13 September 2022

FSB response to the Call for evidence: First phase of online safety regulation

The Federation of Small Businesses (FSB) welcomes the opportunity to respond to the Ofcom call for evidence on the first phase of online safety regulation.

FSB is a non-profit making, grassroots and non-party political business organisation that represents members in every community across the UK. Set up in 1974, we are the authoritative voice on policy issues affecting the UK's 5.5 million small businesses, micro businesses and the self-employed.

Online safety is critical for many internet users, both individuals and businesses, however there must be a balance between the desired outcomes and intentions, and the ability of businesses to comply with set measures. It is imperative that any measures that businesses will have to take are proportionate to risk of harm and do not have a disproportionate impact on their ability to innovate and compete in the market. Small businesses do not have resources that are available to larger businesses, and often will not be able to afford sophisticated technology or tools that larger businesses are able to deploy. If a one-size-fits-all approach is adopted to online safety regulation, the likely consequence is that small businesses will find themselves overwhelmed with compliance burden, and unable to compete with larger established incumbents. Therefore, while we agree with the aim of reducing and tackling illegal activity online, we urge that online safety should be achieved on a proportionate and collaborative basis, with a primary focus on the large and most harmful organisations in the first instance, allowing sufficient time to iron out any issues.

The regulatory environment is already very complex for small businesses, and the ever-increasing regulatory burden continues to impact their ability not only to run day to day operations but also to familiarise themselves with any new requirements. For example, our research shows that 22% of small businesses are reporting changing business costs due to regulations and that two thirds of small businesses perceive the current domestic regulatory environment to be more a burden than benefit to their business.[1]

Small businesses are also likely to over-comply because of the fear of enforcement.[2] This is why regulations should be designed in such a way that they are not only based on potential risk but also the size of the organisation and the ability to comply. Any implementation periods proposed should be generous, with the most harmful services expected to comply first and the focus for small businesses should be on education and support rather than on fines or enforcement.

[1] FSB report, Escaping the Maze, June 2021 https://www.fsb.org.uk/resource-report/escaping-the-maze.html

[2] FSB, Newcastle University and University of Birmingham report, Navigating the COVID-19 regulatory landscape, June 2022, https://www.fsb.org.uk/resource-report/navigating-the-covid-19-regulatory-landscape.html

The cost pressures and difficult economic conditions that small businesses are currently facing, also make it increasingly difficult to dedicate any financial means to anything other than survival. Our recent Small Business Index Q2 2022 survey shows that business confidence is at -25, which is the worst confidence score we have seen since the survey began a decade ago, with the exception of the beginning of the COVID-19 pandemic. The net balance of small businesses reporting an increase in operating costs increased for the fifth consecutive quarter, reaching 89%, driven by fuel, utilities and broader inputs amidst shortages and market volatility.[3] This underlines our concern that any substantial additional time and cost implications of any new regulations must accommodate the ability of businesses to comply, particularly where the risk is low.

Any sophisticated monitoring or assessment technologies may also be out of reach for small businesses in comparison to larger ones, so consideration should be given to the means by which they are able to assess and implement any measures with regard to online safety and frequency of such assessments. Therefore, where regulations are imposed, the number of regulatory requirements should be minimised for small businesses and where small businesses are included within the scope, they must be supported to comply rather than penalised, particularly in the early stages of implementation. There should also be clear guidance and clear examples perhaps layered with some designed specifically for SMEs, not only tailored to business size but also sector. We would also like to see that the largest and most harmful businesses be the first to test and trial any new requirements before any small businesses are considered, as this will not only allow sufficient lead time to prepare but also iron out any outstanding practical or technical issues.

We have not responded to every question in this consultation but, only to those where we can offer a valuable and unique perspective.

Risk assessment and management
Question 2: Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?
Question 3: How do you currently assess the risk of harm to individuals in the UK from illegal content presented by your service?
Question 4: What are your governance, accountability and decision-making structures for user and platform safety?

Small businesses, particularly micro businesses, have limited resources and any time taken dedicated to conducting detailed risk assessments, that larger firms are able to dedicate time to through compliance teams and afford, will detract from the running of their day-to-day business. While risk assessments can be a good way to manage, evaluate and identify risks, we would urge for the requirements and the detail of the risk assessments to be proportionate to the size and the extent of the online harm risk posed by each business. Many small businesses will not only have a smaller user base, but also less sophisticated tools available to them to conduct any more extensive and sophisticated assessments.

There are commonly no dedicated means to escalate risks concerning user safety within the smallest of businesses, such as those with only a handful of employees, where it will often be the same person drafting the risk assessment as trying to understand and comply with the regulatory requirements. Therefore, we would welcome detailed SME-friendly guidance as well as templates for businesses to help them to comply. Guidance for SMEs may need to be framed

[3] FSB report, Small Business Index, Quarter 2, 2022 https://www.fsb.org.uk/resource-report/sbi-q2-2022.html

in different language to that targeted at larger businesses. We would also suggest that for services that are operated by smaller or less harmful businesses, detail and information required as part of the risk assessment should be significantly lower than for those that are deemed larger or more harmful. The regulatory framework should allow for flexibility and provide support to help achieve compliance.

Terms of service and policy statements

Question 5: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?

Question 6: How do your terms of service or public policy statements treat illegal content? How are these terms of service maintained and how much resource is dedicated to this?

User friendly language, tailored to the main or target audience of the terms of service and policy statements would help to enhance clarity and accessibility of terms of service and public policy statements. For small businesses, it may take a considerable amount of time to draft the documents/statements and update their terms on their website therefore, any guidance together with sector/business specific examples that could be provided in order to alleviate the pressure for small businesses would help to reduce the resources required to comply. For instance, there are existing examples of data protection statements which can be adapted to suit the needs of the business and similar ones could be used for terms of service and policy statements, together with examples of what should and could be included. Our recent research on the COVID-19 regulatory landscape and impact on small businesses highlighted the frustration amongst small businesses about lack of clarity in the distinction between regulations that are mandatory and guidance that is non-mandatory, with 22% citing that the distinction between the two was 'totally unclear'.[4] This why we would urge any guidance to include clear information as to what is compulsory to include and what is discretionary, not only offering businesses flexibility but also making any new requirements less onerous to comply with.

Reporting and complaints

Question 7: What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?

Both reporting and complaints need to be effective and easy to access and use as possible both for registered and non-registered users on the websites. However, they should also be proportionate to business size. There should be sufficient opportunity and time allowed to action complaints, as well as escalate them particularly in relation to any illegal content identified. If content is recognised to be of illegal nature, then there should be swift procedures for taking that content down. Appropriate and proportionate action and timescales should be outlined within any guidance and codes of practice.

Similarly, there should also be affordable, independent, time-light and effective appeal solutions and resolution routes available to those whose use of service has been restricted or terminated where the alleged evidence or justification is contested. Businesses and individuals should be able to appeal promptly any content that has been taken down wrongly, and the resolution process must be equally swift. Interruption and delay is particularly significant for small businesses that significantly rely on income from use of online services.

Question 8: If your service has reporting or flagging mechanisms in place for illegal content, or users who post illegal content, how are these processes designed and maintained?

[4] FSB, Newcastle University and University of Birmingham report, Navigating the COVID-19 regulatory landscape, June 2022, https://www.fsb.org.uk/resource-report/navigating-the-covid-19-regulatory-landscape.html#download

Question 9: If your service has a complaints mechanism in place, how are these processes designed and maintained?
Question 10: What action does your service take in response to reports or complaints?

Businesses using online services will usually have communication mechanisms and complaints procedures as required by current regulation and will have to review and adapt those procedures in light of whatever form the proposed Online Safety legislation finally takes. For the reasons outlined above in terms of resources and personnel, smaller businesses will require sufficient time and support to make those changes after the passing of the legislation and issuing of appropriate guidance, and compliance lead times must take that into account.

Moderation
Question 11: Could improvements be made to content moderation to deliver greater protection for users, without unduly restricting user activity? If so, what?

Many technologies that moderate content on services will either be unaffordable or unavailable to small businesses, with many in scope potentially having to try to create other proportional means of reviewing content themselves and moderating it rather than being able to adopt automated systems. However, given that small businesses who only have a limited amount of employees and resources would find it difficult to run day to day operations as well as monitor, identify and assess illegal content, there is a serious risk that what the legislation might expect of SMEs is simply unaffordable or practically impossible. Effective flagging systems or even notifications either through the online service itself or via an email mechanism could also be helpful way of reporting and monitoring any activity that is flagged as illegal by its users. There is no argument that a service provider should be able to remove any illegal content as soon as they become aware of such content, but that is why it is critical that both users and service providers are fully aware of how to report and manage such content.

Consideration should be given to those small businesses who may find it more difficult to prevent or minimise the risk of individuals encountering certain content where they do not already have any age restricted content on their website. For those that already have age restricted content it may be easier to adapt their systems and processes but for those that don’t, the cost implications for monitoring and assessing such content may be prohibitively significant. This is why careful thought should be given to any requirements and enforcement in relation to monitoring and assessing such content, particularly for smaller and lower risk businesses.

Actioning content and sanctioning users
Question 14: How are sanctions or restrictions around access (including to both the service and to particular content) applied by providers of online services?

Whilst it is accepted that there should be effective sanctions or restrictions in place around access, they should be directly proportionate to the scale and seriousness of the content identified, and there must be safeguards in place to protect users’ privacy and prevent unwarranted sanctions. To mitigate the impact of sanctions there should be a notice of intention and objection procedure following initial investigation of a complaint, with a right to request review taking into account counter-evidence prior to implementation. Businesses and individuals who are sanctioned should be able to appeal the decision and the appeal process should be cost effective and independent. There should be a requirement that sanctions such as restricted access to service should not be implemented without proper investigation and objective supporting evidence. Sanctions may include anything from restricted access to complete ban of the use of service, or content being completely deleted for some users, as well as reporting to relevant authorities.

Child protection

Question 22: What age assurance and age verification technologies are available to platforms, and what is the impact and cost of using them?
Question 23: Can you identify factors which might indicate that a service is likely to attract child users?

Sophisticated technologies and monitoring of users on platforms in relation to age assurance and verification can come at a significant cost. For a small business, that cost is likely to be more disproportionate to their overall turnover and profit margins than it will be for a large business.

While it is possible to implement basic age assurance such asking a user to verify their age by inserting a date of birth or confirming that they are over 18, they are not very effective at actually stopping a child from entering the website. Children frequently misrepresent their ages. So therefore, while there is a substantial cost for businesses to implement these requirements, it may not lead to the desired outcome of stopping children from accessing services. Although we do acknowledge that it does remind the user that it is only appropriate for users over a certain age. Indeed, in most cases it should be sufficient and proportionate for a service to have a prominent warning on the home or landing page of a website to say that this is not suitable for persons over a certain age, or possibly that underage access was illegal, which would potentially be more practically effective, and would be easier and more cost effective to implement and monitor.

Other technologies such as AI that can be used for sophisticated monitoring could also be deployed to verify someone's age, entering credit card information, verification through third party websites such as Facebook are also possible options, although expensive and out of reach for many small businesses. They also risk excluding genuine users that for example, do not have a credit card or a Facebook account. There is also a counter argument that by requiring such additional information ostensibly to protect individuals, there is a greater risk to those individuals of that information being misused, hacked or otherwise becoming available to cyber criminals. Verification via third parties whilst on the surface potentially attractive may, if mis-used, create complex liability or regulatory issues.

It is also difficult to predict what may or may not attract a child user. While of course some websites may attract children more than others due to their content such as having games or social media, others such as websites selling property for example may not. However, it does not mean that a child will not access them out of simple curiosity. This is why any measures to assess and monitor access by children should be proportionate, as it is unavoidable that children may access a service which is deemed 'conventionally' unattractive to users of their age. What is or is not within scope of the regulatory reach must be clearly defined and explained in appropriate guidance.

Question 27: For purposes of transparency, what type of information is useful/not useful? Why?

While some information is useful to be made available by regulators such as most severe cases of harm or examples of investigations that have concluded, as is the case for CMA for example, the purpose should be to demonstrate behaviours that would benefit or inform the services that are to be regulated. For services/platforms themselves, it would be disproportionate to expect them to publicise the information as part of any transparency obligations, particularly if that was expected to be detailed. It is also unclear how service users would benefit, or even would be interested in accessing, such information. Publication of information on user base or measures taken to prevent unlawful activities on a service or websites could for example be used negatively used by competitors or be of assistance to criminals. There must be a regulatory and practical purpose and usefulness underpinning any transparency requirements, which must be framed in such a way as to avoid anti-competitive and illegal usage.

Question 28: Other than those in this document, are you aware of other measures available for mitigating risk and harm from illegal content?

It would be helpful if there were a clearer requirement that all websites and online services clearly identify on their home or landing pages their full name, trading status, UK operational address and telephone number/email contact details to enable users to know with whom they are dealing, and for those requirements to be enforced.

Rather than prohibiting or regulating some unpleasant online behaviours, it might be better for the regulator to be able to disclose to anyone adversely affected by such behaviours the name and address of the person or party responsible for them, and for the affected party to have a right to seek appropriate redress elsewhere. That might avoid the regulator and/or the service provider from having to become embroiled in disputed complaints, and could save significant moderation costs for businesses.

Thank you for considering our response to this consultation. If you would like to discuss any of the points further, please contact me via my colleague ✂✂✂, Policy Advisor.

Yours sincerely,

✂✂✂