

# Consultation Response

## Online Harms White Paper

July 2019



## Introduction

---

The Law Society of Scotland is the professional body for over 12,000 Scottish solicitors. With our overarching objective of leading legal excellence, we strive to excel and to be a world-class professional body, understanding and serving the needs of our members and the public. We set and uphold standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession.

We have a statutory duty to work in the public interest, a duty which we are strongly committed to achieving through our work to promote a strong, varied and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. We seek to influence the creation of a fairer and more just society through our active engagement with the Scottish and United Kingdom Governments, Parliaments, wider stakeholders and our membership.

Our Consumer, Mental Health and Disability and Privacy Law sub-committees and Criminal Law Committee welcome the opportunity to consider and respond to the Government's consultation on the *Online Harms White Paper*.<sup>1</sup> We have the following comments to put forward for consideration.

## General remarks

---

We welcome the publication of the white paper and overarching objective for "the UK to be the safest place in the world to go online, and the best place to start and grow a digital business." We consider that action is needed to address online harms and recognise that this is a complex task, given the need to balance the interests of various groups, protect freedom of expression and ensure that citizens, particularly children or other vulnerable users, can use the internet safely. The challenge is to construct a legislative framework that is comprehensive and all-encompassing which needs to be robust and meet the current and future and as yet, unidentified harms.

A balance must be maintained when increasing regulation to ensure that we can and do hear "differing views and opinions to freely and peacefully contribute to public discourse."<sup>2</sup> It is also important to ensure that there is of information: we would be concerned, for example, if the new framework were to curtail free circulation news/reporting services. At the same time, we consider that incidents such as violent attacks, terrorism, etc should be reported in a responsible manner and would support measures to ensure this is achieved.

<sup>1</sup> <https://www.gov.uk/government/consultations/online-harms-white-paper>

<sup>2</sup> Paragraph 1.22

We share concerns around the increasing volume of disinformation and misinformation and the difficulty of identifying real stories from fake news. Online harm is widespread and in the longer term international cooperation in this area is likely to prove more efficient than any single country's initiative.

The White Paper is inevitably very high level and does not address what any proposed regulatory scheme would look like: more detail is needed before it will be possible to provide a full response but our initial observation is that the suggested approach is somewhat piecemeal although the paper states that it will be all-encompassing.

We also note that the language in the paper is very subjective and does not correspond to that usually used in legal regulation. There is vagueness in the paper's use of the term "companies", and – in association with that – terms such as "industry", "businesses", "business activities", and "funding from industry". It is not clear what entities are covered – for example could it include charitable organisations which offer a public discussion forum? The legislation ultimately drafted should use existing terms to provide greater clarity and allow interpreters to draw on existing jurisprudence.

In identifying the actual harm, care needs to be taken to develop consistent Codes of Practice based around objective criteria in order to take account of all "protected characteristics"<sup>3</sup> rather than identifying particular groups for protection, which could lead to fragmentation or discrimination against particular individuals being left out of scope.

Finally, we consider it is essential that communication around this topic makes it very clear that individual criminal responsibility remains on the part of the perpetrators but that the new regulatory regime will deal with civil responsibility on the part of the platforms.

## Response to questions

---

**Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?**

The government should review the effectiveness of annual transparency reporting, to ensure that further action can be taken if annual reporting does not achieve the intended objectives set out at paragraph 3.15.

**Question 2: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?**

Yes.

<sup>3</sup> Equality Act 2010

**Question 2a: If your answer to question 2 is ‘yes’, in what circumstances should this happen?**

We note the example of existing consumer protection law, where it is possible for organisations such as Citizens Advice to bring super complaints to the Competition and Markets Authority (CMA). We consider that a similar approach would be sensible in the context of online harm. However, before considering whether there should be super-complaints, it is important to ensure that any complaints involve an appropriate level of specification within a transparent framework

**Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?**

Different measures may be appropriate depending on the seriousness of the content/activity complained of.

**Question 4: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?**

We envisage a reporting requirement and being subject to a parliamentary committee.

Although we anticipate this will be reserved legislation under the Scotland Act, we note there could be aspects of the regulation which might touch upon devolved matters and thereby engage the devolved legislatures.

**Question 5: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?**

It is questionable whether this will be proportionate in all circumstances as the framework appears to be “one size fits all”.

**Question 6: In developing a definition for private communications, what criteria should be considered?**

We support the definition of “private communications” according to specific and considered criteria. We note that an appropriate definition in this context might not be appropriate in other contexts.

**Question 7: Which channels or forums that can be considered private should be in scope of the regulatory framework?**

We consider that the channel/forum should be technology neutral and the definition of “private communications” should determine whether something is within scope.

There is an interesting Scottish criminal case (the appeal judgement is *William James Kilpatrick v Her Majesty's Advocate* [2014] HCJAC 73) which may be instructive in this context. This concerned a post on a

private social group which was held by a jury to have incited others to commit violence which the accused claimed as 'just banter'. The accused was found guilty and initially given a prison sentence. However, this sentence was overturned on appeal.

**Question 7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?**

As per our comments above, if it is established that communications are indeed private (see need for precise definition identified in response to question 6 above), we do not consider that those communications should fall within the scope of the regulatory framework. The Article 8 infringement involved in monitoring such a private space requires the scrutiny to be proportionate and that is only likely to be the case for CSEA or national security issues, both of which are subject to existing regulatory frameworks and enforcement mechanisms in any case.

**Question 8: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?**

It is important to recognise that content may be used for very different purposes or to produce very different outcomes. For example material relating to self-harm could be framed in such a way as to encourage the reader to take such action or to warn against the dangers and suggest better options for those struggling, eg with mental health issues: the same factual content – for example the ways in which people inflict harm upon themselves – might form the bulk of substantive content in both scenarios. This impact may also depend on the relevant user/reader. Simple factual information on the same topic might encourage some readers and discourage others from taking a particular course of action. The context and manner in which information is presented will therefore need to be taken into consideration in ensuring a proportionate approach which targets those instances where people are seen to be intentionally generating and sharing harmful content online.

Furthermore, we consider that it is important to safeguard not only freedom of expression but freedom of information (in a general sense). Circulation of information on the internet should not be censored just because it relates to illegal activity, violence, harmful behaviour etc. However, we strongly support taking action where the content is presented in such a way as to incite or encourage others to partake in criminal or otherwise harmful activity, is threatening or abusive etc. Similarly, access to particular content, or the level of detail explored in relation to a particular topic may not be appropriate for particular age groups. Setting requirements, such as age limits, around access to certain categories of material could therefore facilitate a more appropriate regulatory regime.

We also note that the functions and duties of any regulator require to be properly and adequately coordinated with those of other bodies and entities having relevant roles. Examples would be the statutory obligation of local authorities to investigate etc. where the personal welfare of an adult seems to be at risk (Adults with Incapacity (Scotland) Act 2000, section 10) and their obligations under the Adult Support and Protection (Scotland) Act 2007; the obligations of the Public Guardian where the property or financial affairs of an adult seem to be at risk (section 6 of the 2000 Act); and the various relevant roles and

functions of Mental Welfare Commission for Scotland (including but not limited to those under section 9 of the 2000 Act).

**Question 9: What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?**

We have no comment on this question.

**Question 10: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?**

As a general rule it is likely to be more cost effective for duties to be taken on by an existing public body. In this case, the nature of the harm may mean that different regulators are more appropriate to take action in specific context.

**Question 10a: If your answer to question 10 is (ii), which body or bodies should it be?**

For example, where the harm is such that it amounts to a criminal offence, the police should take enforcement action. If there has been an infringement of data protection law, then the ICO should be responsible and if there is a consumer or competition impact, we consider that this should remain the responsibility of the CMA, regardless of the fact that the harm is generated online.

The danger with allowing a number of regulators to take enforcement action, is that different standards would inevitably creep in but the is perhaps inevitable anyway in this space.

**Question 11: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?**

We have no comment on this question. However, as set out in response to question 10, we note that in practical terms costs neutrality may be easier to achieve through existing regulatory structures.

**Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?**

Remedies should be tailored to ensure the most appropriate response to particular situations. Action that could disrupt business activities, ISP blocking and implementation of a regime for senior management liability may all be effective remedies in a particular context. However, there is no silver bullet. Other powers might prove more effective, depending on the nature of the harm identified.

We would favour flexible range of tools to be deployed according to clear guidelines indicating the possible approaches in relevant scenarios.

**Question 13: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?**

Yes. We note in this context the provisions of the General Data Protection Regulation as implemented through the Data Protection Act 2018.

**Question 14: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?**

Yes. As a matter of principle, we consider that there should be a mechanism to enable a full right of appeal in addition to judicial review.

**Question 14a: If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?**

If the regulator has the power to decide on guilt and impose a fine then in order to satisfy the right to a fair trial under Article 6 ECHR any appeal would have to be a full appeal of the merits.

**Question 14b: If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?**

See above.

**Question 15: What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?**

Different innovators may face different barriers to progress.

Artificial intelligence will be used by organisations to address these issues and but problems may arise if systems which have not been sufficiently refined are relied upon. Control mechanisms must be put in place to ensure that decisions are made with human input wherever necessary in order to ensure the correct balance is maintained between the prevention of harm and free speech.

## **Question 16: What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?**

Some aspects of privacy by design, an essential requirement of the General Data Protection Regulation/DPA 2018, may prove helpful in providing practical guidance, for example checklists to ensure that safety is embedded across business processes.<sup>4</sup>

## **Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?**

Effective awareness-raising campaigns, highlighting specific safety issues, perhaps differentiated according to the relevant sectors of the population at risk are important in ensuring that people properly understand the risks of online harm and can take appropriate action to protect themselves and their children online.

### *Vulnerable adults*

We are concerned that there is hardly any mention of adults with relevant disabilities, including in particular cognitive and volitional disabilities (“mental and intellectual disabilities” in the language of UN CRPD). There are a few statements such as the assertion at 9.19 of the need to ensure that people with disabilities “are not excluded” from relevant education, but no specific provisions about positively ensuring that they receive such education in forms that they can understand and apply.

While the consultation covers the exploitation of children, there is almost nothing about the exploitation of adults with relevant disabilities. Generally, where there is reference to age-appropriate provision, there should also be reference to disability-appropriate provision, which should cover the whole range of disabilities: physical, sensory and “mental and intellectual”. Issues of bullying and hate should be addressed in relation to people with disabilities.

It is important to note the obligations undertaken by UK Government in ratifying UN CRPD to consult with people with disabilities and their organisations as this project moves forward. References to provision of support should be linked to the obligations undertaken under Article 12 (in particular) of UN CRPD, and should be linked to existing provisions for support, such as provisions in relation to guardians and attorneys, as well as emerging techniques for provision of Article 12-compliant support.

Similarly, it is essential to address issues at the interface of data protection, privacy, and provision of support. It would be helpful to give greater clarity around the role of guardians, attorneys, supporters etc. in this context.

<sup>4</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>



**Question 18: What, if any, role should the regulator have in relation to education and awareness activity?**

Regulators have an important role to play in identifying areas for education and awareness raising. They are likely to hold the data that will allow particular problems to be identified, ensuring that the education programme can focus on areas of greater danger. However, education itself does not sit within their remit and it will be the role of government to provide the necessary guidance.

**For further information, please contact:**

Carolyn Thurston Smith

Policy Team

Law Society of Scotland

DD: 0131 476 8205

[carolynthurstonsmith@lawscot.org.uk](mailto:carolynthurstonsmith@lawscot.org.uk)