

## Your response

### Volume 2: The causes and impacts of online harm

#### Ofcom's Register of Risks

##### Question 1:

- i) Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?

Response:

##### *Search services*

Skyscanner strongly welcomes the decision by Ofcom to include a separate chapter (6T) specifically for search services in the Register of Risks. From an ease-of-use perspective, however, it may be helpful for the assessments of the impact of relevant harms to be re-included in the Search chapter, rather than directing readers to read the relevant parts of the U2U guidance, so that search services can find all the relevant information directly in the search chapter.

The overall approach taken by Ofcom in relation to search services, of giving due consideration to the characteristics of a service when assessing the causes and impacts of online harms is absolutely the right one.

When it comes to risk factors for search services, we agree that "the ability of users to enter search queries relating to illegal content and to receive relevant results is the main underlying driver of risk of harm associated with search services." We strongly welcome recognition of the fact that VSS are, as a result of their more limited functionalities and the fundamentally different way in which they operate, "likely to have a lower level of risk of harm than general or downstream search services". We particularly welcome the use of the example of a travel search site to illustrate this point. The limited search functionality of VSS is a fundamental reason why they pose a relatively lower (and in many cases a negligible) risk of presenting users with the priority illegal harms defined by the Online Safety Act.

As the chapter notes (6T.20), all of the published evidence referenced in the Register to general search services only. We welcome this recognition but believe that it could be more explicitly stated, as it is elsewhere in the consultation documents, that Ofcom is not aware of any evidence of users encountering illegal content on VSS sites. This would make using the Register easier and quicker for VSS when conducting their risk assessments.

As our later answers make clear, we also believe that the fact Ofcom is not aware of any evidence on the risks posed by VSS in terms of illegal content could be better reflected in some of the measures being proposed. It is clearly disproportionate, in our view, for VSS to be required to

comply with some of these measures when Ofcom has no evidence in the Register of Risks that VSS pose the same level of risk as other search services.

When it comes to the question of a search service's user base as a risk factor, we believe that the Register of Risks poses limited utility (for VSS at least). While noting that user base is only considered in "a very limited way" (6T.29) for search services, we do not agree that the size of a search service's user base is a risk factor: if it is not possible for a particular illegal harm to take place on a service due to its functionalities, for example, then the size of a user base is completely irrelevant. Furthermore, there is currently no steer from Ofcom on how user numbers are supposed to be calculated in a consistent way for search services in light of the fact that most do not require users to have an account in order to use their service.

The same point applies to user base demographics too – in cases where it is simply not possible for a particular illegal harm to occur, the demographics of a user base are irrelevant. In addition, there is no steer on how a search service is supposed to identify the demographic characteristics of their users while respecting the requirements of existing data protection law. This is particularly important given that user base demographics are included as a general risk factor in the Risk Profile for Search services. **[CONFIDENTIAL.]**

With regards to search functionalities, we believe that Ofcom has identified the most suitable ones. In particular, we agree that the underlying potential for illegal content on webpages indexed by search services to appear in, or via, search results, is fundamental: it is the main reason that VSS pose a lower risk than general search services. With regards to search prediction and personalisation, it would be helpful for the Register of Risks to make clear that the risk relates to free-form search predictions, and that predictive search functionalities based on a narrow and defined subset of possible search queries (e.g. departure airports or cities) are excluded.

#### *U2U services*

Skyscanner, unfortunately and like many businesses in both the travel sector and wider economy, has seen a worrying rise in the number of scams that seek to deceive people out of money by imitating our business. There is a particular issue with job scams currently. Fraudsters posing as Skyscanner employees cold contact prospective victims via messaging services such as **[CONFIDENTIAL]** to initiate the scam, offering them commission to 'work' for Skyscanner by completing online tasks on a site they have set up impersonating Skyscanner. They sometimes pay them small amounts and, having won their trust, at some point they convince victims to pay them a much greater amount to 'unlock' higher commission levels, effectively scamming them (in many cases out of thousands of pounds). There are variations of these scams, but they can also involve offers of employment followed by requests for bank details in order to pay wages, or promises of payment only after money (often cryptocurrency) has been transferred to an account first (again, in order to 'unlock' payment). **[CONFIDENTIAL]**

When Skyscanner is contacted by someone who has been affected by such a scam, we do everything we can to seek redress for them, while acknowledging that, since the scam took place away from our site, there is a limited amount that we can do. **[CONFIDENTIAL]**

Given the vast difference in user numbers and revenue **[CONFIDENTIAL]**, we strongly welcome the finding contained in the Register of Risks that fraud takes place on a wide range of services. If the Online Safety Act is to be effective at tackling fraud on U2U services, it is vital that smaller but high-risk services like Telegram are captured by the most effective obligations.

Therefore, the inclusion of both social media services and messaging services in the risk profiles for fraud is welcome. The type of scams outlined above also corroborate Ofcom's assessment that the ability to create fake user profiles and messaging functionalities (the ability to communicate via direct messaging or group messaging, and via encrypted messaging) both increase the risk of fraud being committed.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: Yes – the parts in bold and brackets [] is confidential

## Question 2:

i) Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.

Response:

We believe that Ofcom is absolutely correct to identify that VSS are likely to pose a lower risk from illegal harms in general than general search services given their limited functionalities. Such differentiation does not appear in similar laws passed elsewhere, including the European Union's Digital Services Act (DSA), and this is one of the main ways in which we believe this regime will be more proportionate than the DSA. Unsurprisingly, given our nature as a travel metasearch site, we particularly welcome the inclusion of an example recognising that a travel search site "may be much less likely to present illegal content to a user" since sites like Skyscanner only serve up content from our professional partners (or content curated by us).

**[CONFIDENTIAL]**

In short, we believe that this evidence corroborates Ofcom's assessment that VSS are likely to pose a much lower risk of illegal content compared to other search services, and this justifies the subsequent decisions to exempt VSS from many obligations. We argue in our subsequent answers, however, that it also justifies further exemptions or modifications for VSS like Skyscanner in a couple of important areas.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: Yes - the parts in bold and brackets [] are confidential

## Volume 3: How should services assess the risk of online harms?

### Governance and accountability

#### Question 3:

- i) Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?

Response:

We strongly agree with the majority of the proposals in relation to governance and accountability measures, as they relate to large low-risk vertical search services (specifically, the decision to exempt such services from many of the measures). As Ofcom recognises, there is no evidence of large VSS showing illegal content, and due to their nature and functionalities (including the fact that the search results presented are – at least in the case of Skyscanner – curated only from our own professional partners) pose a much lower risk of illegal content compared to the other services in scope. This finding very much aligns with our own data relating to user complaints of illegal content on our site, as detailed in our response to question 2. It is also absolutely the case that, given our nature as a travel search service, our search results and functionalities will not change and evolve quickly. This would make the requirement for an annual review of risk management practices by the board an unnecessary burden on large (but low risk) vertical search services, and so we welcome the proposal by Ofcom to exempt such services from this requirement. We do note later in our response, however, that we believe such services should also be exempt from the proposed requirements to review risk assessments every 12 months at a minimum, and to conduct an annual compliance review, as the same reasoning applies.

We note that the recommendation that all services name a person accountable to the most senior governance body for compliance with illegal content duties and reporting and complaints duties goes beyond what is required of online platforms and intermediary services under the EU's Digital Services Act. That regime only imposes a requirement for these platforms to name a single point of contact. This measure could, therefore, impose a disproportionate burden on low-risk services which are in scope of both pieces of legislation (but are not a VLOP under the DSA).

- ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Response:

- iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

#### Question 4:

i)	Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response: Yes, mostly	
ii)	Please explain your answer.
<p>Response: We strongly agree with the proposal to exempt large, low-risk VSS from most of the governance and accountability measures, in light of the low risk from illegal content posed by such services. As noted in response to question 2, our own data in terms of user complaints shows that, due to the limited functionalities of our site, we do not pose a risk from the types of priority illegal content being regulated by this Bill. The proposals in this area are therefore, overall, in line with Ofcom's commitment to being proportionate and effective.</p> <p>We would reiterate, however, that the proposal for all in-scope services to have to name a person accountable to the most senior governance body for compliance with illegal content duties and reporting and complaints duties goes further than equivalent measures under the DSA. We understand the desire for a minimum level of governance standards among all in-scope services, but we believe that an alternative option for low-risk services could be to name a single point of contact for compliance purposes. This would have the additional benefit of being more aligned with many services' obligations under the DSA.</p>	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

#### Question 5:

i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

#### Question 6:

i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

## Service's risk assessment

### Question 7:

i) Do you agree with our proposals?

Response:

Skyscanner agrees with certain aspects of the proposals, as follows:

- We believe that the four-step process which, if followed, allows services to easily comply with many of the illegal content and reporting and review obligations too, is innovative and helpful for compliance.
- We agree that what constitutes a “suitable and sufficient” illegal content risk assessment is a context-specific requirement. This should allow services flexibility when meeting this requirement based on their characteristics (which are so fundamental to the risk of illegal content appearing on their service).
- We also strongly agree that risk assessments should, as far as possible, be based on relevant evidence on the risk of harm on the service.
- We also welcome the ability to assess the risk level for a given illegal harm as “negligible” where it is not possible for a harm to take place by means of the service. This rightfully recognises the fact that many in-scope services will lack many of the functionalities that Ofcom has identified as risk factors, and so should make the risk assessment process less burdensome for these services.

We have some concerns regarding certain aspects of the proposals, however:

- We believe that the Search Risk Profile needs to be amended and clarified in certain areas to make them easier to use for VSS (see our response to questions 8 and 9).
- We disagree, however, with the proposal that all services, regardless of the level of risk identified by their initial risk assessment, should review their risk assessments every 12 months.
- We also disagree with parts of the guidance on what constitutes a “significant change to the design or operation of a service” that would trigger the legal requirement for a new risk assessment.

ii) Please provide the underlying arguments and evidence that support your views.

Response:

#### *Annual reviews of risk assessments*

The illegal content risk assessment is one of the biggest and most burdensome aspects of the regime, especially for low-risk services. As Ofcom notes at various points in these consultation documents and draft guidance, it is not currently aware of any published evidence that shows that VSS pose a risk to users from illegal content. Ofcom also notes at various points (including when

justifying its proposal not to recommend several of the governance obligations for large, low-risk VSS) that the search content on a VSS is more directly controlled by the service provider and the search results and content on VSS are less likely to change quickly when compared to general search services.

Given all this, we believe that the recommendation for all services to review their risk assessment at least every 12 months is disproportionate for low-risk VSS firms, regardless of their size. While it may be true that a review will be less burdensome than carrying out a new risk assessment, that by itself does not justify this proposal. Any resource that services have to divert away from improving their service harms both that service and its users for no additional online safety benefit.

What's more, there is already a separate requirement for services to carry out a new risk assessment prior to making a "significant change to the design or operation of the service". Since this is the main means by which the risk profile of a low-risk VSS could change, it does not make sense for these services to also be subject to such regular reviews outside of such a trigger event (there are also, of course, similar obligations when Ofcom makes a change to a relevant Risk Profile). It is highly unlikely that, notwithstanding a significant change to the design or operation of the service, the risk profile of a low-risk VSS firm could have changed meaningfully within 12 months, given their limited functionalities.

Ofcom's argument that 12-month reviews will ensure that risk assessments are suitable and sufficient given fast-moving online technology is not applicable to limited functionality VSS. A travel search site is always only going to search a very limited subset of online databases or websites, and any changes that such a site makes to take account of fast-moving online technology (such as integrating generative AI into search results, for example) would trigger a review of the risk assessment anyway under the separate obligation described above.

In short, we believe strongly that VSS (regardless of size) that are not identified as multi-risk in their initial risk assessment, should not be subject to an annual review requirement. This approach would be in line with all the available evidence, including their own risk assessment, that they present a low-risk and that their content evolves much more slowly and is more tightly under the service's control.

#### *Guidance on what constitutes a "significant" change to the design or operation of a service*

We firmly believe that the proposed guidance for what constitutes a "significant" change to the design or operation of a service, which triggers a legal requirement to carry out a new risk assessment before making such a change, is disproportionate. Specifically, we believe that 9.136b is completely detached from any consideration of the actual risk posed by a given change. Just because a proposed change may impact "a substantial proportion of a service's user base" does not, on its own, alter the risk profile of that service.

Surely, the change must be one that risks fundamentally changing the risk profile of the service, and not simply any change that affects a lot of users. Skyscanner is a large service (under the proposed definition) and we, like most large tech businesses, are constantly running experiments

and making code changes across all aspects of our product. These changes could impact a “substantial” proportion (if not all) of our UK users, yet these changes would not alter in any way the risk of users encountering illegal content on our site. If Ofcom is suggesting that we should have to undertake a new risk assessment before every such change, just because they affect many UK users, is clearly disproportionate to us and a deviation from the risk-based approach taken elsewhere in these proposals. 9.136a and 9.136d are much more suitable proposals, for example.

We also disagree with the proposal that the guidance on this point give significant weight to the size of a service’s user base when making an assessment of what constitutes a “significant change.” It makes the guidance in this area for large low-risk services essentially useless, because size in the case of these services is absolutely unrelated to the risk posed by their service. Ofcom notes that the requirement to carry out a new risk assessment prior to implementing a significant change is a direct requirement of the Act, and accepts that this “has the potential to be more burdensome and incur greater costs” compared to the duties to update/review risk assessments. That makes it even more important that the guidance on what constitutes a “significant” change is proportionate. Again, we insist that the argument that “a relatively minor change on a large service is more likely to have a significant impact” is just not relevant to a low-risk large VSS like Skyscanner.

Given that Ofcom estimates over 100,000 services are to be in scope of this Bill, and that this particular legal requirement is one of the more burdensome ones, the guidance here should be more nuanced and proportionate than it is at present. It also appears to be a departure from the rest of the proposals, where it is made clear throughout that risk factors are often a combination of a service’s size and its characteristics. The other proposals are far more appropriate, and we would strongly recommend that Ofcom removes or amends 9.136b.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

***Specifically, we would also appreciate evidence from regulated services on the following:***

**Question 8:**

i) Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?

Response:

The four-step risk assessment process, as currently designed, does help services comply with their wider obligations, and we would support Ofcom keeping this approach. In particular, for likely low-risk services it is a helpful means to comply with the majority of the obligations being proposed in one single process. The inclusion, for example, of the information that services need to record directly in the risk assessment guidance reduces the number of individual pieces of guidance that services need to consult, and we believe that it should be Ofcom’s ambition to provide services with a one-stop-shop that allows an in-scope service to understand all their obligations in one document.



The guidance for the risk assessment is also clear and intuitive, with the grey summary boxes at the start of each step helping understand what exactly is expected of services. In addition, with regards to the guidance on core and enhanced evidence inputs, the provision of examples at A5.110 is a really helpful way of illustrating how the guidance applies in practice. Specifically, the example with Service C is an effective means of demonstrating where, for example, Ofcom's general recommendation that large services use some enhanced evidence inputs may not apply. We would recommend, where possible, that Ofcom adds further examples to other parts of the guidance to illustrate some of the nuances more clearly, as it would bolster services' confidence in applying the guidance.

The Risk Profiles are also, in principle, a helpful means of allowing services to quickly identify their risk factors. That said, we believe that the Search Risk Profile could be further clarified for VSS:

- There is no guidance (as far as we can tell) in the Register of Risks on how search services are expected to consider the demographics of their user base (particularly their protected characteristics, their media literacy levels, or their mental health) when assessing the risk of each type of illegal harm when a services does not collect such data (or where the vast majority of users do not create an account). There is also, despite what it says in the Risk Profile, no evidence that we can find in the Register of Risks on this point, especially for VSS.
- With regards to the commercial profile risk factor, it would be helpful for Ofcom to provide some steer on what it considers to be "low capacity" and "early-stage" (or, if this is provided somewhere, for this information to also be provided in the Risk Profile itself. Ofcom should be aiming for services to be able to comply as easily as possible, without having to sift through multiple guidance documents when carrying out a risk assessment.
- As noted elsewhere in our response, it could also be made clearer that limited search prediction/personalisation is not considered a risk factor (for example, if search predictions are limited to departure airports/destination cities etc).

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

**Question 9:**

i) Are the Risk Profiles sufficiently clear?

Response:

We believe that the search query inputs could be made clearer as a risk factor. Skyscanner does have, technically, a predictive search function, but this is very limited (to departure and destination airports/cities, or pick-up locations). We understand that Ofcom is not referring to this kind of predictive search, and so we would recommend that the Search Risk Profile make clear that this particular risk factor relates to free-form text predictive search.

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Do you think the information provided on risk factors will help you understand the risks on your service?

Response:

As indicated elsewhere in our response, we consider that the information provided on user base demographics and child users could be more helpful. Currently, the information provided on how these are risk factors, and specifically the harms they relate to, is incredibly vague for the Search Risk Profile. This is exacerbated by the fact that the Register of Risks for search services is similarly vague on these points. We understand that the Act dictates that risk assessments must consider a service's user base, but the fact that Ofcom does not address how search services are expected to do this when most of their users are not logged in is still a weakness of the proposals, and does mean that the clarity and utility of the Risk Profile is limited on this point.

iv) Please provide the underlying arguments and evidence that support your views.

Response:

v) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

**Record keeping and review guidance****Question 10:**

i) Do you have any comments on our draft record keeping and review guidance?

Response:

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

**Question 11:**

- i) Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?

Response: No

- ii) Please provide the underlying arguments and evidence that support your views.

Response:

As noted elsewhere in our response with regards to the proposed annual review of risk assessments, we believe that the recommendation that all services review their compliance at least once every 12 months is disproportionate in the case of low-risk vertical search services. Given that a significant change to the service (which is currently defined too broadly) will already require these low-risk services to review their compliance, and the fact that the nature of these services mean that the risk posed by them is unlikely to change quickly, requiring these services to review their compliance as frequently as the other services in scope does not seem proportionate.

Ofcom states (at 10.27) that “our analysis of risk across the sector indicates a wide variation in levels of risk across services independent of type, which we believe would make an exemption by type of service difficult to implement in a reasonable and proportionate way.” However, Ofcom’s Register of Risks does not include any published evidence on the risk of users encountering illegal content on VSS. Indeed, the Risk Profiles specifically state that VSS are likely to pose a lower risk from illegal content. Ofcom has rightly used these findings to exempt VSS (which are not multi-risk) from several of the other obligations under the Act. We therefore do not understand why Ofcom does not consider that there is an obvious candidate for an exemption from the annual compliance review obligation for VSS (or at least, ones that are not multi-risk), which Ofcom elsewhere recognises *by their nature* are likely to pose a lower risk from illegal content.

We would also note that such reviews do still incur a cost, and we believe that this cost is disproportionate when a service is clearly low risk. **[CONFIDENTIAL.]** While a compliance review under this regime may be less resource intensive, this is still time and resource diverted away from other activities. We would also ask Ofcom to consider both existing compliance review obligations services are subject to across multiple regulatory regimes, as well as the growing international online safety regulatory burden. Any costs imposed by this new UK regime should be considered in the context of proliferating regimes across the world, many of which do not neatly map onto the requirements in the Online Safety Act.

- iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: Yes – the parts in bold and brackets [] are confidential

## Volume 4: What should services do to mitigate the risk of online harms

### Our approach to the Illegal content Codes of Practice

#### Question 12:

- i) Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?

Response:

- ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

#### Question 13:

- i) Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?

Response:

Yes, with the important caveat that it is important Ofcom recognises throughout the guidance and in the proposals that size, on its own, does not always increase the risk of users encountering illegal content. For that reason, we do strongly welcome the overall approach taken by Ofcom of deciding not to recommend several proposals for large VSS simply because they are large. This approach is evidence-based and proportionate, and we note that it is not one that has been taken in other jurisdictions. We believe that Ofcom's overall approach is the correct one.

- ii) Please provide the underlying arguments and evidence that support your views.

Response:

- iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

#### Question 14:

- i) Do you agree with our definition of large services?

Response: We do not feel strongly about this either way.

- ii) Please provide the underlying arguments and evidence that support your views.

Response:

We do appreciate the attempts to align this definition with the EU's in the Digital Services Act (DSA). In general, we believe that Ofcom should seek to align as much as possible with the DSA, given the overlap between them and the number of services that are in scope of both, but only when the corresponding proposal in the DSA is itself proportionate and effective.

When it comes to defining large services, we believe that the more important consideration is whether the accompanying obligations that are attached to being defined as a large service are themselves proportionate. In this particular case, we recognise that the definition of a large service comes with less onerous obligations than VLOP/VLOSE designation under the DSA.

That said, we would also note that the EU market is much larger than the UK market, and that reaching over 10% of the population of the EU market is likely to be indicative of a large, multinational firm operating across multiple markets. Such firms are likely to be significantly bigger and better resourced than a firm that reaches 10% of the population only in one market, and so it may not always be appropriate to follow the EU's definition of what constitutes a large service.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

### Question 15:

i) Do you agree with our definition of multi-risk services?

Response: No

ii) Please provide the underlying arguments and evidence that support your views.

Response:

This is one of the few examples where we believe Ofcom deviates from the proportionate approach it has taken elsewhere.

Ofcom suggests at 11.44 that the intention of the 'multi-risk' definition is to catch services that "face significant risks for illegal harms *in general*." It then goes on to present two alternative options which we do not believe fairly reflect the range of ways in which Ofcom could define multi-risk services, to present its chosen definition as the most reasonable and proportionate.

Ofcom rightly argues that defining multi-risk services as those that have identified as medium or high risk for just one kind of illegal harm would be disproportionate, with relatively few online safety benefits, arguing at 11.44 that "if services have only identified a single area of risk, the extent of harm will tend to be lower compared to if they have identified *a range of kinds of offence where they are high risk*." This is obviously true. It is also true, as Ofcom notes, that if a service is at medium or high risk for only one kind of illegal harm, it is more likely to be well understood and addressed already by the service, compared to if a service has "multiple areas of risk."

Ofcom then goes on to suggest an alternative would be to set the definition "at a high level" (without stating what it considers that level would be), but that this would mean the benefits from measures would be smaller due to being applicable to fewer services.

We would argue, however, that there are many other options between those two extremes which would better balance proportionality and online safety benefits than the option being proposed by Ofcom.

Firstly, when there are 15 kinds of priority illegal harm, over 100 individual priority offences, as well as any other relevant non-priority offences for services to assess their risk against, we would consider that having only a high risk of two kinds of harm would still make that service fairly low risk compared to many of the other services in scope of this Bill. This is even more so if a service has only a medium risk of two kinds of harm. That a service found to be medium risk from just two kinds of illegal harm could face many of the same obligations as a service found to be high risk for 5/6/7+ kinds of harm is, to us, clearly disproportionate.

Second, the definition of "multiple", when used as a prefix, is "having more than one and usually several of something", according to the Cambridge Dictionary. We do not consider that Ofcom has

provided any persuasive reasoning as to why it is necessary to deviate from the usual meaning of the word “multiple” in this instance (i.e., more than one or two).

Third, if we follow Ofcom’s line of argument, it is not at all clear why a service’s understanding of their illegal content risks would suddenly fall significantly when their risk areas rise from one to just two.

Taken together, we do not see any justification for how the proposed definition catches only services that “face significant risks for illegal harms in general.” A service facing medium risk from just two kinds of illegal harm is, in our view, clearly not facing “significant risks for illegal harms in general” – such a definition stretches common understanding of both “significant” and “in general” beyond breaking point.

Ofcom itself, in the quote above from 11.44, appears to provide a reasonable definition of multi-risk: a service that has identified “a range of kinds of offence where they are high risk.” There is no convincing argument in the following paragraphs as to why Ofcom then proposes to deviate both from the idea of “a range of...offence” (by basing the definition on only 2 kinds of harm) and high risk (by making services with medium risk subject to the same provisions as those with a high risk).

There are numerous, more suitable alternatives to what is being proposed that would be more proportionate and still effective. Multi-risk could be defined as a service facing a high risk for illegal content from at least two kinds of harm, with the threshold higher for medium risk (two high risk or at least five medium risk, for example). Alternatively, the threshold could simply be raised, or there could be a focus on high risk only. Any of these solutions would be much more suitable, given that being defined as a multi-risk service significantly increases the regulatory burden on services, particularly for search services.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

#### Question 16:

i) Do you have any comments on the draft Codes of Practice themselves?

Response:

We find the draft Code of Practice for search services to be, overall, clear and easy to use. The index of recommended measures, in particular, is a very effective means of quickly getting an idea of which measures apply to your service.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

#### Question 17:

i)	Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
Response:	
<b>[CONFIDENTIAL]</b>	
We would also urge Ofcom to give due consideration to the opportunity costs imposed by these measures, particularly for low-risk services. Resource dedicated to complying with measures that do little to increase the safety of UK consumers online (when applied to low-risk firms) is resource that cannot be dedicated to innovation, product development, or hiring new staff. These costs should be given due consideration by Ofcom.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes – the part in bold and brackets [] is confidential	

## Content moderation (User to User)

<b>Question 18:</b>	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	



## Content moderation (Search)

Question 19:	
i)	Do you agree with our proposals?
Response: Skyscanner broadly agrees with these proposals.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:  In particular, we welcome the desire by Ofcom to avoid setting overly prescriptive rules.  We also strongly support the decision to reserve the majority of recommendations for large general search services or any other multi-risk search service (although we do have serious concerns that the definition of multi-risk is set too low), since these clearly pose a greater risk of illegal content based on the Register of Risks. We also believe that, in the spirit of proportionality, it is right not to require services to use automated tools to review content.  We would, however, welcome updated definitions and wording to reflect the fact that VSS do not “deindex” or “downrank” content, due to the fundamentally different way in which they operate compared to general search services. Given our control over the search results we present, for example, we already have a robust policy of removing any content that is deemed to be illegal or in breach of our terms of service, when we become aware of it. We believe an update to the guidance, which makes clear that other forms of removal beyond deindexing are acceptable, would aid clarity.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

## Automated content moderation (User to User)

Question 20:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

### Question 21:

i)	Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

***Do you have any relevant evidence on:***

<b>Question 22:</b>	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

<b>Question 23:</b>	
i)	Ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

<b>Question 24:</b>	
i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

**Question 25:**

i) Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;

Response:

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

**Question 26:**

- i) An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.

Response:

- ii) Please provide the underlying arguments and evidence that support your views.

Response:

- iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

## Automated content moderation (Search)

**Question 27:**

- i) Do you agree with our proposals?

Response:

- ii) Please provide the underlying arguments and evidence that support your views.

Response:

- iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

## User reporting and complaints (U2U and search)

**Question 28:**

- i) Do you agree with our proposals?

Response: We believe that these proposals have the potential to be unduly burdensome on services.

- ii) Please provide the underlying arguments and evidence that support your views.

Response:

Given the existence of similar provisions in the EU's DSA, Ofcom should ensure that these duties are closely aligned to avoid services having to make multiple changes across the two jurisdictions to achieve the same objectives. We would also disagree with the judgement of Ofcom that at least two separate processes for users (a report function for illegal content and a broader complaint function) is necessarily needed.

A joint reporting/complaints function could be designed in such a way that allows users to either report illegal content or complain about the illegal content reporting function itself if, for

example, the system takes the form of sending an email to a dedicated team. An email format provides sufficient scope, in our view, to allow for the broad spectrum of reports or complaints envisaged under the Act.

We also believe that the requirement to acknowledge receipt of all relevant complaints and provide indicative timelines for their resolution is an unnecessary administrative burden on low-risk services, when they will already be under a separate obligation to respond promptly.

We are also slightly concerned that the requirement for a reporting function for illegal content that is “clearly accessible in relation to that search content” could lead to an overly prescriptive approach that could undermine the usability of search services. Our own research shows that users are put off by overly crowded search results. When it comes to travel search, we already have to provide users with a significant amount of information to help them make informed decisions. Ofcom should make clear that they do not expect reporting functions to be immediately next to each individual piece of search content, which would clutter the page.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

## Terms of service and Publicly Available Statements

### Question 29:

i) Do you agree with our proposals?

Response:

Given the similarity in proposals between the Online Safety Act and the DSA, we would urge Ofcom to make sure that its proposals are in line with the DSA, to allow services operating in both jurisdictions to provide the same terms of service/publicly available statement in both markets.

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

### Question 30:

i) Do you have any evidence, in particular on the use of prompts, to guide further work in this area?

Response:

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

## Default settings and user support for child users (U2U)

### Question 31:

i) Do you agree with our proposals?

Response:

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

### Question 32:

i) Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?

Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

<b>Question 33:</b>
i) Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

### Recommender system testing (U2U)

<b>Question 34:</b>
i) Do you agree with our proposals?
Response:
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

<b>Question 35:</b>
i) What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

***We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive.***

<b>Question 36:</b>
i) Are you aware of any other design parameters and choices that are proven to improve user safety?
Response:

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

## Enhanced user control (U2U)

<b>Question 37:</b>
i) Do you agree with our proposals?
Response:
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

<b>Question 38:</b>
i) Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

<b>Question 39:</b>
i) Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

## User access to services (U2U)

<b>Question 40:</b>
i) Do you agree with our proposals?
Response:
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:



***Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:***

<b>Question 41:</b>	
i)	What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)?
Response:	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

<b>Question 42:</b>	
i)	How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

***There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users.***

<b>Question 43:</b>	
i)	What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

## Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

## Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response:	

As noted elsewhere, we strongly support Ofcom's proposals to exempt large, low-risk VSS from many of the provisions. We believe that, in the case of VSS, Ofcom is taking a mostly proportionate approach that reflects the actual risks posed. However, as noted in our answers, we believe that the burden on large, low-risk VSS could be more proportionate with an exemption from the requirement for an annual compliance review and an annual review of the risk assessment.

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

## Statutory Tests

### Question 48:

i) Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?

Response:

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

## Volume 5: How to judge whether content is illegal or not?

### The Illegal Content Judgements Guidance (ICJG)

#### Question 49:

i) Do you agree with our proposals, including the detail of the drafting?

Response:

ii) What are the underlying arguments and evidence that inform your view?

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

#### Question 50:

i) Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?

Response:

ii) Please provide the underlying arguments and evidence that support your views.

Response:

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

#### Question 51:

i) What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?

Response:

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

## Volume 6: Information gathering and enforcement powers, and approach to supervision.

### Information powers

Question 52:	
i)	Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

### Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

## Annex 13: Impact Assessments

Question 54:	
i)	Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response:	
ii)	If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	