Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

Mozilla submission to the UK government Online Harms white paper consultation

Introduction

Mozilla is comprised of the Corporation behind the Firefox web browser and the Pocket 'read-it-later' application; products that are used by hundreds of millions of individuals around the world. Mozilla is also comprised of a not-for-profit Foundation that focuses on fueling the movement for a healthy internet. Finally, Mozilla is a global community of thousands of contributors and developers who work together to keep the internet open and accessible for all.

Mozilla welcomes the opportunity to respond to the UK government's public consultation on its Online Harms white paper. The white paper responds to legitimate public policy concerns around how technology companies deal with illegal and harmful content online. We understand that in many respects the current European regulatory paradigm is not fit for purpose, and we support an exploration of what codified content 'responsibility' might look like in the UK and at EU-level, while ensuring strong and clear protections for individuals' free expression and due process rights.

As we have noted elsewhere, we believe that the white paper's proposed regulatory *architecture* could have some promising potential. However, the UK government's vision for how this new regulatory model could be *practically* realised contains serious flaws. These must be addressed if this proposal is to reduce rather than encourage online harms.

Our three general concerns are as follows:

- **Scope issues:** The duty of care would apply to an extremely broad class of online companies. As such, there is a risk that smaller companies will be disproportionately burdened if the Codes of Practice are developed with only the tech incumbents in mind. In addition, the scope would include both hosting services, cloud infrastructure services, and electronic communications services,

despite the fact that they have radically different technical structures.

- **A conflation of terms:** The duty of care would apply not only to a range of *types* of content – from illegal content like child abuse material to legal but harmful material like disinformation – but also harmful *activities* – from cyber bullying, to immigration crime, to 'intimidation'. This conflation of content/activities and legal/harmful is concerning, given that many content-related 'activities' are almost impossible to proactively identify, and there is rarely a shared understanding of what 'harmful' means in different contexts.

- **The role of the regulator:** Given that this regulator will have unprecedented power to determine how online content control works, it is worrying that the proposal doesn't spell out safeguards that will be put in place to ensure its Codes of Practice are rights-protective and workable for different types of companies. In addition, it doesn't give any clarity as to how the development of the codes will be truly *co*-regulatory.

Yet as we noted earlier, Mozilla is committed to advancing internet health and we thus provide a number of recommendations in our response as to how the white paper's flaws could be addressed. In general terms, there are some crucial changes that the UK government should adopt if and when it brings forward the relevant legislation.

These relate to:

- **The legal status:** There is a whole corpus of jurisprudence around duties of care and negligence law that has developed over centuries, therefore it is essential that the UK government clarifies how this proposal would interact with and relate to existing duties of care.

- **The definitions:** Before proceeding, there needs to be much more clarity on what is meant by 'harmful' content and much more clarity on what is meant by 'activities'. The duty of care must acknowledge that each of these categories of 'online harms' requires a different approach. Moreover, The definition of any 'online harm' must thus be spelt out with far more detail and clarity by Parliament before they can be

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

made the object of a duty of care.

- **The regulator:** The governance structure must be truly *co*-regulatory, to ensure the measures are workable for companies and protective of individuals' rights. The regulator's competences must clearly exclude adjudications of legality of online content or issuing takedown notices to service providers. At the same time, it must be explicitly clarified that the regulator may not develop Codes of Practice that mandate the weakening of security measures or that mandate the imposition of general monitoring obligations.

We hope that our responses to the government's public consultation can help move the policy conversation forward, and ensure the future UK regulatory regime protects against online harms in a manner that is both rights-protective and supportive of online challengers.

If you have any questions about our submission or if we can provide any additional information that would be helpful as you continue your important work, please do not hesitate to contact Mozilla's Internet Policy Manager Owen Bennett, at obennett@mozilla.com.

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

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?

To understand the nature of 'online harms' and to ensure the policy responses to them are proportionate and justified, we need clear insight into how such online harms manifest and the factors that give rise to them. Furthermore, to ensure adequate protection by governments of individuals' rights - and respect for those same rights by private companies - we need broad and granular transparency with respect to online content removal orders issued by public authorities, as well as content removal undertaken by private actors pursuant to their own terms of service.

There are many areas of the digital sphere where such transparency by private and public actors in this regard is essential. Here we list three key ones.

- **Advertising transparency archives:** In order to develop effective policy responses to disinformation, there must be fully functional, open Application Programming Interfaces (APIs) that enable advanced research and the development of tools to analyse political adverts targeted to individuals. This requires access to the full scope of data relevant to political advertising, including targeting and engagement data, and such access must be provided in a format that allows for rich analysis. Contemporary tools provided often lack the necessary data or, due to their limited functionality, do not allow for meaningful analysis.

  Only with access to granular and comprehensive data sets can independent researchers and policymakers be able to begin to understand the structural factors that fuel the spread of disinformation online. More critically, absent such data and understanding, our policy responses will always be sub-optimum.

  As a signatory to the EU Code of Practice on Disinformation, Mozilla has taken clear steps to address the phenomenon of disinformation online. Moreover, as part

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

of our commitment through the Code of Practice, we have also encouraged the other signatories (incl. Google, Facebook, and Twitter) to provide more transparency with regard to political advertising on their platforms, specifically through offering effective advertising archive APIs. Our detailed recommendations to the companies on how to implement these advertising archives in a truly transparent way can be read here. The UK government should similarly encourage the companies to implement their advertising archives in this way.

- **Removal orders by governments:** Takedown requests by public authorities must always be grounded in the rule of law, with clear transparency as to what content is being removed and for what reason. Moreover, when public authorities issue content takedown requests, affected companies and individuals should have recourse to some form of appeals process and - in instances where content has been erroneously removed - effective remedies.

  In addition, public authorities should refrain from issuing 'referrals'; that is, takedown notices issued by public authorities to private companies for 'voluntary' review of conformity with the companies' terms of service. This approach to online content regulation - most prominent with respect to terrorist content online - undermines the rule of law and undermines the ability of the UK and other European governments to press for better human rights protections in speech regulation globally.

- **Voluntary takedowns by companies:** Companies rightfully apply their terms of service to protect their users from harm and ensure the online spaces that they operate are healthy. However, as web centralisation increases and a smaller number of online services become gatekeepers of free expression online, it is essential that companies' private content moderation practices are undertaken in respect of clear human rights standards. For instance, terms of service should be accessible, foreseeable and applied consistently.

  The UK government could play an important role in facilitating multistakeholder development of best practice guidelines for private companies' content moderation practices, and in encouraging companies to improve the accessibility and

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

foreseeability of their terms of service.

The Santa Clara principles on transparency and accountability in content moderation, and the dedicated content moderation report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, would serve as helpful guidance to the UK government in this regard.

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

Groups representing various interests, including consumer groups, child protection groups, human rights defenders, and anti-discrimination organisations, should be encouraged to direct their concerns to the regulator.

However, there is no need for a dedicated mechanism for 'super complaints'. Similarly, the regulator should not have competence to review complaints that concern individual instances of alleged 'online harm' and to take a decision as to whether such content should be taken down. Complaints should rather serve to provide intelligence to the regulator as to companies' efforts and users' experience under the duty of care framework.

Moreover, the involvement of the relevant third party organisations of the kind suggested above should be codified in the regulator's governance model. Rather than limiting the role of these third parties to simply bring complaints, they should be involved in the development and evolution of the Codes of Practice (as should the companies subjected to them). The inclusion of this external expertise in the regulatory model will ensure that measures taken to address online harms are justified, proportionate, rights-protective, and supportive of their stated aim.

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?

The regulator's monitoring of the sector, as well as the submission of complaints to it by

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

individuals and relevant organisations (as discussed in question two), will likely be sufficient to ensure effective adherence to the duty of care.

However, it is important to clarify that the submission of a complaint regarding individual instances of illegal or harmful content online - even if determined to be accurate in their identification - should not in and of itself determine a breach of the duty of care. Just as the most secure system can fall victim to a persistent attacker, so too may the most responsible and well-designed moderation systems occasionally fail to identify a specific instance of adversarial behavior. The ultimate determination of a breach of duty must depend on a far more rigorous assessment, including gathering more information on the company's practices, a clear demonstration of systematic breach, and offering an affected company the opportunity to appeal.

In any case, individuals should flag the existence of potentially illegal or harmful content to the relevant service provider in the first instance. This allows the service provider to take swift action to review the content and if necessary, remove or block access to it and notify law enforcement authorities.

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

The democratically-elected Parliament must act as the primary overseer of the regulator's work. The regulator must be obliged to report regularly on its work to Parliament, and Parliament must be equipped with the power to summon the regulator and request specific information regarding its operations.

Moreover, the regulator should not be empowered to define, elaborate, or extend the list of 'online harms' that fall under the duty of care. Given the sensitive nature of this task and its relation to broader rights and policy issues, only the democratically-elected Parliament ought to have competence to decide matters of such importance. When defining, elaborating, or extending the list of 'online harms' Parliament should engage in rigorous consultation with all stakeholders and adhere to the laws, standards, and conventions enshrined in domestic and international human rights law.

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

In contrast to a determination of the legality of behavior online, the Codes of Practice must be developed in a truly *co*-regulatory manner, that is, in a collaborative manner with a meaningful role for the affected companies and relevant third parties. Parliament should be consulted as part of this co-regulatory process, but should not be the sole definer of the Codes of Practice.

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

The duty of care should be restricted to application layer content disseminators ('content disseminators'), rather than the broader scope proposed. Content disseminators should be understood as web applications operating on the application layer of the OSI model, that *store and publicly disseminate* content uploaded by third parties[1]. Content disseminators are the most effective parties to help realize the goals of the white paper, and the only feasible entities able to undertake the foreseen mitigation techniques.

Indeed, many of the 'online harms' that the government's white paper aims at addressing - such as the proliferation of hate speech, disinformation, and so forth - are most typically associated with content disseminators operating at the application layer. Moreover, many of these harms occur in part due to the technical and commercial architecture of such services (e.g. recommendation engines, targeted advertising-based business models, public availability of third party content). Consequently it is logical to target measures at *that* layer of the internet stack, and those specific content-disseminating types of services.

Yet equally important is the fact that almost all of the measures envisaged in the Codes of Practice are *technically* feasible *only* to content disseminators that operate at the application layer of the stack. Indeed, to include services that sit on lower levels of the stack, such as electronic communications services, internet service providers, or enterprise cloud services, would give rise to a range of extremely concerning technical,

[1] This definition seeks to limit itself to services that operate on the open web, and that store and publicly disseminate user-generated content uploaded by third parties. This excludes, for instance, electronic communication services within the meaning of Directive (EU) 2018/1972 of the European Parliament and of the Council, web browsers, internet service providers, as well as providers of cloud services.

operational, and rights-based concerns. For instance, most enterprise cloud contracts typically bar the service provider from engaging with the content that the client is storing, to protect sensitive commercial or customer data, or intellectual property. Were enterprise cloud services to be made subject to a harm reduction duty of care they would almost certainly be forced to take operational measures that violate this basic sectoral practice (e.g. by scanning or filtering their clients data sets). Moreover, cloud service providers operate at a purposeful distance from the content they store - with little to no awareness of the content the customer is storing, and little actual engagement with the content that is stored. As such, they do not exhibit the required proximity to be made subject to a duty of care.

The situation for electronic communications services is equally concerning. Were they to be made subject to a harm reduction duty of care, services like WhatsApp, Skype and Gmail would likely be forced to undermine their own encryption implementations and violate their existing legal obligations under the EU E-Privacy acquis, in order to proactively identify 'online harms' being transmitted by individuals using their services. For users, the guarantees of end-to-end encryption with minimal collection of metadata is an assurance of privacy and security in the products. Compelling companies to modify their infrastructure based on government requests undermines this trust and denies them the ability to provide secure products and services to their customers. Again, as with cloud services, electronic communications service providers operate at a purposeful distance from the content they store - typically with no awareness of the content the customer is transmitting, and no actual engagement with the content that is transmitted.

Ultimately, to include such services within the scope of the duty of care would give rise to unacceptable security and privacy risks, and would be wholly unsuitable for their technical and operational nature. We thus advise the government to restrict the scope of the duty of care to the application layer content disseminators outlined above.

6. In developing a definition for private communications, what criteria should be considered?

In seeking to define 'private communications' we recommend that the UK government adopt the definition of interpersonal communications services under the EU Electronic

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

Communications Code (2018/1972).

This definition is clear, precise, and future-proof. Moreover, by retaining this existing definition (which is already entering the UK legal framework as per the transposition of Directive 2018/1972) the government will ensure domestic policy coherence and legal certainty for companies, while also avoiding fragmentation with other jurisdictions.

In any case, as per our response to question five such services should be excluded from the scope of the duty of care, and the definition should be utilised simply to clarify that delineation when legislating for the duty of care.

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

Services that are understood as private communications services as per the criteria outlined in our response to question six should be excluded from the regulatory framework. See also our response to question five above.

7(a). What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

Services that are understood as private communications services - as per the definition outlined in our response to question six - should be excluded from the proposed duty of care, as per the reasons outlined in our response to question five above.

This is notwithstanding the fact that many providers of electronic communications services (ECS) already undertake measures to address misuse of their services. For instance, some ECS providers have implemented product changes to restrict the number of times a private message can be forwarded to new users or channels, to limit the speed at which misinformation can spread[2]. In addition, some ECS providers offer user blocking

[2] See for instance, The Verge (2019) WhatsApp limits message forwarding in fight against misinformation, Available at: https://bit.ly/2R32mgf

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

functionality and the ability for users to report harmful or likely illegal behaviour to the provider[3].

Such procedural measures are proportionate and effective at addressing harms related to electronic communications services, in a manner that reflects the technical and operational architecture of such services and does not necessitate a weakening of essential security protections. We encourage the UK government to work with electronic communication services to explore how such measures could be furthered operationalised, outside of the duty of care regime.

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

- **Clarity on definitions:** According to the government's white paper, the proposed duty of care is constrained by the principles of 'reasonableness' and 'proportionality'. Understood as such, companies must take 'reasonable steps' to keep their users safe, in a manner that is 'proportionate to the severity and scale' of the relevant online harm.

  These principle-based constraints are of little value in and of themselves. It is therefore essential that when enshrining the duty of care in statute, Parliament should provide clear interpretive guidance as to how these terms should be understood by the regulator, the duty-bound companies, civil society organisations, and the individuals using online services.

  For duty-bound companies this clarification of meaning is crucial to ensure some degree of compliance certainty and to avoid stifling innovation - companies need to know what is expected of them to ensure their compliance resources are optimised for the task. For the regulator, clarification of meanings will ensure that the Codes of Practice that it must develop respect the spirit of the duty of care and the will of the legislator. More precisely, the principles of 'reasonableness' and 'proportionality' should have the effect of ensuring that the Codes of Practice are

[3] See for instance, Skype trust & safety, Available at: https://bit.ly/2FzSgR2

future-proof, balanced with industrial policy priorities, and respective of individuals' rights. Their clarification by the Parliament should focus on elaborating this further.

Additionally, these principles must be spelled out in detail as they are likely to double up as the key rights safeguards within the duty of care. In all instances, the impact on individuals' rights arising from content control actions should be understood *inter alia* with reference to the concepts of 'reasonableness' and proportionality'. As such, it is essential that the terms are clarified such that the regulator, courts, and civil society organisations can make the assessment.

Finally, the duty of care would apply not only to a range of *types* of content – from illegal content like child abuse material to legal but harmful material like disinformation – but also harmful *activities* – from cyber bullying, to immigration crime, to 'intimidation'. This conflation of content/activities and legal/harmful is extremely concerning, given that many content-related 'activities' are almost impossible to proactively identify, and there is rarely a shared understanding of what 'harmful' means in different contexts. The definitions of each and every 'online harm' must thus be spelt out with far more detail and clarity before making them the object of a duty of care.

- **Co-regulatory developments of the Codes of Practice:** Given that the regulator will have unprecedented power to determine processes underpinning online trust and safety, it is worrying that the white paper does not spell out safeguards that will be put in place to ensure the regulator's Codes of Practice are rights-protective and workable for different types of companies. In addition, it does not give any clarity as to how the development of the codes will involve input from affected stakeholders.

  Companies that are subject to the duty of care must play an integral role in drafting the Codes of Practice. They are best-placed to identify and understand the evolution of the 'online harms' on their services. Moreover, the companies themselves are likely to be best placed to understand the technological and operational solutions that are most likely to bring about a meaningful reduction in

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

the relevant online harm.

Linked to this, the co-regulatory Codes of Practice must be granular and comprehensive in volume. It should not be the case that there is one all-encompassing Code of Practice for a type of service or a type of harm. Given the plethora of business models, operational and technical architectures, and types of harm, the Codes must be equally diverse. A one-size-fits-all approach only benefits the largest incumbent platforms who have the resources to comply with vague and broad obligations.

Finally, the suggestion in the white paper that the Home Secretary should direct the development of, and sign off on, all codes of practice related to terrorism and child sexual abuse material runs contrary to the co-regulatory ethos. Such a unilateral approach would undermine the proportionality and operational effectiveness that the co-regulatory model is designed to achieve, as well as undermining due process safeguards. We thus strongly encourage Parliament to avoid making this process carve-out when legislating for the white paper.

.

- **Focus on practices over outcomes:** The regulator's role should be to operationalise the duty of care with respect to companies' *practices* – the steps they are taking to reduce 'online harms' on their service. The regulator *should not* have a role in assessing the legality or harm of individual pieces of content, and should not be empowered to issue takedown notices to companies. Such a role calls into play a number of critical legal and constitutional considerations, and exposes a real and significant risk of rights abuses. As such, when assessing companies' compliance with the duty of care and when developing the Codes of Practice, the regulator should focus exclusively on *practices, not outcomes.*

  Further to this, when assessing adherence to the duty of care then, the regulator should not base its decision on the existence of specific pieces of illegal or harmful content. As per our response to question three, just as the most secure system can fall victim to a persistent attacker, so too may the most responsible and well-designed moderation systems occasionally fail to identify a specific instance of adversarial behavior. The ultimate determination of a breach of duty must depend

on a far more rigorous assessment, including gathering more information on the company's practices, a clear demonstration of systematic breach, and offering an affected company the opportunity to appeal.

Finally, as will be explained in more detail below, the regulator's assessment of companies' practices must be constrained by a prohibition on general monitoring obligations as well as a prohibition on requirements for companies to weaken their security measures. Moreover, any alleged breach of the duty of care must provide for the opportunity of judicial review, and must not have the effect of depriving companies of their intermediary liability safe harbour..

- **Due process:** The duty of care will interfere with a number of the rights that citizens' expect to enjoy online, including their right to receive and impart information and their right to privacy. As with any such rights restriction, it is paramount that due process is built into the system by design. This is particularly important with respect to the regulator's enforcement power. Prior to issuing a sanction for breach of the duty of care, the regulator must be obliged to meaningfully demonstrate that a breach has occurred, and companies must have recourse to an appeals mechanism if they wish to contest the judgement.

  At the same time, companies facing sanction by the regulator for an alleged breach of the duty should retain the right to request judicial review of the regulator's decision before a court.

- **No general monitoring obligations or weakening of security features:** When legislating for the duty of care, Parliament should explicitly prohibit the regulator from including any generalised monitoring obligations within its Codes of Practice. Generalised monitoring would contradict the existing legislation in this space (particularly the EU E-Commerce directive). This legal prohibition that exists on general monitoring obligations remains as relevant as ever: as the Court of Justice of the European Union and national courts have consistently ruled, such a practice gravely interferes with citizens' fundamental data protection and privacy rights, as well as their right to receive and impart information. Moreover, general monitoring obligations place a huge financial and operational burden on tech challenger

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

companies, and undermines their ability to compete against the incumbent tech firms. Linked with this, any so-called 'targeted' monitoring obligation that the Codes of Practice seek to impose should take the utmost account of the principles of proportionality, reasonableness, and feasibility, and respect the spirit of the CJEU's reasoning in the SABAM v Netlog case[4].

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

As a general rule, the regulator's Codes of Practice should be advisory and principles-based. Understood as such, companies would use the Codes of Practices as benchmarks and guidance when implementing their own unique measures to comply with the duty of care. This co-regulatory approach is essential to ensure the duty of care is scalable, finely-tailored, and future proof.

For smaller companies in particular, the regulator must function as a source of best practice, guidance, and feedback. The regulator should assist companies when developing specific duty of care compliance strategies on demand, and advise companies on operational or technical measures that can streamline or enhance their trust & safety approaches.

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

The regulator should be a new public body, rather than an existing body. Its mission should be to operationalise the duty of care, and crucially, it's mission statement and terms of reference must also include a clear obligation to preserve internet openness and protection of citizens' fundamental rights. Its governance model should be optimized for co-regulatory approaches, as per our response to question eight. Moveover, the regulator should work closely with existing regulatory authorities that today have overlapping competences, including OFCOM and the National Cyber Security Centre. It should also

[4] Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, 16 February 2012

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

place a special emphasis on collaboration with the Information Commissioner's Office, given the linkages between personal data and many 'online harms'.

As per our response to question four, it should be answerable to Parliament, and as per our response to question nine, its governance model should be co-regulatory and there should be clear prohibitions on Codes of Practice that include general monitoring obligations or security-weakening obligations. Finally, as we have asserted at various points in this consultation response, the regulator's terms of reference should clearly disbar it from adjudicating the illegality of content or issuing content takedown orders to private companies.

Finally, given the technical role of the regulator, it should be staffed with suitable expertise drawn from engineering, legal, and data science backgrounds amongst others.

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

No answer.

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?

The regulator should not be empowered to implement:

- **Senior management liability**: Senior management liability should not be considered as a potential sanctioning mechanism for breaches of the duty of care. Such an approach would be disproportionate to the objective pursued and likely undermine the ability of multinational companies to attract senior staff to the UK. Moreover, senior management liability also would have a negative impact on free expression, as the likely cost of breaching the duty of care would create an incentive for companies to undertake over-removal of user content.

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

- **ISP access blocking:** Access blocking by internet service providers is a blunt and ineffective instrument that should not be considered as a potential sanctioning mechanism. ISP blocking at the domain name system (DNS) level typically leads to the blocking of a disproportionate quantity of legal and public interest content. Moreover, with the advent of VPNs and public DNS resolvers, ISP blocking at the DNS level is easily circumvented and an increasingly ineffective mechanism at preventing access to content online.

However, the regulator could be empowered to:

- **Name and shame:** Brand image considerations are an effective incentive for companies to operate diligently. This holds true both online and offline. In that context, a possible useful enforcement tool for the regulator could be to 'name and shame' companies that are found to be failing to adhere to the duty of care. As with all sanctioning powers, this should only be considered upon completion of a thorough investigation and a resolution of any relevant appeals by the duty-bound company.

- **Request further information:** Before issuing any sanctions, the regulator should be obliged to request further information from the service provider to understand the company's trust & safety processes and the steps it is taking to demonstrate compliance with the duty of care. Requests for additional information should be clear, precise and justified, and provide the service provider with an opportunity to submit additional qualitative and quantitative data that may aid its demonstration of compliance. Such information requests should not have the effect of conflicting with data protection law, the company's security processes, or intellectual property law.

  The information provided therein should be taken into account before any sanctioning by the regulator is considered.

- **Request changes to processes**: The regulator should not be empowered to disrupt business activities, as this is likely to be a disproportionate response and require far greater assessment and consultation than the regulator's governance model allows.

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

However, in certain cases where a company is judged to be failing to adhere to the duty of care, the regulator could be empowered to recommend changes to a company process that the regulator considers as potentially aiding compliance (e.g. hiring more localised content moderators, undertaking regular algorithmic audits, etc).

These recommendations to change certain processes should be non-binding, and subject to a demonstration of effectiveness. Moreover, if the company chooses not to implement the regulator's recommendations, it should be able to demonstrate the effectiveness of alternative solutions.

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?

The obligation to appoint a nominated representative within the UK or EEA would cause considerable compliance costs for small and medium-sized companies and disrupt cross border e-commerce, without meaningful gain.

Instead, the government should explore solutions that allow appropriate company staff to easily connect with the regulator where the situation warrants it. This could involve, for instance, companies making the contact information for their legal and trust & safety teams clearly available on their websites, or disclosing a single issue-based point of contact to the regulator.

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?

No answer.

15. What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role

Mozilla EU Policy

Rue du Trône 51
Brussels 1050
Belgium

should government play in addressing these?

No answer.

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

No answer.

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

No answer.

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

No answer.