The Information Commissioner's response to the Department for Digital, Culture, Media & Sport consultation on the Online Harms White Paper

Summary

- The impact of online harms is an issue of significant public concern. It is essential that we have regulation that makes a real difference, but also remains proportionate so that people are able to continue to enjoy the real benefits of the internet.
- How to regulate harms on the internet is one of the most complex and challenging issues of our times. It requires innovative solutions and an approach that ensures we can continue to balance competing rights in a democratic society.
- It is essential that the full breadth of internet harms are considered in the round, both at an individual and societal level. This includes electoral interference and greater transparency in online advertising.
- Data protection regulation needs to be seen as part of the wider ecosystem of regulating the internet and should not be positioned separately. It is the personalisation of data that is driving the delivery of content online.
- Given the need to act swiftly, it makes sense for an existing regulator who already has experience of content regulation to take on the new regulatory role outlined in the White Paper.
- This should be accompanied by a strategic coordinated approach to regulation – chaired by the regulator with responsibility for online harms but involving all the key regulators in the space of internet regulation.
- The proposed duty of care is an important part of the solution – but it is not a quick solution and will need to be backed by appropriate sanctions and powers.

Introduction

As Information Commissioner I have responsibility for promoting and enforcing the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Privacy and Electronic Regulations 2003 (PECR) and the

Environmental Information Regulations 2004 (EUR). I am independent of Government and uphold information rights in the public interest, promoting transparency and accountability by public bodies and organisations and protecting individuals' privacy and information access rights.

I welcome the opportunity to respond in detail to the Government's Online Harms White Paper (White Paper). As the regulator that operates across the online tech ecosystem, I am able to bring a unique perspective on the experience of regulating the big tech giants using the GDPR and new enforcement powers that have been updated for the digital age.

Our response is divided into a number of key headings, which aim to cover the broad spectrum of issues detailed in the White Paper, including the 18 specific questions set out in Annex A. This builds on the paper I submitted to the DCMS Select Committee in May.

The White Paper is a serious intervention in a global debate about how to protect individuals and society from online harms. The UK Government is the first of any major country to set out a route map for regulating the content and conduct generated by tech companies that make up the internet.

Its proposals reflect people's growing mistrust of social media and online services. While we can all benefit from these services, we are also increasingly questioning how much control we have over what we see and how the information is used. This is reflected in my office's engagement with the public, where there is increasing anxiety around people's experience of the online world, and a deterioration in the trust they place in large technology companies to protect them, their family and friends.

Developing solutions in this area is very challenging – enabling the protection of individuals against online harms and at the same time upholding freedom of expression and other fundamental rights. But it is clearly an urgent and critical issue. For many people their online experience has given them (at least) some moments of distress (as found in the Ofcom/ICO research into internet users experience of online harms[1]), and risks deterring them from engaging in the many benefits of the online world.

It is of course ultimately a matter for Government and Parliament to decide the nature and shape of the regulatory landscape in this area. The White Paper has identified an important gap in the existing regulation of the internet – namely harmful online content.

[1] https://ico.org.uk/about-the-ico/research-and-reports/internet-users-experience-of-harm-online-ofcom-and-the-ico/

However, the White Paper does not include a detailed analysis of what is already regulated in the online world and the bodies that are responsible for that regulation in the UK. In particular, the paper currently views the different regulatory frameworks separately and does not contain an analysis of how these frameworks knit together – for example, data protection, electoral and competition law – and how this relates to or overlaps with the identified gap in the White Paper of the regulation of harmful content online.

It is essential that the policy focus should be on addressing the significant and growing gaps in internet regulation that carry the risk of harm, particularly to vulnerable groups. But it is important that in doing this, we don't view regulation of this area in isolation of existing regulatory frameworks or other online harms.

I therefore remain surprised and disappointed at the lack of engagement within the White Paper with the societal harm of electoral interference and the need for greater transparency in online political advertising and micro targeting. If left un-addressed, this risks undermining the fabric of our democracy. I therefore welcome the Government's commitment to launch a consultation on electoral integrity that I understand will include consideration of recommendations for increasing transparency on digital political advertising. I look forward to contributing to this process.

The current online harms regulatory landscape and the role of data protection regulation

The evolution of the internet over the last 30 years suggests it is not possible to see it in isolation of existing regulatory frameworks. My view is that the development of society's approach to internet regulation can be seen in broadly four stages:

- At the outset many in society took the view that the internet would be largely self-regulatory and would act as a forum for freedom of expression.
- This was followed by an approach of applying analogue solutions to the problems of the internet.
- We then began treating the internet as a single non-analogue entity, rather than a complex set of networks.
- Society has now arrived at a position of better understanding the complex interactions online between individuals and online services. The internet provides many benefits, but given the anonymity and freedom it provides, sometimes amplifies offline harms, and sometimes creates new harms. This requires complex solutions, in which the internet consistently and proportionately falls within the

scope of regulation, and regulation is supported by other measures to support society's evolving engagement with the online world.

In respect of my own area of regulatory responsibility, the White Paper rightly identifies data protection regulation as an area of the law that has already been updated and modernised for the digital age, with the implementation of the GDPR in May 2018. But whilst this is an area of internet regulation that requires little attention in terms of modernisation, it is too simplistic to completely separate data protection from the consideration of regulation of harmful content online, as it is personalisation and targeting (using and inferring personal data) that is driving the delivery of content. And it is the GDPR and the DPA18 that governs the use of personal data and algorithms in the delivery of content online, which includes the UK's world leading 'Age Appropriate Design Code'.

The use of personal data is an integral part of many of the harms outlined in the White Paper. For example, in the case of self-harm content, children and young people are being directed to these sites through nudges built on information drawn from personal data relating to previous behaviour online. Profiling and cross device tracking are now fundamental to the internet platforms' business models.

In addition, there are a number of other areas where there is already a clear regulatory mandate with regard to aspects of internet regulation:

- Ofcom covers the broadcast of content from TV that is played over the internet 'on demand', and licenses linear TV channels that are delivered over the internet.
- The Advertising Standards Authority (ASA) covers standards of advertising on the internet (but not political advertising).
- The Competition and Markets Authority (CMA) promotes competition for the benefits of consumers, including conducting market studies and investigations in markets where there may be competition and consumer problems.
- The Electoral Commission oversees the conduct of elections and in particular regulates electoral spending, including that spent on digital advertising.
- Many of the internet harms that rightly concern the public are already clearly illegal, such as the distribution of terrorist content or child pornography, or making threats to kill.

Regulators are already working together in relation to big tech and the internet, both in terms of joint initiatives and the sharing of intelligence

for investigations. Examples of this include a trilateral programme of work between the ICO, Ofcom and the CMA, and initiatives co-ordinated through the UK Regulators Network, of which the ICO is a member. I provide more detail about future collaboration under the proposal for an online harms regulator below.

Learning that can be drawn from data protection legislation

Addressing questions Q1, Q2, Q2(a) Q3, Q15, and Q16.

The White Paper draws on the experience and concepts in the GDPR and broader data protection regulation to inform the proposed new regulatory framework for the regulation of harmful content online.

The GDPR is still only one year old and our understanding of the effectiveness of some of its new principles and measures, and our powers to enforce it, will become clearer over time. For example, the obligation on non-EU entities in the GDPR to appoint an EEA representative, if offering online services into the EU, has not been fully explored or tested during the first year of the GDPR, which makes it difficult for us to comment on the merits of similar proposals in the White Paper. However, there are a number of concepts and provisions within data protection legislation that can be used in tandem with, and applied to, the regulation of harmful content online.

It is important to note that as principle based legislation, the data protection regulatory framework has been able to adapt to developments in technology. The Data Protection Act 1998 (EU 1995 Directive), although drafted before the digital economy established itself, was able to in large part successfully adapt to the rapid growth in the digital economy. The GDPR/DPA18 – also principle based - provides an important upgrade for the digital age.

Accountability and Fairness

The accountability and fairness principles in the GDPR have begun to change the culture of organisations by making data protection a boardroom issue. Concepts such as data protection by design, data protection impact assessments, the public's right to know, algorithmic auditing (the DPA18 rather than the GDPR), codes of conduct and certification mean that innovation and privacy now need to go hand in hand.

The Centre for Information Policy Leadership, in its 'GDPR One Year In' report[2], makes a number of observations about how the GDPR has improved organisations' data accountability and transparency arrangements. This includes making data protection a board level issue, resulting in greater awareness of and tackling of privacy issues at this level; enabling organisations to position privacy compliance as a business enabler; unlocking the potential for organisations to benefit from wider responsible data uses and data driven innovation; increasing uptake of comprehensive privacy management programmes; and driving more efficiencies at the organisational level and more effective and better protection for individuals and their data, thus increasing trust in how organisations handle data in a digital age.

Whilst this applies to data protection regulation, sound accountability and transparency mechanisms are transferable into the area of content and conduct regulation. The large tech firms have already had to make changes to their business models to comply with the requirements of the GDPR. It therefore makes sense to expand these into the area of harmful content online regulation to reduce the regulatory burden of organisations having to comply with two completely separate regimes – providing a key bridge between the two regulatory regimes.

An accountability model at the core of online harms regulation will also provide scalability, proportionality and flexibility. This is important as scalability will be a particular challenge for the new regulator operating in this space.

Given this experience we are very supportive of the proposed improvements to transparency reporting in the White Paper. We are also supportive of the proposal to enable designated bodies to bring 'super complaints' to the regulator. There are parallels with the redress mechanism under Article 80 of the GDPR which the ICO views as an important mechanism for enabling data subjects to exercise their privacy rights.

Sanctions and Enforcement Powers

The GDPR and DPA18 have provided us with a range of modern powers and sanctions essential for carrying out complex investigations in a digital age, which will often cross multiple jurisdictions and where the regulator needs to act swiftly to seize and protect evidence. These include no notice Assessment Notices and the power to issue 'urgent' information notices.

[2] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_report_on_gdpr_one_year_in_-_practitioners_take_stock_of_the_benefits_and_challenges.pdf

The ICO exists to uphold individual rights in the digital age. To do this we act as an educator, ombudsman and enforcer – supporting businesses to comply with the law and enabling individuals to access their information rights. It is essential for a modern regulator to have a range of tools in its toolbox. The ICO is independent of Government and is accountable to Parliament for the exercise of is functions. This is underpinned by our Regulatory Action Policy that provides transparency in how we exercise our powers. We think this offers a useful model to consider when looking at the accountability of the proposed new regulator described in the White Paper.

Definition of Private Communications

As the White Paper rightly suggests, there are significant challenges in defining what is a private communication. Article 2.2c of the GDPR – which exempts from the regulation processing of personal *data by a natural person in the course of a purely personal or household activity* - could be useful here. Although not strictly transferable from data protection regulation to online harms regulation, it may offer a basis for drawing a distinction between private messaging and public broadcasting (although it is not straightforward defining the line between the two) given that the technologies used for these two types of activities are effectively on a sliding scale so cannot be distinguished just by regulating the technologies differently.

The ICO's experience of regulating Big Tech

Addressing questions Q4, Q6, Q7, Q7(a), Q8, Q9, Q17, and Q18.

This paper has already outlined the role data protection plays in the regulation of the delivery of content online. The selection and provision of online content is often personalised using a personal data profile. This horizontal remit means that when the regulation of the internet involves personal data, we have a role to play. We have well established engagement with the tech firms such as Facebook (including WhatsApp and Instagram), Google and Twitter, and have undertaken actions against Facebook, WhatsApp and Google in recent years. The new enhanced powers and sanctions in the GDPR and DPA, including extraterritorial powers, mean that we will be able to continue to hold the tech firms to account for how they are handling citizens' data online.

Specific examples include:

- The Facebook/Cambridge Analytica investigation into the use of data analytics in political campaigns, that resulted in Facebook

receiving a maximum fine of £500,000 for breaches of the Data Protection Act 1998.

- An investigation into the sharing of user data by Whatsapp with Facebook, following Facebook's acquisition of the company, that resulted in Whatsapp signing an undertaking in March 2018 not to share data until data protection concerns were addressed.
- A current investigation into the operation of the Tik Tok app; in particular how it obtains and uses the personal data of children. This follows concerns by a number of regulators, including the Federal Trade Commission, who have fined the company for violations of US laws protecting children on line. We will be examining how the app meets the GDPR requirements for better protections of children's personal data.

We also have relevant experience in relation to Google (and other search engines) and the original 'Right to be Forgotten' principle, following the European Court of Justice judgment against Google Spain[3]. Under this mechanism, individuals make the initial request to Google for search engine results to be delisted. If the individual is not satisfied with the outcome of this request, they can complain to the ICO for adjudication, which involves exercising a careful balance between the rights to freedom of expression and privacy. The ICO has dealt with approximately 600 cases to date.

Furthermore the ICO is pursuing its Innovation Agenda, in which we are witnessing a vibrant and evolving market for privacy enhancing technologies in data processing that are both GDPR compliant and privacy respectful. An example of this is the ICO's Regulatory Sandbox, which will proactively support organisations to develop innovative products and services that make use of personal data and that benefit the public. It will do so in a way that is focussed on both achieving compliance and supporting these developments coming to fruition – and so avoiding them becoming problems which require investigation and enforcement later in their development.

Another example, is our approach to algorithmic auditing. We are creating a methodology to audit AI applications and ensure that the necessary measures to assess and manage data protection risks arising from them are in place. This will also inform future guidance for organisations developing AI. We're consulting a wide range of organisations and roles, including data protection officers, data scientists, AI engineers, and

[3] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González case, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

stakeholders, to understand AI-related risk areas such as fairness, accuracy, and security.

The ICO's Age Appropriate Design Code is also an important tool for tackling online harms. It sets out world leading standards expected of those responsible for designing, developing or providing online services likely to be accessed by children, when they process their personal data. It implements the intention of GDPR to provide special protections for children and will be backed by existing data protection laws, which are enforceable by the ICO using the full raft of our powers, including fines of up to 4% of global turnover. This has the express support of Government and Parliament and, subject to the statutory timetable, will be in force before the end of 2019.

Whilst the above highlights the ICO's clear role in the regulation of content delivery online, there are clear limits to data protection regulation in this space. It is important to distinguish between the regulation of the delivery of content online (through data analytics and algorithms) where data protection is front and centre, and the online harms in scope of the White Paper. Preventing many of the latter harms involves elements of tracking and surveillance that create tensions with the ICO's role of protecting privacy. The scope of the regulation proposed in the White Paper is quite broad. We will therefore continue to have a strong interest in how the aims of the White Paper are fulfilled during the development and drafting of the legislation, particularly where there is likely to be a tension between how an individual's activities may be monitored and addressed, and the rights and freedoms of that individual.

Finally, there are many challenges around the delivery of digital literacy. There are a number of initiatives to address aspects of digital literacy, but current work is disparate and does not appear to be fully 'cutting through' to the wider population. There may be a role for Government, or a body such as the Centre for Data Ethics and Innovation, to coordinate existing efforts to ensure coherence and avoid duplication.

Proposals for an online harms regulator

Addressing questions Q10, Q10(a),Q11,Q12, Q13, and Q14.

As previously stated, there is a growing sense of urgency across government, civil society, industry and regulators to plug the gap of regulation of harmful content online. In order to take this forward quickly, it seems sensible for the regulation of harmful content online to be taken on by an existing regulator who already has experience in this area. This aligns with some elements of Ofcom's existing mandate and it is appropriate that Ofcom is named in the White Paper as a candidate for

this role. However the White Paper only discusses Ofcom taking this role on an interim basis - we believe an interim approach would be difficult to execute in practice, and unnecessary given the capabilities of Ofcom and its ability to develop capacity to support this work permanently. The regulator would need to continue to work collaboratively with other regulators in this space, including the ICO, the CMA, the Electoral Commission and the Financial Conduct Authority.

We would also support the view given in recent evidence to the DCMS Select Committee by the Chief Executive of Ofcom, Sharon White, in which she explained that given the sheer volume any new regulator could not be expected to handle first line complaints (and acknowledged in the White Paper). They would be dealt with by the in-scope platforms themselves and the new regulator would focus solely on the systems and controls each platform put in place to manage such complaints and remove harmful content. In addition, the presence of an industry ombudsman for those complaints that could not be satisfactorily dealt with between the user and the platform, such as those in telecoms that Ofcom already work with.

This could be an industry funded arbitrator that sits between the platforms. This couldn't be a form of self-regulation but would need to have a statutory underpinning to guarantee its independence. However to meet public expectation the regulator might need own motion powers to act on specific issues when public concern is very great.

However, for any new model of regulation to be successful it is essential that all regulators operating in the space of internet regulation have comparative powers and sanctions to those provided to the ICO in the GDPR, including the power to compel information, carry out non-consensual audits, take cross-jurisdictional action and the ability to issue substantial fines.

It is also essential for public trust and confidence in any regulatory regime that the regulators themselves are able to carry out their statutory duties independently of government. Government and Parliament set the statutory framework, but the regulator operates independently within those boundaries. I therefore think clarification needs to be given to the proposal around codes of practices for terrorism and CSEA online. It is absolutely right that companies should take robust action to tackle terrorist and extremist action online and that the regulator responsible for content and conduct moderation would have role in overseeing this – but the public must have confidence that the regulator is operating independently of government when making regulatory decisions in relation to these cases.

Strategic coordinated approach to regulation of the digital economy, including online harms

Another solution would be a strategic coordinated approach to regulation of the digital economy, including online harms. This approach would assign responsibility for online content regulation (to fill the gap – as above) but would also bring relevant existing regulators together on a formal footing, and create a joined up approach to the full breadth of internet regulation.

As complaints are likely to be multifaceted in this space and involve more than one regulator, we would recommend that this approach be underpinned by a statutory gateway to enable regulators to conduct joint investigations where appropriate. A model for this would be The Regulatory Reform (Collaboration etc between Ombudsmen) Order 2007[4]; which allows the Local Government and Social Care Ombudsman, and the Parliamentary and Health Service Ombudsman, to work together if a complaint covers both jurisdictions. The benefits of this approach include efficiency gains as a single investigator would look at the case and provide a quicker more focused investigation, access to shared intelligence; and the organisation(s) being investigated only having to deal with a single contact point.

The Committee/Body could be chaired by the regulator with responsibility for online harms regulation. All regulators in this space would maintain their clear independence from each other which would define the boundaries on which the proposed cooperation would be structured.

This would be preferable to a single or 'super' digital regulator, which as well as taking considerable time to establish and being extremely costly, would inevitably be victim to a number of conflicts within its huge range of overlapping regulatory remits, not least the inherent tension between freedom of expression and privacy. We favour the model described above as it clearly requires and empowers regulators to work together in a coherent and targeted manner when addressing undisputed online harms - being able to pool technical expertise and infrastructure and designate a lead authority to investigate but still retaining their all-important independence when societal and public interest clearly call for them to do so.

[4] https://www.legislation.gov.uk/uksi/2007/1889/contents/made

The proposed Duty of Care

Addressing questions Q4, Q6, Q7, and Q7a.

The ICO welcomes the proposal for a Duty of Care in the White Paper. It is a valuable addition to the debate and a useful way of applying general obligations on platforms. The concept of a Duty of Care appears aligned with the accountability duty in the GDPR and many of the benefits outlined earlier in this paper – in respect of greater awareness at board level, greater transparency and accountability programs – could be realised in this context too.

However, the Duty of Care on its own may not be a sufficient framework for achieving the White Paper's aims. The White Paper notes the increased urgency in which the public expect this issue to be tackled. However we know from other sectors where a Duty of Care has been introduced – for example in the environmental sector – it takes time to implement and then develop case law. In addition, previous examples of applying a Duty of Care are all from the physical world, and time will therefore need to be taken to ensure it translates effectively into the online world.

On this basis the Duty of Care wouldn't have an immediate impact by itself. To address public anxiety we need visible and immediate action, with some rules that the public can readily understand, and in particular specific regulation with effective sanctions for the regulator, so that the public can see that swift action will be taken if platforms breach the rules. The Codes of Practice mechanism envisaged in the White Paper will help here, by setting out in a transparent way what is expected of the platforms.

However, it is our view that the Codes of Practice must be, and must be seen to be, independent of Government. The named statutory Codes of Practice in Sections 121-125 of the DPA18 offer a good model for this. The power to develop the Codes is given to the Information Commissioner by Government and Parliament but the Codes are drafted and enforced independently of Government with the Information Commissioner accounting to Parliament in how she does this.

The scope of the Duty of Care and how it applies to private messaging will need careful consideration, including a clearer explanation in law. As the White Paper rightly points out, there are many potential definitions for private communications online, involving a number of different channels and forums. It is essential that we get the balance right between protecting and respecting individuals' privacy in their personal communications, and developing a proportionate, transparent and accountable approach to identifying when the nature of a particular

messaging channel changes the status of some of its communications from being 'private' to 'public'.

The Investigatory Powers Act 2016 already contains provisions to enable the lawful interception and obtaining of communication data. The checks and balances in this Act reflect the importance of supporting the ability of the vast majority of people to enjoy private and secure communications in their everyday life. However, there is a difference between accessing the content of encrypted end to end messages which is covered by the IPA 2016 and closed private groups on Facebook for example. In the latter this might be about ensuring the right algorithms are assessing the content – but this does need further clarification. This is a very complex and challenging area to get right, but there is a potential risk to trust and confidence if measures to address online harms were perceived to compromise the privacy of private communications.

Conclusion

In conclusion, the White Paper demonstrates that the UK is at the forefront of this timely debate. This is one of the most complex and challenging issues of our times – requiring innovative solutions and an approach that ensures we can continuing to balance competing rights in a democratic society.

We believe that the urgency in needing to address public concern means that it makes sense for an existing regulator already operating in the area of content moderation to take on the role of regulating harmful content online.

The ICO as the regulator for the delivery of content online when that involves personal data, will continue to play a significant role in this space. But the conflicts that we highlighted between the ICO's existing remit and the level of surveillance that is necessary to effectively regulate content online means that would shouldn't be the regulator to take on a role with such additional breadth.

Our submission highlights a number of relevant areas where the ICO is already acting to tackle online harms – for example, the Children's Code, collaboration with other regulators, and working with organisations to develop compliant innovative technological solutions – and we will continue to seek out other ways within our statutory remit.

The duty of care is an important proposal and one which we would wish to support the Government in developing further thinking on. However, this is not a quick solution and will need to be backed up by appropriate sanctions and powers.

The ICO is committed to continuing to support the Government and fellow regulators in developing solutions to the issue of online harms and we look forward to engaging further on a number of the issues we have highlighted.

Elizabeth Denham
Information Commissioner

1 July 2019