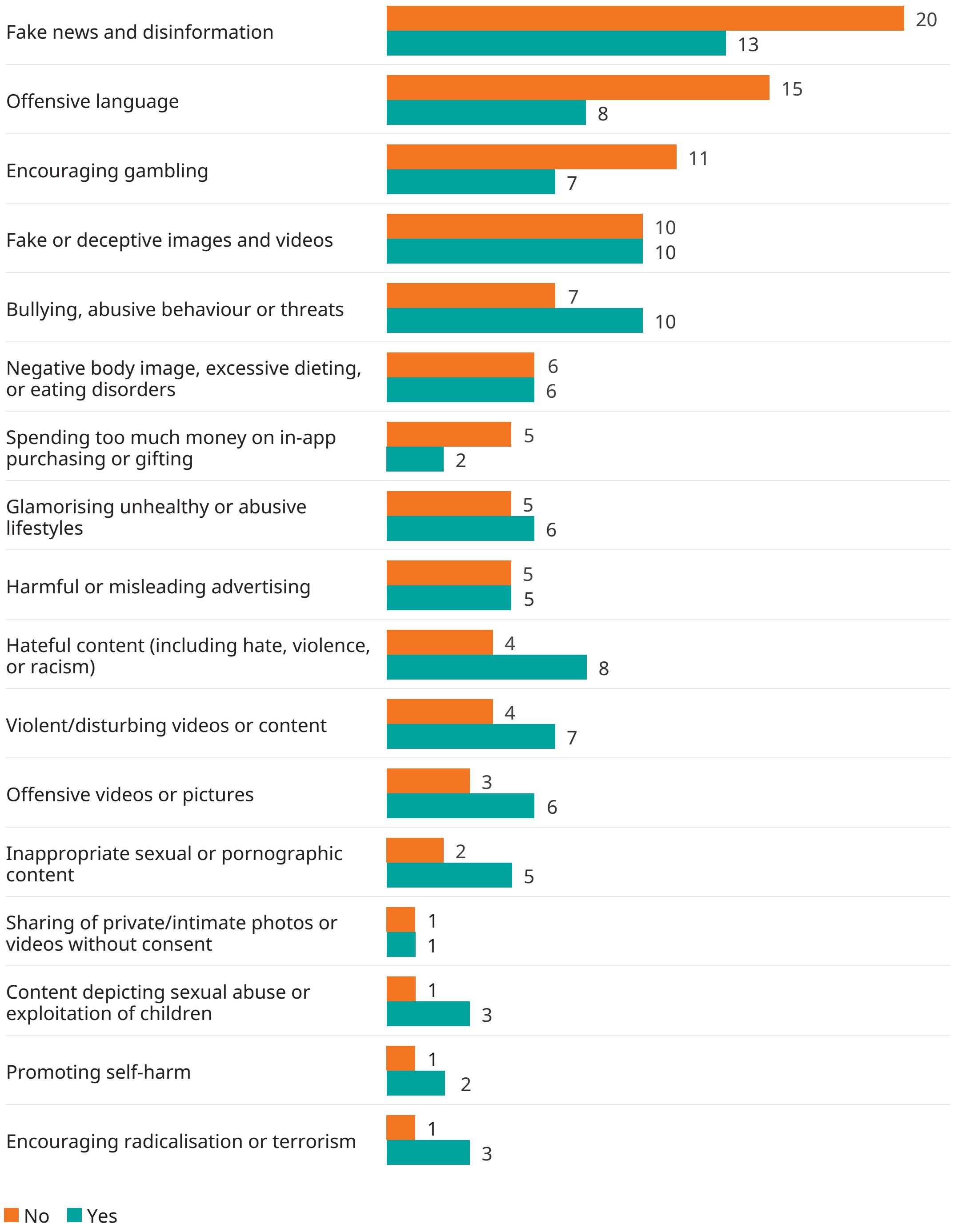
Note: answering "No" results in being prompted by a list of categories of harmful content before being asked to recall an instance again; results of the open-ended survey responses were manually categorised post-collection

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

We observe differences in the categories of harmful content that survey participants reported to have encountered when comparing responses of those who recalled an instance unprompted compared to those who could not initially recall an instance and were prompted with a list of categories. See Exhibits 44 and 45 for a comparison.

- In practice, the ability to see the list before trying to recall an instance can functionally differentiate the way in which respondents interpret the definition they were provided with ("content that is inappropriate, distressing or deliberately misleading") and can subsequently impact the qualitative responses themselves.
- **Violent and disturbing content was most frequently recalled** in the open-ended question by those who did not see the categories list before giving a qualitative response. Irrespective of seeing the list, respondents very frequently recalled an instance of **fake news and disinformation** as their example of harmful content encountered. Among others, examples of fake news recalled were often related to the Covid-19 pandemic or the political situation at the time the survey was conducted. Furthermore, **inappropriate sexual content** also ranked highly when respondents did not see the checklist first.
- **Some of the other types of harm were more frequently mentioned in open-ended answers by respondents who were shown the list of categories.** These include: glamourising unhealthy lifestyles (GUL) and negative body image, excessive dieting and eating disorders (NBD), as well as offensive language (OL). This may indicate that some respondents may not initially consider these as harmful until reminded otherwise. Materials that encourage gambling are another example, ranked third most frequently selected type of harm from the list of categories (see Exhibit 45) as well as recalled almost exclusively by respondents who initially reported not having encountered any harmful content and were prompted by the list (see Exhibit 44). In this context, respondents commonly voiced concern over gambling adverts and materials having potential to cause harm despite being legal, especially if encountered by young people or those susceptible to gambling addiction.

Exhibit 45: Categories of harmful content that survey respondents reported to have encountered, by response to the question if they previously encountered harmful content, Percentage



Note: Respondents able to select multiple categories from a list

Source: Oliver Wyman and CogCo Behavioural User Experience survey, February 2022

APPENDIX

APPENDIX A

GLOSSARY OF KEY TERMS

Deepfake: Synthetic media (e.g. videos or photos) in which a person is replaced by a computer-generated copy of someone else. This is done using artificial intelligence, specifically machine learning, combined with advanced computer-graphics techniques. Synthetic media is most commonly present in adult entertainment (especially in the creation of pornographic videos), but it is also a commonly used tool to enable the spread of disinformation.[1]

Digital identity: Virtual form of personal identification through which people can legally prove who they are. It offers an alternative to physical credentials (such as passports or drivers licences). In the context of the VSP space, digital identity could be potentially used in age verification of users.[2]

Hash database: In database management systems (DBMS), hashing is a technique to directly search the location of desired data on a disc without having to go through the elements of the database. In the context of harmful content on VSPs, hashing databases are used in detecting Child Sexual Exploitation and Abuse material (CSEA) and other types of illegal content. From a database of known illegal images and video files, unique IDs or hashes are created to represent each image, which can then be used to identify other instances of those images.[3]

Herfindahl Hirschman Index (HHI): An index that measures the size of firms relative to the size of the industry they are in and provides an indication of the level of competition in a market. The higher the calculated HHI metric, the more concentrated the industry. The HHI is calculated by adding up squared market shares of industry participants. The HHI is calculated using the formula below:

$$HHI = S_1^2 + S_2^2 + S_3^2 + \dots + S_n^2$$

[1] www.spectrum.ieee.org

[2] www.gov.uk

[3] www.news.microsoft.com

Where s_$_i$ represents the market share of an individual firm in a given sector and n represents the number of firms in that sector.[4]

Metaverse: Network of shared, immersive digital environments in which users can interact with each other in virtual reality.

Network effect: a phenomenon whereby a good or service increases in value when it is used by a larger number of people. Social media platforms and VSPs are an example of the network effect in play: a platform that is already used by many and therefore hosts a sizable amount of content, is more likely to appear attractive to other users.[5]

Video Sharing Platform (VSP): An online service which allows users to upload and share videos with members of the general public. The provider of the service controls the organisation but not the selection of videos on the platform. This includes platforms for which facilitating user-sharing of video content is:

- either the principal purpose of the service (or a dissociable section of the service); or
- an essential functionality of the service as a whole (i.e. where the provision of videos contributes significantly to the commercial and functional value of their service).

In this context, a platform provider that allows users to view content which is exclusively not user generated (e.g. journalistic media, on-demand video streaming such as Netflix or Amazon Prime) is not a VSP.

Under the UK VSP regime, Ofcom regulates VSPs with the required connection to the UK. VSPs that are established in an EU country fall under the jurisdiction of that nation’s domestic VSP regulations. In order to capture all platforms relevant for the future Online Safety regulation, the VSP definition used throughout this report goes beyond the VSPs regulated by Ofcom under the VSP regime. Consequently, VSPs in scope of this study include VSPs with the required connection to the UK who notified their status to Ofcom at the time of writing this report, as well as other VSPs.

Web3: A next-generation iteration of the World Wide Web based on blockchain technology which applies concepts such as decentralisation, a process by which the activities of an organisation are distributed or delegated away from a central authoritative location or group, and token-based economics, where the consumption of goods and services are exchanged for tokens (e.g. cryptocurrencies) without the need for intermediaries.[6,7]

[4] www.investopedia.com

[5] www.investopedia.com

[6] www.bloomberg.com

[7] www.oreilly.com

APPENDIX B

USER EXPERIENCE SURVEY

EXPLANATORY NOTE ON THE SURVEY FLOW

The survey has been structured in a way that maximised the response quality for the qualitative answers in which respondents shared an example of a previous encounter with harmful content. Every respondent initially started the survey by viewing the instructions and information on taking the survey, as well as answering some screening questions to ensure that all respondents were users of VSPs.

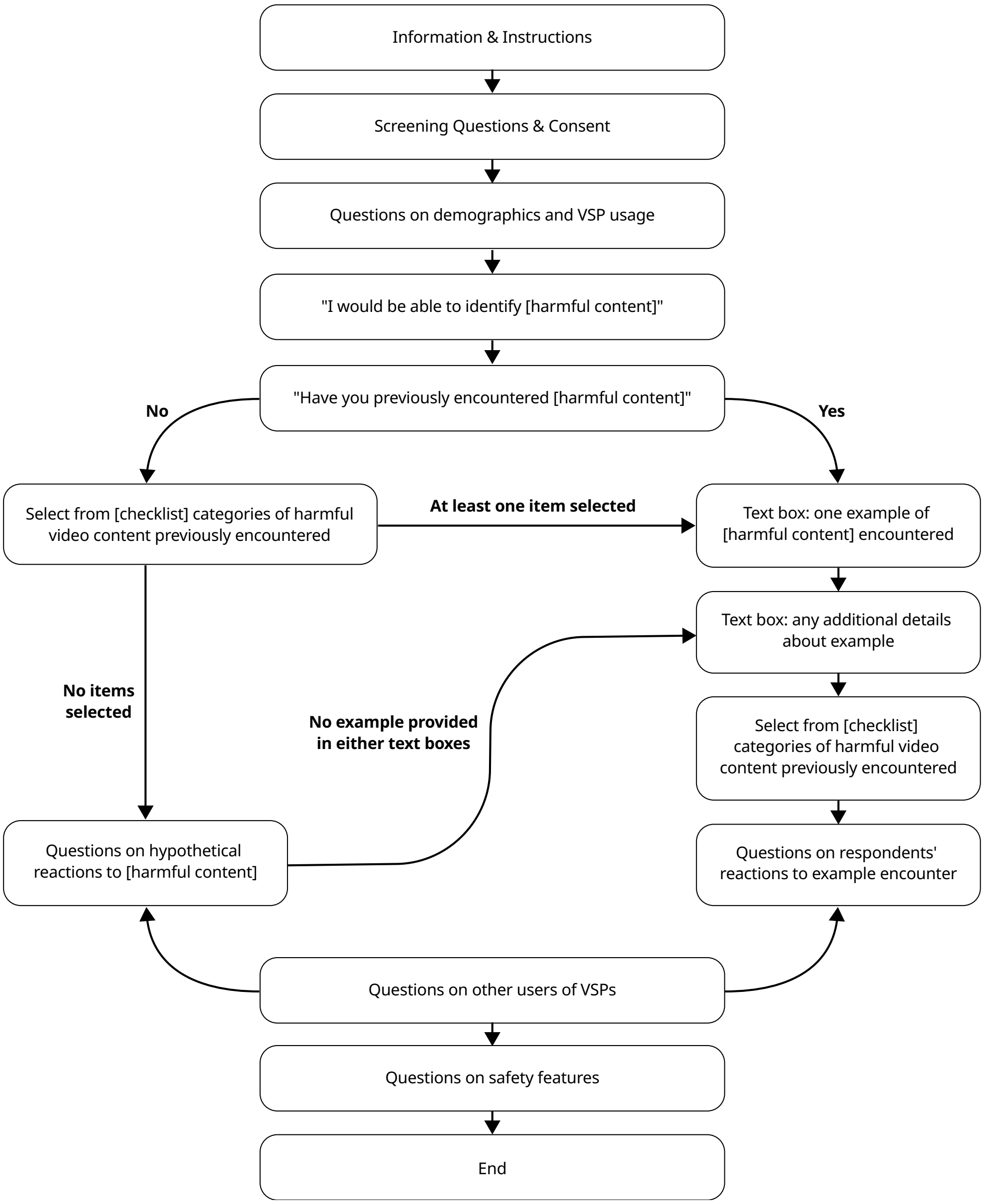
Following this, respondents were asked questions regarding their demographics (age, gender, ethnicity, and region of residence), as well as questions about their general usage habits of VSPs such as which platforms they regularly watched and for how long.

After answering demographics questions, respondents were then asked how well they believe they would be able to recognise harmful content, phrased in such a manner that "harmful" was not explicitly used in order to avoid cueing respondents with preconceptions based on phrasing. Instead, harmful content was referred to as content that was either distressing, inappropriate, or intentionally misleading. Respondents were also asked whether they have encountered such content before, and it is at this point that the survey would then split the respondents into one of two branches.

For respondents who answered that they had not previously encountered harmful content, they were provided with a list of categories of harmful content adapted from a pre-existing list defined by Ofcom for the purposes of this survey (see appendix on further detail on categories of harmful content used in the user experience survey). This list was presented as a checklist from which respondents could select any number of items, or none at all.
If respondents selected at least one single item, this would indicate that they had in fact previously encountered harmful content despite answering "No" to the previous question asking whether they had. Subsequently, they would be redirected to the same text entry question that was presented to respondents who answered "Yes" and would proceed as if they had answered similarly.

For those who answer that they have encountered an instance of harmful content before, the survey then immediately provides them with an information screen that leaves the respondents unable to proceed for 30 seconds. During this time, respondents are given guidance on how to recall and describe this experience. The following screen provides a large text box for respondents to enter their experience, along with repeated information and guidance on what to write. Respondents were also able to leave this text box empty and proceed to the next section of the survey if they chose to do so. After the first text box, a

Exhibit 46: Survey flowchart


Information & Instructions
Screening Questions & Consent
Questions on demographics and VSP usage
"I would be able to identify [harmful content]"
"Have you previously encountered [harmful content]"
No
Yes
Select from [checklist] categories of harmful video content previously encountered
At least one item selected
Text box: one example of [harmful content] encountered
Text box: any additional details about example
No items selected
No example provided in either text boxes
Select from [checklist] categories of harmful video content previously encountered
Questions on hypothetical reactions to [harmful content]
Questions on respondents' reactions to example encounter
Questions on other users of VSPs
Questions on safety features
End

Source: Oliver Wyman and CogCo analysis

second text box was also provided to respondents to provide any further details they may have missed in the first text entry box, along with additional prompts. Finally, after answering both open-ended questions, this group of participants was provided with the same checklist as respondents who had initially answered "No". This checklist then allowed us to capture data on how frequently different types of harm were encountered by respondents.

The rest of the survey then proceeded in the same manner for all respondents, with a block of questions on respondents' views of other users and their behaviours, and a block of questions on respondents' opinions on different safety features.

FURTHER DETAIL ON CATEGORIES OF HARMFUL CONTENT USED IN THE USER EXPERIENCE SURVEY

As part of the user experience survey, respondents were presented with a list of categories of harmful content and asked to select those they encountered when using Video Sharing Platforms. The list of categories was adapted from categories used in a previous report on 'User experience of potential online harms within VSPs' published by Ofcom.[8] We synthesised it with a focus on content harms, given the scope of this report and the user experience survey.

Survey respondents were asked to select from the following list of 16 categories:

- Bullying, abusive behaviour or threats,
- Content depicting sexual abuse or exploitation of children,
- Encouraging gambling,
- Encouraging radicalisation or terrorism,
- Fake or deceptive images and videos,
- Glamorising unhealthy or abusive lifestyles,
- Harmful or misleading advertising,
- Hateful content (including hate, violence, or racism),
- Inappropriate sexual or pornographic content,
- Negative body image, excessive dieting, or eating disorders,
- Offensive language,
- Offensive videos or pictures,
- Promoting self-harm,
- Sharing of private/intimate photos or videos without consent,
- Spending too much money on in-app purchasing or gifting,
- Violent/disturbing videos or content.

[8] www.ofcom.org.uk

After the collection of the qualitative open-ended survey results, responses were manually classified under different categories of harmful video content. As part of this process, new categories were added to the above list whenever there was a high incidence of a previously uncategorised type of harmful video content recalled.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialised expertise in strategy, operations, risk management, and organisation transformation.

For more information, please contact the marketing department by phone at one of the following locations:

EMEA	Americas	Asia Pacific
+44 20 7333 8333	+1 212 541 8100	+65 6510 9700

AUTHORS

Oliver Wyman:

Lisa Quest	Dr Krzysztof Bar	Joanna Kalemba	Vla Stanojevic
Partner Head of the Public Sector, UK & Ireland	Engagement Manager	Senior Consultant	Art Director

Cognition Company:

Owain Service	Dr Umar Taj	Dr Ruth Horry
Chief Executive Officer	Director	Senior Associate

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.

Oliver Wyman – A business of Marsh McLennan www.oliverwyman.com