5Rights Foundation response to the Online Harms White Paper

July 2019

About 5Rights Foundation

The digital world was imagined as one in which all users would be equal, yet 1/3rd of internet users are children. Nearly one billion children are growing up in an environment that systematically fails to recognise their age, and in doing so, fails to uphold the protections, privileges, legal frameworks and rights that together constitute the concept of childhood. 5Rights Foundation works towards a digital environment that anticipates the presence and meets the needs of all children, so they can access it ***knowledgeably, creatively, and fearlessly.***

5Rights Foundation's activities focus on developing policies and implementing standards that support systemic change of the digital world on behalf of under 18s. Current projects include: supporting the Council on the Rights of the Child in writing a codicil (General Comment) on the Convention of the Rights of the Child (UNCRC) to determine how children's rights should be applied in the digital world; a set of universal technical standards for childhood with the IEEE (Institute of Electrical and Electronics Engineers); a Child Online Protection Policy and five-year Implementation Plan that has just been adopted in cabinet by the Government of Rwanda; and we sit on in a number of relevant international bodies e.g. UN Broadband Commission for Sustainable Development, MIT's Council on Extended Intelligence, We Protect Technical Working Group and the UNICEF AI 4children.

General comments

We welcome the Government's Online Harms White Paper and the ongoing commitment to making the UK the safest place in the world to be online. 5Rights Foundation is responding to the consultation from the perspective of and in consultation with children and young people, alongside and on whose behalf we work. We associate with the submission made by Carnegie UK Trust and Carnegie's broader work on the duty of care.

Children and 'public harms'

We welcome the importance that the White Paper ascribes to the risks posed to children and young people, which is reflected both in the frequent references to the need for children to be given special consideration online and to the list of harms in scope. However, it is important to recognise that children are also subject to the risks and harms that affect the population more broadly, both on an individual level and on a community or societal level. 'Public harms' like electoral interference, disinformation, polarisation, fraud, data breaches, and threats to public health, all impact the lives of children and young people. As Professor Sonia Livingstone OBE has repeatedly explained, these issues actually affect children *disproportionately*, given both their developmental vulnerabilities and the fact that children's status as 'early adopters' of emerging technologies make them 'the canaries in the coal mine for threats to all'.

Children are a huge demographic online – one fifth of users in the UK and a third worldwide are under 18 – and they are accessing a vast range of services, not simply those few services

that are *targeted* directly at them. All online services *accessed* by children must therefore be subject to specific responsibilities, and specific regulatory oversight. In short, internet companies need to anticipate the presence of children on their online services, and design their services accordingly. Children must not be required to navigate a digital environment that systematically fails to cater for their needs – rather, we need to forge a digital future and a digital world that children and young people can access knowledgeably, creatively and fearlessly.

Scope

We acknowledge that certain kinds of online service pose more risk than others. The White Paper is right to identify, for instance, that services that 'allow users to share or discover user-generated content or interact with each other online' pose particular risks. However, *all* services (online and off) have a responsibility to the welfare of those with whom they engage, so all online services should be covered by a regulatory framework that formalises this responsibility for any sector.

Online services that do not operate in ways that are likely to lead to harm will clearly have very little to do, if anything, and will rightly expect not to be the focus of any proactive regulatory action or oversight as a result. The proposed duty of care (which we see as a vital, thoughtful, and world-leading intervention by the UK Government) is by its nature a requirement to consider the welfare of users *in advance*. Given the fast pace of change online and the constant emergence of new services and types of service, a broad scope with clear criteria for action is the best way to future-proof the regulatory framework.

We recommend that the scope of the White Paper and the duty of care is broadened, but that the regulator clarifies both the proportionate approach it will take to oversight and enforcement, and the types of online services that it sees as posing particular risk. Services that are likely to be accessed by children should always be a priority. The Government might usefully set out the criteria by which it will judge compliance with the duty of care, and ask the regulator to publish guidance that makes clear how online services of different kinds will be considered.

Enforcement of terms and conditions and community guidelines

We welcome the White Paper's statement that 'Relevant terms and conditions will be required to be sufficiently clear and accessible, including to children and other vulnerable users. The regulator will assess how effectively these terms are enforced as part of any regulatory action.'[1]

Published terms and conditions and community guidelines, including age restrictions, enable users, and particularly children or parents, to decide if a service is age-appropriate and to anticipate any risks it might pose. Terms and guidelines are therefore fundamental to the safety of children online and to their trust and confidence in the services they are using. This principle that companies must 'say what they do and do what they say' must be at the heart of the duty of care, and a priority for regulatory action (see question one for further comment).

[1] Online Harms White Paper, UK Government, April 2019

Innovation
Innovation and safety are often portrayed as binary opposites, but they are not. Innovation is driven by the need to solve a problem. In its work around the White Paper, the Government is identifying problems regarding the safety of citizens online, setting out the responsibilities that companies have to solve those problems, and asking them to find the solutions. In this way, regulation supports innovation. The development of KYC ('Know your customers') solutions, multi-factor authentication, and other technological protections are all recent examples of where positive innovation has followed regulation.

We would also note that dynamic, innovative markets are supported by clear, reasonable, and proportionate regulation, in which the needs of consumers and the expectations of authorities are well expressed (see, in addition, our comments under question 15).

Privacy
Privacy is fundamental to safety in the digital environment. This is especially the case as increasingly we inhabit 'connected environments', capable of and designed to collect our personal data: often with a view to supporting automated decision-making. Particular care must be taken in setting out regulations relating to services of this nature, and privacy must be at the core.

Moreover, in ensuring that online services take their responsibility to protect users' privacy seriously, regulation must be clear that individuals have a right to privacy not simply in relation to other users of an online service, but also in relation to the company that provides that online service, as well as any other parties (including but not limited to Government) with whom that company might have a relationship.

Identifying which users are children
The White Paper is right to recognise that companies should 'implement effective measures to identify which users are children, and adopt enhanced safety measures for these users.' It is self-evidently impossible to provide children with specific protection if companies do not identify (to whatever extent) their child users **(i.e. those under 18).**[2]

As we note below, a recent YouGov poll revealed that 76% of parents think that internet companies should establish the ages of the people who use their online services, to enable child specific protections to be put in place. Just 16% disagree. The same poll found that 90% of parents think it is important that internet companies are required to follow rules to protect children.

The Government should also make clear in legislation that companies will be failing to fulfil their duty of care to children specifically if they have 'constructive knowledge' that underage children are using their services, or that child users (under 18) of their services are not receiving the necessary safeguards. 'Constructive knowledge' is defined as

[2] See for example, UNCRC Article 1: 'a child means every human being below the age of eighteen years unless under the law applicable to the child'.

knowledge that one using reasonable care or diligence should have, and therefore that is attributed by law to a given person.'[3]

Given that the Information Commission Office (ICO)'s draft Age Appropriate Design Code includes provisions in this area, the regulator should work closely with the Information Commissioner in developing such regulation.

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?

Companies' published terms

In our report *Towards an Internet Safety Strategy*, 5Rights recommended that a regulator be given:

> 'powers to demand information where it is necessary to come to judgments in relation to promises made in published community guidelines, terms and conditions, privacy notices, age restrictions, company advertising or published information about services.'

We therefore welcome the White Paper's proposal that 'evidence of effective enforcement of the company's own relevant terms and conditions will form a key part of the transparency requirements.

We recommend the regulator should be given strong statutory information-gathering powers in order to support it in determining if an online service has upheld its own published terms and conditions and community rules.

Promoting children's rights

Companies should be held to account for more than the mitigation of risk and harm – they also have a responsibility to promote the welfare and rights of the children who access their services. Technological progress should be harnessed for societal good, to promote individual and collective rights, and to meet the needs of vulnerable users, particularly children. It should also reflect the values embodied in our culture, laws and international agreements in all areas of a child's life. In short, the digital environment must be one in which the rights of children are promoted and all aspects of their development, not simply their safety, are supported. This would improve trust in the services that children use, allowing them to access them more confidently.

We recommend that companies be required to account for the efforts they take to promote the rights of children, and for any impact – positive or negative – that their online services have had on the rights of children.

Research access to commercial data

[3] Black's Law Dictionary, 2014

The White Paper states that 'the regulator will encourage and oversee the fulfilment of companies' existing commitments to improve the ability of independent researchers to access their data, subject to appropriate safeguards.'

We support the proposal for existing commitments to be overseen by a regulator. However, as the White Paper concedes, existing commitments are not sufficient to ensure that risks and potential harms can be identified and evaluated by researchers and academics, independently and in good time.

The duty of care approach means 'companies must improve their understanding of the risks associated with their services and take effective and proportionate steps to mitigate these risks'. This responsibility, and therefore the duty of care as a whole, would clearly be well-supported by stronger requirements to make relevant data available to independent researchers.

We recommend that the Government introduces a public interest data access law in order to allow independent researchers to be licensed to access particular data from the online services in scope. This should build on the principles established by the Approved Researcher Scheme used by the Office for National Statistics (ONS).[4]

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

Yes.

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

We note that Article 80(2) of the GDPR already provides for a super complainant regime, albeit in relation to data rights specifically, but the UK Government has chosen not to implement it so far. We agree with the Noble Lords that made the case for implementation during the passage of the Data Protection Bill, that 'a super-complainant system would help to protect anonymity and create a stronger enforcement framework', that it would 'give consumers power', and that it 'supports their rights without them having to specifically understand that the rights exist', which we know is a barrier.[5]

This is particularly the case in respect of children, who are likely to be less aware of both their rights and the means by which they can exercise them. Indeed, in the absence of a mechanism allowing designated bodies to seek redress on behalf of children, their rights *cannot* be adequately defended. Rights that cannot be enacted cannot reasonably be said to be offered.

The need for a super-complainant regime or collective redress mechanism is also important given the impact that online services have at a societal level. Such societal harms, including

[4] Approved Researcher Scheme, ONS
[5] Columns 132, 144, 158, Data Protection Bill [HL], 10 October 2017

algorithmic bias and discrimination, disinformation, and democratic interference, may have a significant impact on individuals, including or especially children, but may be less open to individual complaint.

The Government should draw from established principles regarding both the eligibility of super complainants and the process of super complaints, including those regimes overseen by the Competition and Markets Authority and the Financial Conduct Authority. Particular emphasis should be placed on the independence and impartiality of designated bodies.

We recommend that super-complaints should be permitted where an online harm relates to children, either specifically or as part of a wider group. The Government or regulator should ensure that a body or bodies with experience representing the interests of children and with specific expertise on children's rights online are designated as a super complainant.[6]

We recommend that the Government also implements Article 80(2) of the GDPR in relation to the Age Appropriate Design Code specifically, so as to ensure that (in respect of their data) children can benefit from the protection that a super complainant regime provides.

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?

The White Paper states that 'while the regulator would not normally adjudicate on individual complaints about companies, users will be able to report concerns to the regulator. This will be an important part of the regulator's horizon scanning to identify where companies might not be fulfilling their duty of care.' Learnings might be drawn from Ofcom's 'Broadcaster First' system, in which user complaints go through the service's own reporting procedures and are only referred to the regulator if not satisfactorily redressed. Provided this system is supported by strong requirements around transparency and timeframes, it avoids undue burden on the regulator itself while also incentivising services to improve their processes.

We recommend that companies be required to signpost users to where they can report concerns to the regulator, including concerns about the failure of companies to resolve user reports adequately or within expected timelines, and concerns about the misuse of personal data.

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

We support the recommendation of the House of Lords Communications Committee that, 'to ensure a strong role for Parliament in the regulation of the digital world, the [regulator]

[6] We note that this a departure from the principle set out in the Financial Services and Markets Act 2000, which provides that 'the Treasury may designate a body only if it appears to them to represent the interests of consumers of any description'. However, given the specific protection that children require online and their relative in ability to seek redress themselves, we believe the departure is justified.

should report to a joint committee of both Houses of Parliament whose remit is to consider all matters related to the digital world.' The regulator should report 'on a quarterly basis and regularly give evidence to the new joint committee to discuss the adequacy of powers and resources in regulating the digital world.'[7]

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?

Prioritising services that pose a risk to children
The White Paper states that:

> 'The regulator will take a risk-based and proportionate approach across this broad range of business types. This will mean that the regulator's initial focus will be on those companies that pose the biggest and clearest risk of harm to users, either because of the scale of the platforms or because of known issues with serious harms.'

We support this approach, but the regulator must be clear about which online services it sees as posing the biggest risk to users.

We recommend services that are likely to be accessed by and pose risks to children be a priority for the regulator, whether those risks are content, conduct, contract, or contract risks.[8] It will be particularly important for the regulator to focus on services that allow for interaction between children and adults.

Risk-based approach
In addition, we note that the proposed codes of practice that will form a large part of the duty of care are not sufficiently focused on risk.

For instance, the White Paper states that the code of practice for Child Sexual Abuse and Exploitation (CSEA) should include details of reasonable steps companies should take to 'proactively identify and act upon CSEA activity such as grooming', and to 'proactively identify accounts showing indicators of CSEA activity and ensure children are protected from them'. While both crucially important, there is not enough that directs online services to undertake preventative measures, since they involve identifying CSEA activity first and *then* dealing with it.

A risk-based approach would start by identifying the types of service and the elements or features of a service that might facilitate (or even promote) CSEA, and then taking reasonable steps to change them so as to reduce or eradicate this effect. In the case of a social media network or an online game, for instance, this might mean preventing child users from being identified or contacted unsolicited by other or adult users, or preventing children's location from being publicly viewable to other users. These are just two examples of how a risk-based approach would reduce harm, by driving better safety-by-design.

---

[7] Page 4 & 63, Regulating in a digital world, Select Committee on Communications, 9 March 2019
[8] Page 4-6, Towards an Internet Safety Strategy, 5Rights Foundation, 2019

We recommend that taking steps to mitigate risk, particularly at the design level, should be a core pillar of the duty of care and more clearly reflected in the codes of practice proposed in chapter seven. In taking a targeted and proportionate approach, therefore, the regulator should focus attention on those services that by their nature and design pose risks to children, rather than simply on those services through which harm has already arisen.

'Every day' harms

The range of harms considered by the regulator must also be expanded. The White Paper focuses on what might be considered 'extreme' harms, and these are separated in chapter two into three categories: 'harms with a clear definition', 'harms with a less clear definition', and 'underage exposure to legal content'. Addressing all of the harms listed is clearly of huge importance, but there are also a range of more every day or 'quotidian' harms that the White Paper fails to cover, either to a sufficient extent or at all, and which effect huge numbers of children.

Services that expose large numbers of children to these 'every day' harms require attention just as do services that expose smaller numbers of children to more extreme harms. Harms are not 'hierarchical', and are often cumulative and interrelated. A focus on 'extreme' harms may not be sufficiently preventative, therefore, as it fails to recognise that children's experience of a 'lesser' harm may well contribute to their subsequent experience of, or susceptibility to, more 'extreme' harms.

We recommend that the regulator considers a broader range of harms in assessing services' fulfilment of their duty of care, including more 'every day' harms. Where evidence on these harms is lacking, the companies should be directed to uphold the precautionary principle, which though a key aspect of the duty of care model developed by Professor Lorna Woods and William Perrin, does not meaningfully feature in the White Paper. Given the fast-changing nature of technology and the difficulty of building a robust evidence-base around a variety of online harms, the precautionary principle is crucial to ensuring that due consideration is given to the risk of harm before such harm arises. This is especially the case given that children are often the 'canaries in the coalmine' in the digital environment.[9]

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

In the course of consulting on a definition for private communications, the Government or regulator could also usefully consult on and publish a definition of 'privacy' itself. Any definition must reflect the fact that privacy is multifaceted and includes both privacy between different users of an online service, as well as privacy between users and the provider of an online service, or any other parties (including government agencies) with whom a provider might have a relevant relationship.

We recommend that a service cannot be described as private simply because its users enjoy privacy from other users, and the definition of private communications must make this

[9] Rethinking the rights of children for the internet age, Dr Sonia Livingstone, LSE, March 2019

clear. Any definition must also be clear to users themselves. If a user has reasonable expectation of privacy from a commercial company, third party or government whilst accessing a service, then any limits to that privacy must be both justifiable and clearly communicated.

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

While we agree that a 'differentiated approach for private communication' is needed, this should not mean that private platforms are not within the scope of the regulatory framework. All online services have a duty of care to their users, irrespective of whether they facilitate private interaction or public interaction between services users. As above, different requirements will need to be applied, but this is no case for private channels to be removed from the scope of regulation altogether.

This is especially the case given the recent moves of certain online services towards encryption.[10]

The Government and regulator must ensure that such moves do not serve to diminish companies' responsibilities to protect children or to fulfil their duty of care more broadly. While many companies are understandably keen to shore up the privacy of their online services, this must always be balanced with the need for child protection.

We recommend that companies be required to take reasonable steps to protect children on private and/or encrypted channels, and to consider to the needs of children when deciding what encryption technology to use in any element of a service.

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

The White Paper states that 'requirements to scan or monitor content for tightly defined categories of illegal content will not apply to private channels.' While we appreciate the Government's concern not to encroach on the privacy of individuals engaging in private communication, we believe this must be balanced against the Government's recognition that there is 'a strong case for mandating specific monitoring that targets where there is a threat to…the physical safety of children, such as CSEA.'

As automated scanning and filtering of encrypted channels (where no data need leave a user's device) become more possible, we do not believe it is necessary to rule out the scanning of private channels for known child sexual abuse material (CSAM). Provided this was tightly defined, strictly limited to known CSAM, and the regulator was satisfied both that the service was secure and that the service provider had no access to users' personal data, we would support the development of regulation to provide for it.

10

Scanning of private channels notwithstanding, there are a range of requirements that might apply to private channels that would reduce the risk of harm without trespassing on questions of privacy.

For instance, private messaging services would evidently be safer if they introduced robust, privacy-friendly age-verification mechanisms. Certain safeguards around adult/child interaction might also be introduced, such as blocking unknown adult users from making initial contact with child users through the service or restrictions on children being added to group chats with adults they don't know. Any potential for unintended consequences would obviously need to be considered carefully, but a failure to introduce any requirements on private channels, particularly those with child users, would mean that a great deal of preventable harm would continue to go unaddressed.

We recommend that the Government relaxes its proposed position on not introducing requirements to scan for illegal content on private channels, specifically to allow for the scanning of known CSAM. Where the safe-by-design principles set out by the regulator do not encroach on the privacy of users, such principles should apply equally to services offering both public and private channels.

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

We strongly support the White Paper's commitment to 'prioritising action…where children or other vulnerable users at risk'.

We recommend that online services that are likely to be accessed by and pose a risk to children is the focus of the regulator's work. The proportionate approach to be adopted by the regulator must be tied closely to the nature of the risk that users, particularly children, are exposed to in using a service, noting that some risks are cumulative or promote behaviours that lead to harm.

Question 10/10a: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body? If your answer to question 10 is (ii), which body or bodies should it be?

We support the House of Lords Select Committee on Communications in suggesting that a Digital Authority be established, bringing together existing regulators in the digital world, and be empowered to extend or recommend an extension to the remit of these regulators where it deems necessary. This should include recommendations for an entirely new regulator in a specific area or areas, if the need arises.

We believe that a new regulator will be necessary, though given the time it will take for a new regulator to become operational and effective, an existing regulator should be mandated to support the regulation of online services in the meantime (and to scope a permanent regulator in due course).

Child-focus

In our report *Towards an Internet Safety* Strategy, we recommend the following:

> 'A child-focused body is required, resourced with staff and funds, to carry out research and make policy recommendations against predetermined, long-term objectives and to support the work of all departments to develop and implement evidence-based, consistent policy across government. Such a body would put the views and experiences of users (under 18s) at the heart of its work and it would work closely with, but not be directed by, industry. This work should be backed by statutory powers, including the power to require disclosure of information and people to appear before it. Such a body would provide critical leadership and ensure that all stakeholders (including government and industry) were held accountable for progress.'

Such a body may be standalone or (more likely) a division or department of a more general regulator.

Crucially, we recommend that regulators make provision for the rights, needs, and vulnerabilities of children to be given specific attention, and allocated specific expertise, as part of their role.

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

Well-funded regulators are essential to effective regulation. Since the 1970s, the 'Polluter Pays' principle has met with widespread acceptance as the most efficient method of mitigating external costs created by corporate activity. Regulators should be able to recover costs of regulating from those that they regulate, and the Government/Parliament should create mechanisms to support any new regulation in this manner.[11]

Additionally, tax revenue should come via the anticipated international tax reforms for internet companies, and should support central Government to adequately fund an independent regulator.[12]

We recommend that the regulator be supported both by funds received from those companies within scope of the regulation, and by the Government through the taxes it receives from internet companies.

[11] Section 38 of The Communications Act 2003 requires service providers over a certain threshold to pay fees to Ofcom annually in order to fund the operations of Ofcom. This system relies on a self-certification system that may not be appropriate for regulation with the scope envisaged here, but it offers precedent on which the Government and the regulator can draw.

[12] Digital Services Tax: Consultation, HM Treasury, 7 November 2018; Hammond Targets US Tech Giants With 'Digital Services Tax', The Guardian, 29 October 2018; Big Tech's Next European Nightmare: A Tax on Revenues, CNN, 31 October 2018

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?

Yes, to all three.

All of these powers are necessary if regulation is to 'bite' on companies with such dizzying market value. The proportionate, risk-based approach to regulation outlined in chapter five will ensure that those that pose less risk avoid any undue regulatory burden.

We recommend that any sanctions or enforcement action escalates in line with the nature and extent of the risk, and the efforts a company has made to mitigate them.

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.

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?

Care must be taken to ensure that any statutory mechanism to appeal a decision of the regulator does not lead to 'game-playing' by companies seeking to undermine the effectiveness of regulation or the regulator. We note that the Competition Appeal Tribunal has the power to 'strike out' appeals for which there is no proper case, or where the appellant has persistently instituted 'vexatious' proceedings.[13] This is an important power for the regulator to have at its disposal.

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

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?

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?

First and foremost, innovation and safety are often presented as binary opposites. This is a) not true and b) allows internet companies to avoid the responsibilities to the welfare of their users that are the norm in all other sectors.

[13] The Competition Appeal Tribunal Rules 2015, Statutory Instrument 2015 No. 1648, UK Parliament

Innovation can be and is directed towards safety and public benefit in the digital environment. For example:

- The ICO has launched 'Sandbox', a new service designed to support organisations using personal data to develop products and services that are innovative and have demonstrable public benefit.
- The Centre for Immersive Technologies, recently established by the University of Leeds, has committed that: 'This new centre will help ensure that the next technological revolution is harnessed for the benefit of society. By working with a wide range of partners, from technology companies and hospitals to museums, we are ensuring that the work carried out by researchers in Leeds is making a real difference to the world.' [14]
- The Centre for Data Ethics and Innovation 'will seek to deliver the best possible outcomes for society from the use of data and AI. This includes supporting innovative and ethical uses of data and AI. These objectives will be mutually reinforcing: by ensuring data and AI are used ethically, the Centre will promote trust in these technologies, which will in turn help to drive the growth of responsible innovation.'[15]

In our view, a key barrier to innovation in the development of safety technologies and safer services is the lack of any meaningful regulatory obligation. In the absence of the 'carrot' of commercial incentive, regulators play an important role in providing the 'stick'. So, while the Government and regulator must play a role in commissioning research and development itself, innovation will naturally be provoked by setting standards for companies to meet.

We note that Doteveryone's *Tech Workers' View* report found that regulation is the 'preferred mechanism' for ensuring that the consequences of technology are taken into account by companies, with almost half of tech workers stating that their sector 'is currently regulated too little.'[16]

We recommend that Government produce clear enforceable regulation to drive responsible and safe-by-design innovation.

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

Above all, organisations need clarity about the standards and requirements they are expected to meet, such as how a duty of care will be assessed, including their obligations to enforce their minimum age restrictions, transparency requirements, etc. It should also be a priority for the regulator to avoid a situation in which smaller organisations, or those who lack the relevant expertise, are unsure of their obligations and therefore misdirect their resources, engage in overcompliance, or simply wait until clarity is provided. Uncertainty, rather than regulation, stifles innovation.

[14] Immersive technologies become the new reality at Leeds
[15] Centre for Data Ethics and Innovation, November 2018
[16] People, Power and Technology: The Tech Workers' View, doteveryone, 2019

We recommend in addition that the regulator should encourage larger companies to make available to smaller companies their safety technologies and safe designs.

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

We address the need for education and awareness in response to question 18, but the best way of ensuring children are safe online is to make the services they use safe by design. It is not reasonable to ask parents to ensure the online safety of their children in an environment that has not been built with them in mind.

Parents overwhelmingly support regulation to this effect and are increasingly concerned that whilst many announcements have been made, they have not seen a corresponding change in service design.

A poll conducted by YouGov in June 2019 (commissioned by 5Rights) asked parents of children under the age of 18 about their views on internet regulation, with a focus in some questions on data protection regulation. The results were as follows:

- 90% of parents think it is important that internet companies are required to follow rules to protect children ('children' defined as those under 18 years old) online.
- 76% of parents think that internet companies should establish the ages of the people who use their online services, to enable child-specific protections to be put in place. Just 16% disagree.
- 67% of parents think an official regulator or Government should decide the rules for how internet companies should use children's personal data. Just 15% thought this should be left to the internet companies themselves.
- 82% of parents think internet companies should be held accountable in law for how well they uphold their own community guidelines, terms and conditions, and privacy notices.
- 78% of parents think that regulation on the use of children's data should apply to all online services likely to be accessed by children, rather than just online services that are targeted at children specifically.

In sum, parents overwhelmingly support regulation to protect children online. We would draw particular attention to the support among parents for services to establish the age of users. Parents could clearly be more confident about their children's online use if they knew that any age restrictions or other child protections were properly upheld.

The polling also demonstrates strong support among parents for the protections offered by the Age Appropriate Design Code, published in draft form by the Information Commissioner earlier this year. While separate from the White Paper, the Code should act as an exemplar for the many codes that will be introduced under the umbrella of the duty of care.

We recommend that online services be required to recognise the needs of children by adopting a safety-by-design policy, rather than outsourcing responsibility to parents and children who have insufficient control over the safety of service design.

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

In our recent report *Towards an Internet Safety Strategy*, we note that 'Education is a key component of any safety strategy'. **As such, the regulator should have a clear duty to promote digital literacy and competency, particularly among children, similar to the education duties of other regulators such as Ofcom and the ICO.**

We also note in our report, however, that '[education] is frequently used to demand that users, particularly children, be resilient to a system that does not respect or protect their safety and security.'

While children's digital literacy and competency must be promoted (as we come on to), children will only be able to access the online world positively if they are recognised and respected in it. Any education and awareness strategy that complements the Government's plans for regulation must therefore include the introduction of ethics and safety by design to relevant tertiary education, and to professional training too.

On children's education specifically, the White Paper notes that 'many companies have invested in education and awareness activities.' However, some initiatives (Google's 'Be Internet Awesome', for example) have been criticised for presenting tech companies as 'impartial and trustworthy', as well as for 'glossing over' the risks associated with the sector's treatment of its users for commercial purposes (e.g. profiling, promoting compulsive use, geolocation tracking, and targeted advertising).[17]

For example, whilst the National Crime Agency are deeply concerned about the ability to track children in real-time and the social and physical risks associated with that; or the Chief Medical Officer is concerned about the ubiquity of 'addictive capabilities' on online services used by children; or the Information Commissioner is worried about the effect of smart toys that enable interaction with strangers: tech-led education programmes tend not to address these issues at all.

As we explain in *Towards an Internet Safety Strategy*:

> 'A review of digital competency programmes (including those offered in the curriculum in England, Scotland, Wales and Northern Ireland) undertaken by BT and 5Rights (2017) found the overwhelming majority, 50 of the 73, covered e-safety; 17 looked at the impacts on personal wellbeing; nine considered digital rights and only one considered commercial drivers/design, which are broadly understood to be at the core of many of the issues that children face online. There is considerable

[17] Google is teaching children how to act online. Is it the best role model? Natasha Singer and Sapna Maheshwari, NY Times, October 2018.

evidence that children want a very different approach to education; focused on the purposes of technology, and offering social and critical skills.[18] Education must not be used as 'tech wash' or as a substitute for robustly enforced design standards.'[19]

We recommend that the regulator sets out a framework for what children should be taught and made aware of, and that education material or public awareness material provided by companies that also offer commercial services to children are subject to oversight.

The White Paper also notes that companies have 'created tools to empower their users, such as software from Apple and Google that produces reports for users that help them to assess and control their online activity'. Again, while there is a role for these tools, they must not obscure or dampen the need for regulation. Indeed, Google's 'Digital Wellbeing Tool', Instagram's 'Your Activity' tool, and others do not address the design features of various services that cause children to lose control of their digital usage in the first place. Providing users with tools to monitor their use, while at the same time deploying extended use strategies, is plainly an attempt to play both arsonist and firefighter. The regulator must be resilient to claims that companies can fulfil their duty of care through these tools alone, as opposed to ensuring that their services are better and age-appropriate by design.

We recommend that data literacy be a compulsory part of a child's education, whatever the status of the school that they attend.

Finally, we have said previously that 'public awareness/education is needed to counter the volume of unethical and unbalanced media reporting. Disasters make powerful headlines, but at the same time, there is little coverage of the impacts of digital footprints, data regimes, targeting and the sheer volume of information gathered and shared or the amount of interaction demanded – with the corresponding impact on user choice and opportunity. This is particularly true of guidance relating to children, who are over associated with a narrow set of online harms and little considered when discussing, data, privacy, fake news, hacking, AI ethics, security and cybercrime.'

We recommend that Government offers a clear set of messages that are sophisticated, broad, non-hysterical and which signpost to its own resources.

For further comment or information please contact Jay Harman on 020 7502 3818 or jay@5rightsfoundation.com.

[18] Our Digital Rights, 5Rights Young Scot, May 2017; The Internet on our Own Terms, University of Leeds, University of Nottingham, 5Rights, January 2017

[19] The Right to Tech Competency – A Framework for 8-13 Year Olds, BT, EdComs, October 2017