doteveryone

Regulating for Responsible Technology: Making the case for an Independent Internet Regulator

A Doteveryone Green Paper

25th May 2018

This report was written by Doteveryone's Jacob Ohrvik-Stott and Catherine Miller. We are grateful to the following people for their contribution to this research:

- Harry Armstrong, Nesta
- Bill Batchelor, Baker Mckenzie
- Corinne Cath, Oxford Internet Institute
- Alina Dimofte, Google
- Jack Hardinges, Open Data Institute
- Mallory Knodel, Article 19
- Professor Daithí Mac Síthigh, Queen's University Belfast
- Imogen Parker, The Nuffield Foundation
- William Perrin
- Dr Nick Srnicek, King's College London
- Robbie Stamp, Bioss
- Dr Jack Stilgoe, University College London
- Steve Wood, Information Commissioner's Office

Contents Page

Executive Summary

Society is at a critical moment in its relationship with the internet. Digital technologies are changing the world at a speed never seen before, in ways no-one could have imagined.

Doteveryone is seizing the urgency of this moment to advocate for a digital future founded on technology that recognises its responsibility to society. We're championing technology that understands, minimises and mitigates its social consequences.

The current system of regulation in the UK is not equipped to deliver this future. Our research into the public's digital attitudes and understanding has shown people are concerned about the impacts of the internet on society, feel disempowered in the face of technologies and have a strong appetite for greater accountability from private and public sector organisations that create and use digital technologies[1][2].

In our *People, Power and Technology* report we called for independent regulation and accountability, so standards are upheld and people know who to turn to when things go wrong. This paper develops that idea further and makes the case for a new regulatory body, that understands the complexities of the internet and can develop new thinking for regulating in a fast-moving digital world.

In April 2018 we spoke to individuals and organisations from across the technology and regulation landscape to sketch out a vision for how this body might work. This paper brings together these conversations, and other research, and identifies the issues the need to be addressed to improve the regulation of internet technologies.

The current problems we identify are:

- Regulators adopt a reactive approach to digital issues, which can mean accountability comes too late and is harder to enforce.
- Regulation focuses on outcomes, which means the processes and design of technology are under-scrutinised.
- There's a tendency to focus on individual rights and issues such as safety, data use and security which crowds out concern for social impacts, such as technology addiction and algorithmic discrimination.

We are calling for an independent regulator that will champion new digital social contracts and uphold common standards across government, big tech and emerging technologies. But accountability cannot be achieved by a single regulator alone. This

[1] http://understanding.doteveryone.org.uk/
[2] http://attitudes.doteveryone.org.uk/

body must bring together the tech sector, civil society, government and the public to create a system that is flexible and centred around shared human values.

Key roles for an independent body include:

- Building up regulators' digital capabilities to match the tech sector so they can scrutinise the underlying technical structures of digital technologies; for instance auditing design processes, conducting independent impact assessments at an early stage of a technology's lifecycle and developing industry standards for responsible design.
- Developing a collective long-term vision for an internet that works for the good of society, through deep public consultations and collaboration between industry and the public sector. This includes understanding the ethical implications of digital technologies but rooting them in a real-world environment.
- Expanding horizon scanning and foresight activities to identify emerging digital challenges and conduct studies to develop an evidence-base around social impacts.
- Strengthening collaboration between regulators on technological challenges that cross over traditional sector boundaries.
- Empowering the public to understand the impacts of digital technologies so people can make use of regulation.
- Developing mechanisms for consumers, citizens, creators and civil society to seek redress for issues that fall in the gaps between existing regulatory mechanisms.

Introduction

Digital technologies are shaping every part of our lives, our economy, democracy and society at vertiginous speed and the UK's regulatory system has struggled to keep pace.

The findings of our People, Power and Technology survey show the need for greater accountability from government and from the companies that create and use them. Public mistrust of technology companies is high, with 43% saying there is no point reading terms and conditions because companies do what they want anyway. Two-thirds of respondents feel that government should be responsible for ensuring digital companies treat their customers, staff and society fairly, but only 36% agree that government is currently able to address the problems they have with the internet.

While people continue to get great personal benefit from online technologies, they are concerned about their societal impacts. Half of survey respondents felt the internet made their lives a lot better, only 12% felt it had a very positive impact on society. As social harms, from democracy hacking to technology addiction, grow in complexity and scale, action is needed now to address them. As the meagre resources with which the Information Commissioner's Office is attempting to tackle the Facebook-Cambridge Analytica scandal demonstrate, the current blend of ad hoc interventions and industry self-regulation is unable to cope with these challenges.

Regulation is an important lever for change but it is only one part of a wider ecosystem. Industry, civil society, tech users, workers and the public must all play a part in fostering responsible technology that benefits everyone in society.

Doteveryone sees a need for a new body to bring these groups together; that understands the complexities of the internet and can develop new thinking for regulating in a fast-moving digital world. For true accountability this body must be independent: as data sharing and automated decision-making in public services becomes the norm, government must be subject to the same scrutiny as industry. In this context we see regulation not simply as a set of rules but as a system to bring about new digital norms, ranging from legislation to governance of the practices and culture of digital organisations.

In April 2018 we spoke to individuals and organisations from across the technology and regulation landscape to imagine how this new approach could work. This Paper brings together those discussions to outline the challenges currently facing digital regulation in the UK and sketch out a vision for a new regulatory body to address them. This paper is the start of a conversation, and in June 2018 we will be consulting further on how to make this vision a reality.

We first describe the existing regulatory landscape, showing how a patchwork of regulatory bodies and legislation covering aspects of digital technologies has built up.

We then discuss where regulatory gaps lie, highlighting areas which lack oversight, the lack of capacity of existing regulators as well as the lack of awareness in how to use these mechanisms.

We explore what regulatory principles and frameworks might be required to underpin successful internet regulation, looking beyond the narrow focus of the debate on content regulation to a wider scope of accountability. Finally we consider how a forward-looking approach that is able to keep up with the pace of digital change can be adopted by regulators.

Internet regulation in the UK - the current landscape

There are currently a number of regulators with remits which touch on digital technologies. In our consultation, contributors stressed the need to consider where a new regulator might sit in the large ecosystem of other regulators.

"there are already a number of organisations in this space, whether existing regulatory bodies or others in the process of being established to address some of the ethical issues surrounding new technology. Establishing a new regulatory body with a broad remit is no small task and will not be completed quickly." (The Corsham Institute)

In the UK the following regulators are explicitly focused on the internet and digital technologies:

- Ofcom – Independent regulatory body established by the Office of Communications Act (2002) to regulate communications industries in the UK, with the principle duty of *"furthering the interests of citizens and of consumers, where appropriate by promoting competition"*[3]. Ofcom's online mandate is relatively limited, and primarily focuses on the distribution, use and consumption of online media content.
- Information Commissioner's Office (ICO) - Independent regulator *"upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* covering both public and private sectors[4]. Operates a public register of all organisations in the UK processing personal data and enforces compliance with UK data regulation, from requesting information through to the issuing compulsory penalties. With the EU's General Data Protection Regulation (GDPR) coming into force, the ICO's power to fine will increase to £17 million, or 4% of an organisations global turnover.

Many other regulators' remits extend into the digital economy, including the Competition and Markets Authority (CMA), Payment Systems Regulator and the Financial Conduct Authority (FCA), with the FCA addressing specific issues such as digital fundraising and crowdsourcing and cyber resilience for financial information systems.

In the democratic space the Electoral Commission regulates digital and online campaigns, and primarily focuses on enforcing current spending rules and limits. Following the 2017 election the Commission called for changes to improve their scrutiny of digital political campaigns, including increased transparency of online advertising

[3] http://www.legislation.gov.uk/ukpga/2003/21/section/3
[4] https://fetview.com/2014/01/15/registration-ico-uk-data-protection-act/

spending and regulation requiring digital ads to be labelled with which political group has funded them[5].

The industry-funded Advertising Standards Agency (ASA) regulates quality standards for online digital advertising, covering websites, paid-for search engines and other digital platforms, but the statutory powers it has over TV and Radio ads don't extend to the online space. This means that they cannot force marketers to remove non-compliant material from websites - organisations that don't co-operate are instead named and shamed on the ASA website[6].

The Independent Press Standards Organisation (IPSO) regulates around 1,000 digital titles and mediates public complaints about online materials[7]. Although they have recently announced the development of IPSO mark for online content that meets the standards of their editors' code[8], their practices only cover member organisations, not the wider online media sector.

Other non-regulatory bodies focus on online safety and security. The UK Council for Child Internet Safety and UK Safer Internet Centre are two networks working to improve child safety on the internet, whilst the not-for-profit Internet Watch Foundation polices child sexual abuse content. GCHQ's National Cyber Security Centre provides independent guidance on managing cyber security threats to industry and government departments.

Underpinning all of these bodies is legislation. The new Data Protection bill, which incorporates the the EU General Data Protection Regulation (GDPR) has recently been brought into UK law. GDPR retains existing personal data rights around accessing, objecting and erasing data and querying certain automated decision making and introduces new rights to erasure, restriction of processing and data portability[9]. The Electronic Commerce Regulations (2002) provide protections for consumers, platforms and businesses in online marketplaces, and exempts 'intermediary platforms' such as search engines from liability for online transactions. Others such as the Communications Act 2003 and Digital Economy Act 2017 cover the operations of internet service providers and telecommunications infrastructure.

While this landscape has evolved over time to cover aspects of digital technologies, it is clear that the current system of regulation is fragmented and fails to create effective oversight in a digital age.

---

[5]https://www.electoralcommission.org.uk/__data/assets/pdf_file/0004/237550/Political-finance-regulation-at-the-June-2017-UK-general-election-PDF.pdf
[6] https://www.asa.org.uk/codes-and-rulings/non-compliant-online-advertisers.html
[7] https://www.ipso.co.uk/about-ipso/who-ipso-regulates/
[8]https://www.ipso.co.uk/news-press-releases/press-releases/regulator-announces-new-ipso-mark-for-its-2-500-publications/
[9]https://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-4-souped-up-individual-rights

Gaps in the UK's digital regulation

The patchwork of regulation and legislation described above results in an inconsistent and fragmented system and leads to some significant gaps in ensuring comprehensive oversight and accountability. In addition, there is a marked lack of capacity within existing regulators to address the new issues posed by digital technologies and a slow and reactive approach to them. The effectiveness of regulation is also undermined by the failure to consider the wider, social harms of technology and by a disempowered public which is not able to exploit the regulation which exists.

There are grey areas between regulators and sectors which allows some practices to evade scrutiny. For example, targeted advertising based on people's personal information sits across the remit of both the ASA and ICO, yet neither are currently looking at the issue directly.

The nature of technologies also allows some to slip between different oversight mechanisms. This is most notable in the debate around whether platforms should legally be considered as publishers. The European Commission has noted that current E-commerce legislation *"was designed at a time when online platforms did not have the characteristics and scale they have today"*[10]. However the problem of definition should not be overstated - Ofcom for example has publicly recognised platforms as media companies[11], and yet it has still been reluctant to regulate in this space[12].

Regulatory capacity

Even where technologies are subject to regulation, existing regulators are struggling to modernise and face major gaps in their knowledge and capacity.

Despite the ICO's increased powers, many contributors to the consultation expressed doubts about its ability to keep pace with technology. The Information Commissioner has stressed she needs significant staff numbers who are paid salaries appropriate to their expertise to be able to work effectively[13]. Cambridge Analytica whistleblower Christopher Wylie echoed these concerns to the Digital, Culture, Media and Sport Committee: *"One of the weak points of the ICO is the lack of technical people. The fact is, they've had to ask me a lot of questions that a database engineer would not ask".*

[10]https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe
[11]https://www.thetimes.co.uk/article/ofcom-boss-dame-patricia-hodgson-google-and-facebook-are-publishers-3hkrcmq58
[12]http://blogs.lse.ac.uk/mediapolicyproject/2017/09/29/why-regulators-like-ofcom-are-dropping-the-ball-on-fake-news-dark-advertising-and-extremism/
[13] https://www.ft.com/content/01641ac6-9081-11e7-a9e6-11d2f0ebb7f0

The spread of Internet of Things (IoT) technologies through a vast range of previously analogue sectors, from household items to cars exacerbates this issue, bringing a range of complex security and data issues onto the radar of regulators with no experience of these issues.

Finally, many regulators prove ineffective due to their reactive approach - for example, the Electoral Commission's reports into election financing which come weeks after an election's conclusion, with the outcomes already decided.

Many contributors to the consultation said competition regulators were particularly slow to respond to a changing environment.

"Anti-trust and competition laws can be leveraged better and more regularly... Regulators typically don't understand how a technology works. They have a hammer and everything else is a nail." (Corinne Cath, Oxford Internet Institute)

Catching up with technology: A digital consumer market case study

The Competition and Markets Authority provides a useful illustration of how regulators are struggling to address the needs of a digital world. The CMA is the primary regulator for many online consumer markets. Post-Brexit the Authority is likely to take a more prominent role in the regulation of multinationals operating in the UK.

Traditional competition regulation has largely focused on the relationship between competition and consumer prices. Wider societal impacts have been a secondary concern[14]. As large technology companies change the fundamental structures of the market, this approach seems unable to maintain the balance of power between industry, consumers and the state, posing several challenges to the CMA:

The changing role of 'price'. Digital technologies have disrupted the traditional concept of price. Many platforms offer free-to-use services in exchange for users' data, making the notion of consumer price as an indicator of the health of a market redundant. Platforms that sell products and service may also deploy variable pricing and it can be hard to gauge where this practice is fair and where it's discriminatory. And on marketplace platforms, connecting buyers and sellers, regulators must ensure both sides receive a fair price.

The increasing influence of network effects. Many tech companies are loss-making until they reach a critical mass of users. After this point network effects (where the value of a service to a user increases as more users join) often mean a platform can quickly become dominant in a short period of time[15]. Focusing on profitability can

[14]https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Practical_competition_policy_tools_for_digital_platforms.pdf
[15] ibid

mean a regulator only intervenes after companies gain market dominance - at which point effective regulation becomes harder[16].

Blurring of traditional market boundaries. Some technology companies operate across multiple markets that historically had limited influence on each other (eg Amazon purchasing Whole Foods Market). With many sectors yet to be fully digitalised, large tech companies could gain an unfair advantage in emerging online markets[17]. Some companies may also cross subsidise services, selling a service or product at a loss to generate data that is valuable in other markets, as is the case with the Amazon Echo device[18]. The effects of combining data across different markets on competition and consumer welfare, are not yet clear.

Assessing collusion in automated environments. Traditional cartel laws make it illegal for companies to agree to limit competition or fix prices. Pricing algorithms are difficult to understand, making it hard to determine if companies have knowingly colluded.

Digital mergers and acquisitions. It's common for large digital companies to acquire smaller, innovative start-ups[19]. Historically regulators considered the combined market power of mergers but it is now tricky to determine where digital organisations are acquiring potential future rivals, and whether that amounts to weakening competition.

The CMA is reacting to these challenges, with a new data unit in the pipeline to look at the role of digital technology in consumer markets[20] and a consultation exploring modern consumer markets underway. But these initiatives come when the digital economy is already mature and the market capitalisation of technology companies exceeds all other sectors globally[21], indicating how slowly regulators are responding to technological disruption.

Addressing social harms

While many regulators and government bodies in the UK focus on the protection of individuals, less attention is given to the impacts digital technologies are having on society as a whole, for example the effects of algorithmic bias or the impact of social media on mental health. Broader social impacts, including the impact of technology on inequality and digital device addiction were explicitly highlighted in the consultation as deserving of more attention.

There is also a need for a more holistic view of consumer welfare, considering not just price but also issues such as consumer privacy, value of personal data and the ability of

[16] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1578762
[17]https://www.reuters.com/article/us-whole-foods-m-a-amazon-com-antitrust/critics-say-whole-foods-deal-would-give-amazon-an-unfair-advantage-idUSKBN19D2Q8
[18]http://speri.dept.shef.ac.uk/wp-content/uploads/2017/11/SPERI-IPPR-Digital-platforms-and-competition-policy-literature-review.pdf
[19]https://www.econstor.eu/bitstream/10419/169462/1/Giron-Vialle.pdf
[20] https://www.ft.com/content/349103ba-c631-11e7-b2bb-322b2cb39656
[21]https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2017-final.pdf

consumers to switch between services. This could help break down silos between regulators and promote a more collaborative approach. In the case of the Facebook/Whatsapp merger for example, data protection bodies expressed public concerns about data sharing following to the merger[22] - If competition regulators had factored in privacy standards, US regulators may not have approved this deal[23].

Public capacity

An informed public that can demand redress in instances where regulation and their rights have been breached is also a fundamental part of making technology companies and government accountable.

Outside of the ICO's protection of data rights, Ofcom and the Ombudsman Services (whose remits' are limited to internet providers) there are few routes for the public to settle disputes with digital services and platforms outside of the courts. In 2017 the UK's children's commissioner Anne Longfield called for a specialist ombudsman to protect the rights of children on social media[24], emulating the model of Australia's e-safety commissioner.

Research comparing regulators and ombudsman across Europe highlights the effective role of collective redress, where groups of individuals affected by similar issues can take collective action against the same defendant. Regulatory authorities which allow collective action are faster and more successful in addressing systematic infringements of market rules[25]. In the UK several regulators have shown the effectiveness of such powers, such as Ofwat returning £7 million to customers affected by Thames Water's misreporting of sewer flooding data[26]. But despite support from the ICO and civil society organisations[27] an amendment to the Data Protection Bill to allow for collective redress in situations where multiple individuals have been affected by a breach of data rights was not accepted by parliament[28]. New thinking around how collective action applies to the digital space is needed to shift the balance of power between big tech companies, government and society.

The current gaps in the regulatory landscape mean that digital technologies are not effectively being held to account for their impacts on society. Reactive, under-resourced and poorly focused regulators working in isolation from one another are unable to keep

[22]https://www.cnil.fr/sites/default/files/atoms/files/20161027_letter_of_the_chair_of_the_art_29_wp_whatsa pp.pdf <
[23]https://globalcompetitionreview.com/article/usa/1147829/mcsweeny-privacy-competition-standard-could-have-sunk-facebook-whatsapp
[24]https://www.childrenscommissioner.gov.uk/2017/10/11/anne-longfield-childrens-commissioner-for-england-responds-to-governments-green-paper-on-internet-safety/
[25]http://www.fljs.org/sites/www.fljs.org/files/publications/Delivering%20Collective%20Redress%20in%20Markets-New%20Technologies.pdf
[26] http://www.bbc.co.uk/news/business-27710187
[27] http://tech.newstatesman.com/policy/data-breach-compensation
[28]http://lordsamendments.parliament.uk/LordsAmendment/2017-2019/DataProtectionBill/Report/10584/2158

pace. This confusing picture and a lack of avenues for collective action do not help the public to gain redress.

Consultation Questions

1. Which current and emerging social impacts of technology are in need of stronger regulation?
2. What tools can support regulators to adopt a proactive regulatory approach?
3. What mechanisms are most effective for building the digital capabilities of all regulators?

Regulatory principles and frameworks

To build internet regulation which will be resilient and flexible in the face of as yet unknown technological change, it's important to consider what underlying principles and values are needed. The current focus of debate has been around how technology companies are classified and specifically around how content on social media is regulated. However Doteveryone favours the development of a holistic approach which will help foster responsible technology and there is a need for an underlying framework to achieve this.

Frameworks for content regulation

Attempts to legally classify technology companies as either publishers or utilities were seen by many of those who contributed to Doteveryone's consultation as over simplistic and counter productive as they operate across sectors and offer a broad range of services. Platforms' current neutral status as intermediaries absolves them of liability for content, but 'blunt regulation' that places full liability onto platforms can also be problematic. York University's Professor Natasha Tusikov summed up the concerns for both approaches: *"governments in the United States and United Kingdom require intermediaries to remove problematic content and ban users "voluntarily"... however, there are significant problems with informal regulatory programs that operate in the absence of legislation or judicial processes. Internet intermediaries are often not qualified to distinguish legality from illegality online... my research shows government and industry pressure on intermediaries often results in intermediaries over - blocking legitimate content in efforts to mitigate their risk of liability. The result is a chilling of freedom of expression and a regulatory environment that privileges rights holders and the enforcement of intellectual property rights."*

William Perrin, a former civil servant with experience setting up regulators, offered an alternative approach by using the principles of "duty of care" and harm reduction that are commonplace in many other sectors such as medicine and employment. Under this approach, platforms and service providers would be obliged to prevent users from harm and demonstrate the steps they are taking to do so. A regulator could then map all issues arising from a service, develop plans to address them and share good practice with other organisations working in a similar space to prevent problematic practices spreading across the industry. In placing a proactive obligation on companies, they are encouraged to innovate to tackle issues head-on.

Wider frameworks

Although it absorbs much of the policy debate, content liability is only one part of the regulatory landscape. There is a need to address the wider social impacts and unintended negative consequences of digital technology.

The precautionary principle used commonly in environmental sectors offers a legal precedent in this area. This principle is applied in situations where there are reasonable grounds for concern that an activity is causing harm, but the scale and risk of these issues is unproven. The onus is then on organisations to prove that their practices are safe to a reasonable level. In the UK, the Environment Agency has the power to enforce 'stop notices' that require organisations to halt activities until they have been proven to be safe. Applying this thinking to internet regulation, technology companies could be forced to stop or alter practices that preliminary evidence suggests cause harm until an independent auditor has assessed their impact and stakeholders have been consulted. Taking algorithmic discrimination as an example, organisations could be required to halt their use until they have been tested for bias[29].

The widespread participation on some platforms means they could also be viewed as online public spaces, as William Perrin has also suggested, meaning they could be governed by the same safety principles as offline public spaces such as the Health and Safety at Work Act. Within this a regulator could work with bodies in civil society and academia such as the UKCIS to develop a broad definition of on "online health and safety". By shifting the regulatory focus towards the general safety of platforms, the debate around liability for individual incidents (such as hate speech on social media or criminal offences committed by platform service providers) takes on less significance.

Within all regulatory approaches, the need to see technology companies in the context of their size and capability is crucial. Placing a proactive obligation on small organisations to police their platforms and services may place excessive financial and legal burden on them to comply, stifling their growth and playing into the hands of established technology companies. A degree of "regulation asymmetry", where technology companies within the same sector operate under different regulations is likely to be necessary in the internet space. A key role for any regulator is defining the threshold for regulation. This decision could be influenced by more nuanced indicators of power such as market capitalisation, user numbers, content reach or projected social impact.

Regulatory scrutiny of digital technologies should address the processes around their development, not just their impacts. Queen's University's Daithi Mac Sithigh spoke of the need to *"look beyond visible harms to examine the structures of technology"* during the consultation. With governance by design, the onus is on organisations to consider the impacts of their services during their design and take reasonable steps to mitigate them. A regulator can play an active role in this by encouraging transparency and understandability of technical processes, auditing them where necessary and intervening where design proposals don't meet a suitable standard. More broadly regulation can

[29]https://www.newscientist.com/article/mg23431195-300-bias-test-to-prevent-algorithms-discriminating-unfairly/

influence aspects such as professional standards that also have a significant impact on the design of technology. The ICO's privacy by design[30] work is an example of how this 'governance by design approach' is already being applied to a specific issue, and includes privacy impact assessments and codes of practice for anonymisation and data sharing.

Doteveryone's responsible technology programme[31] has also explored ways to make consumer technology products more responsible and accountable to society. This work has identified three core concepts that are central to the design of responsible technology:

- Context - looking beyond the individual user and taking into account the technology's potential impact and consequences on society
- Contribution - sharing how value is created in a transparent and understandable way
- Continuity - creating and supporting products and services that are safe, secure and reliable in a real-world environment, and ensuring people with different needs are accounted for in technology design.

These principles can be applied to a regulatory context in a number of ways. To ensure digital technologies are inclusive, standards for dark design patterns could be developed using a similar approach to the W3C Web Accessibility Initiative[32], and compliance with these standards could be made mandatory. For-profit platforms and services could be encouraged to be more transparent around their products' value flows, for example by reporting the value and source of revenues they receive from targeted digital advertising for each user. To consider context, technology organisations could be supported to carry out and report social impact assessments before their products reach market.

A similar approach has been used by the civil society organisation Article 19 and the Danish Institute for Human Rights, who have developed a model for assessing the human rights impacts of internet infrastructure providers[33] derived from the United Nations Guiding Principles on Business and Human Rights. The model is applied through a combination of self-assessment surveys and an independent review of policies, financial records and interviews with senior leadership. Cloud services and data centres are being considered as the next area the tool could be applied to The approach represents an example of a light-touch tool that a regulator could use to champion responsible design.

Human rights have been used by legislators and civil society as the foundation for a range of digital regulation initiatives, for example the Manilla Principles on Intermediary Liability[34] and UNESCO Broadband Commission for Sustainable Development[35] and thanks to their wide acceptance offer a useful framing for considering future internet regulation in the UK.

[30] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/
[31] https://doteveryone.org.uk/responsible-technology/
[32] https://www.w3.org/standards/webdesign/accessibility
[33] https://www.article19.org/resources/assessing-human-rights-impacts-internet-registries/
[34] https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf
[35] http://www.broadbandcommission.org/Pages/default.aspx

Some consultation respondents were however cautious about seeing digital regulation solely through the lense of traditional rights. The Open Data Institute's Jack Hardinges pointed to the emergence of new rights, such as the right to data portability, which is described by the GDPR, that relate specifically to digital technologies. This view was shared by the ICO's Steve Wood, who during the consultation spoke about the natural evolution of rights through case law and the emergence of grass-roots issues - for example the right to be forgotten was established by precedent in the Google Spain vs Gonzalez case[36] before it was adopted through GDPR. Digital technologies and human rights develop iteratively together, and effective regulation should account for this relationship.

Incorporating ethics

In the consultation, respondents drew an important distinction between rights and ethics. Many felt that ethical practices should be championed using 'softer' collaborative approaches, whilst legal mechanisms were more appropriate for protecting fundamental rights. A range of ethical frameworks (in particular in the fields of data and artificial intelligence) are already established or in development[37][38][39][40]. In the UK, bodies such as the Centre for Data Ethics and Innovation and Ada Lovelace Institute will be established in 2018 to lead in this area and build upon this extensive body of existing work. Organisations Doteveryone spoke to during this consultation felt there were three priorities for around ethics:

- Understanding how ethics can be applied to a messy real-world environment.
- Embedding ethical practice across the private and public sectors.
- Developing mechanisms for accountability where ethical standards have been breached.

While responsibility for these challenges lies with across society, consultation respondents saw a range of roles for regulation in addressing them:

- Developing ethical codes of practice. The Human Fertilisation and Embryology Authority's (HFEA) Code of Practice was cited as an example of good practice. This code is updated on an ongoing basis by an independent Code of Practice review working group, who engage with stakeholders through open workshops and consultations.
- Periodic audits of organisations to monitor compliance with ethical frameworks and codes of practice, as is currently done by the Global Network Initiative for the ICT infrastructure sector[41].

[36] http://www.5rb.com/case/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/
[37] https://theodi.org/article/data-ethics-canvas/
[38] https://www.gov.uk/government/publications/data-science-ethical-framework
[39]https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk
[40]http://www.unesco.org/new/en/media-services/single-view/news/robotics_ethics_a_technology_based_ethical_framework_for_to/
[41] https://globalnetworkinitiative.org/independent-assessors/

- Establishing formal mechanisms for employees or external parties to raise concerns when ethical codes have been breached - this could take the form of a 'digital standards panel' who investigate and mediate disputes. Consultation respondent Robbie Stamp raised the importance of *"reviewing to learn over reviewing to blame"* - the panel could produce publicly available case studies to promote learning across the digital sector, as is currently done by the Fundraising Regulator[42].
- Developing widely-accessible ethical design standards for specific technology areas, such as the British Standards Institute for the ethical design and application of robots and robotic systems[43].
- Promoting knowledge transfer between technology organisations and ethicists, through initiatives such as establishing an independent ethics advisory board to advise digital companies.
- Voluntary or non-voluntary transparency reporting. The government's response to the Internet Safety Green Paper outlined plans for an annual 'internet safety transparency report' for platforms to report incidences of illegal content, user complaints and moderation strategies[44]. This reporting could be expanded to encourage accountability that goes beyond content - organisations could for example be required to report the steps they have taken to evaluate the impacts of their algorithms, or publish the range of prices different consumers have paid for the same service/product due to personalised pricing.

Effective regulation of digital technologies will require a foundation of regulatory principles which underpins it. Ensuring this underlying framework is forward looking and flexible will determine the success of new measures for accountability and will create a coherent regulatory environment. It is important that these regulatory principles work in tandem with initiatives to promote ethical standards.

Consultation Questions

4. The idea of applying a "duty of care", "precautionary principles" and "governance by design" offer some approaches to regulating the unintended consequences of emerging digital technologies. What underlying framework can best regulate the issues associated with these new technologies?
5. Obliging small and emerging digital organisations to police their platforms and services may place excessive burden of them and stifle their growth. What metrics could be used to define thresholds for exempting digital organisations from regulation in these circumstances?
6. What regulatory tools can encourage more accountability during the design and development of digital technologies and services?
7. What approaches are most effective in encouraging the widespread adoption of ethical principles and frameworks by technology organisations and government?

[42] https://www.fundraisingregulator.org.uk/make-a-complaint/case-studies/
[43] https://shop.bsigroup.com/ProductDetail?pid=000000000030320089
[44]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf

Regulating the future

Understanding how public accountability can function in times of uncertainty and fast-paced change is a fundamental priority for digital regulation.
Focussing on a specific technology risks regulation being made redundant by technological change, whilst the standard "reactive" approach to regulation means a technology may grow until its social adoption overwhelms attempts to regulate (such as in peer-to-peer file sharing, where courts and regulators have struggled to keep up with a constantly evolving suite of file sharing services[45]).

'Anticipatory regulation' was raised by Nesta's Harry Armstrong as an alternative to conventional static and reactive regulation. In this approach, regulation is developed iteratively as a technology and its impacts on society emerge. A regulator plays an active role in building up an evidence-base through research and engagement with other stakeholders, identifying future risks and opportunities and tracking them as they develop. Central to this regulatory ethos is the development of a strategic future vision for the role a technology will play in society, that is underpinned by a set of collective values.

In this context bringing together industry, government, civil society, technology users and the wider public to define these collective values is an integral part of effective regulation. It is also important that the regulator sits outside government so that the use of technology in the public sector is subject to the same scrutiny.

This "multi-stakeholder approach" was advocated by many of those responding to the consultation. A regulator can work directly with the public using 'deliberative dialogue' tools such as citizen juries[46] or multicriteria mapping[47] to gain an insight into the views and values of the public on emerging technologies. Through such work public concerns and potential ethical concerns can be flagged before a technology has reached scale, giving regulators time to address issues before they occur. The government and Food Standards Agency's failure to engage with the public at an early stage was cited as a contributing factor to the backlash against genetically modified crops in the UK, and shows the importance of such "upstream" engagement. Establishing a transparent and open dialogue with the public gives democratic legitimacy to independent regulators, whose are typically non-elected bodies.

Another established approach for monitoring future risks is horizon scanning, which is used by existing regulators such as Ofgem and the Human Fertilisation & Embryology Authority (HFEA). Within this the HFEA reviews the future legal, ethical and commercial implications of new clinical developments, with issues identified by their internal policy team and independent expert panel and compiled into a public-facing annual report. This

[45] Brown, I. and Marsden, C. (2015) *Regulating Code* Cambridge: The MIT Press
[46] https://www.epa.gov/international-cooperation/public-participation-guide-citizen-juries
[47] http://www.sussex.ac.uk/spru/impact/mcm

scanning then leads to future policy reviews and new sectoral guidelines and codes of practice. Much of this work within government sits with the Horizon Scanning Programme Team and the Parliamentary Office for Science and Technology (POST). The broad focus of both these groups and their relatively small size however means that they are only able to undertake horizon scanning for specific issues, meaning that are ill-suited to provide comprehensive scrutiny of the digital space.

Giving a regulator an open mandate to conduct market studies on areas of interest is another approach for spotting emergent issues. Currently the CMA holds this remit and a future digital regulator could have powers to review the social impacts of specific digital technologies across the population and develop an evidence-base to inform future regulatory priorities. An index could be developed that attempts to compare severity of online harms in a similar way to the Cambridge Crime Harm Index[48] or Drug Harm index used by the New Zealand Ministry of Health[49]. Through comparing the relative increase in emerging harms over time, such an index could also shed light on their trajectory and be used to anticipate future social issues, as well as flagging areas where regulation is disproportionate to the severity of an issue.

The FCA's regulatory sandboxes represent another example of a forward-thinking regulatory tool, and allow firms to test products in a live market under supervision of the regulator. As part of this the FCA put in place 'bespoke safeguards' to prevent consumer harm and monitored the impact of the tested products on consumers[50].

University College London's Jack Stilgoe raised a broader concern around the timescale of government horizon scanning - with governments' thinking often not extending beyond the 4-year election cycle, longer term issues are afforded less attention. This underlines the need for any regulator to sit outside of government.

In an economy where the boundaries between technologies and markets are blurring, there is also a need for regulators to work together more closely. Increasingly regulators are looking at the same issues through different lenses, and a collaborative approach is needed. The ICO and the CMA's proposed joint inquiry into terms and conditions is a good example of this in practice. Greatly enhanced collaboration and knowledge transfer will be vital to change the current status quo of siloed regulators focusing on bounded sectoral impacts. Whilst the Better Regulation Executive[51] and the announcement of a £10 million Regulators' Pioneer Fund[52] in the Autumn Budget represent a step in the right direction, their broad nature means there is still a need to develop initiatives specific to digital technologies.

[48] https://academic.oup.com/policing/article/10/3/171/1753592
[49]https://www.health.govt.nz/system/files/documents/publications/nz-drug-harm-index-2016-2nd-ed-jul16.pdf
[50]https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf
[51] https://www.gov.uk/government/groups/better-regulation-executive
[52]https://www.gov.uk/government/publications/autumn-budget-2017-documents/autumn-budget-2017

The importance of regulatory collaboration on an international level was also a recurrent theme in the consultation. Many contributors felt the UK's attempts to regulate multinational technology companies in the absence of international collaboration would be toothless. Despite this some voiced concerns about existing global regulatory networks such as the Internet Governance Forum, which they criticised for excluding lower-GDP states and over-representing the interests of US-based organisations. Against this backdrop many felt EU-level collaborations would be most effective for a UK regulator. With the UK currently likely to leave existing initiatives such as the EU Digital SIngle Market[53] and the EU Competition Network[54] after Brexit, developing a strategy for leveraging international networks will be an important part of fostering genuine accountability in multinational digital organisations.

Anticipating the future regulatory landscape

Bringing about a paradigm shift from reactive to proactive regulation is a vital part of regulating in fast-moving digital sectors. To understand the medium and long-term issues, regulators should explore existing tools such as horizon scanning and regulatory sandboxes whilst developing new forward-facing regulation tools.

To cut through the uncertainty that is inherent in any prediction of the future, regulators can look to techniques such as scenario planning and risk analysis to attempt to quantify the future risks associated with emerging digital issues. Similar approaches are used widely in sectors such as finance and the environment and offer a model for digital regulators to learn from.

Consultation Questions

8. What tools should be used by regulators to identify and address emerging and long term regulatory issues?
9. What tools should be used by regulators to explore the views and values of the public around digital issues?
10. How can regulators build and maintain their knowledge of the digital sector, and how is this best shared across sectoral regulators?
11. How can UK regulators working in the digital space promote international collaboration following Brexit?

[53] https://www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union

[54] https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/67/67.pdf

Further consultation questions

In the preceding chapters we have attempted to outline the overarching principles and activities for an independent internet regulator in the UK, and in the process many new avenues for discussion have opened. In June 2018 we are inviting responses to the questions found throughout this paper which are summarised in the box below. To share your views for internet regulation in the UK, please get in touch at hello@doteveryone.org.uk before Friday 22 June.

1. Which current and emerging social impacts of technology are in need of stronger regulation?
2. What tools can support existing regulators to adopt a proactive regulatory approach?
3. What mechanisms are most effective for building the digital capacities of all regulators?
4. The idea of applying a "duty of care", "precautionary principles" and "governance by design" offer some approaches to regulating the unintended consequences of emerging digital technologies. What underlying framework can best regulate the issues associated with these new technologies?
5. Obligating small and emerging digital organisations to police their platforms and services may place excessive burden of them and stifle their growth. What metrics could be used to define thresholds for exempting digital organisations from regulation in these circumstances?
6. What regulatory tools can encourage more accountability during the design and development of digital technologies and services?
7. What approaches are most effective in encouraging the widespread adoption of ethical frameworks by technology organisations and government?
8. What tools should be used by regulators to identify and address emerging and long term regulatory issues?
9. What tools should be used by regulators to explore the views and values of the public around digital issues?
10. How can regulators build and maintain their knowledge of the digital sector, and how is this best shared across sectoral regulators?
11. How can UK regulators working in the digital space promote international collaboration following Brexit?

Conclusions and next steps

Digital technologies are reshaping society, blurring the distinctions between consumers and suppliers, industry and the state, citizen and worker and offline and online sectors. In doing so, they pose deep challenges to conventional regulatory frameworks and bring about a need to develop new mechanisms for improving the accountability of the institutions developing and using digital technologies. This paper makes the case for an new independent regulatory body to lead this process.

In reviewing the current landscape of internet regulation in the UK many challenges have emerged. Regulators tend to adopt a reactive approach to the issues associated with digital technologies, waiting until a harm has already manifested itself to intervene. The design and use of digital technologies evolves at a unprecedented pace, meaning such ad hoc regulatory actions are ineffective. The proliferation of the IoT and pervasiveness of data, algorithms and other digital technologies across historically offline sectors also means all regulators are now grappling with internet-related issues. There is a widespread need to build up digital understanding and technical capabilities across the regulation sector and promote collaboration on digital issues that sit across the traditional market boundaries.

Regulators also have a tendency to focus on individual rights and issues such as safety, data use and security. Social impacts that are only visible through assessing the effect of technologies across large groups of users need stronger regulation. Issues including the impact of technology on inequality, the use of design dark patterns and technology addiction were highlighted as deserving of more regulatory attention during the consultation.

Looking beyond the impacts of established technologies to regulating the design processes of emerging digital technologies can also make technology developers more accountable for their work. Tools such as auditing of technologies' processes (including algorithms and design patterns), social impact assessments at an early stage of a technology's lifecycle and developing industry standards for responsible technology design can help embed accountability into this design process. Established legal principles such as "duty of care" and the precautionary principle found in other sectors also offer an underlying legal framework for regulating the unintended consequences of technology.

Human rights frameworks offer a starting point for developing regulation of digital technologies, and their broad acceptance means they are a useful means of gaining consensus from the diverse range of stakeholders affected by internet regulation. Many digital issues however fall outside of the scope of such basic frameworks, and regulators need to go beyond them to provide protection to society. Many consultation respondents felt that ethical frameworks for technology should be championed using 'softer' collaborative approaches bringing together industry, government and regulators. A broad

range of organisations are working in the digital ethics space, and many ethical frameworks (in particular around AI and data) are already established. In this context applying ethical frameworks to real-world organisational context and developing mechanisms for accountability in instances where ethical codes have been breached should be the current priority for regulators.

To address these challenges, we see a vital role for an independent regulatory body to:

- **Build up industry-standard expertise** to scrutinise the underlying technical structures of digital technologies, auditing design processes, conducting independent impact assessments at an early stage of a technology's lifecycle and developing industry standards for responsible technology design.
- **Lead horizon scanning and foresight activities** to identify emerging digital issues and conduct studies to develop an evidence-base around issues whose impact is seen on a societal level.
- **Advise current sectoral regulators on emerging technical challenges** and co-ordinate unified responses for cross-sectoral issues such as the use of data in healthcare.
- **Convene stakeholders to develop a collective long-term vision for an internet that works for the good of society**, running deep public consultations and working with industry, civil society and government to understand how ethical frameworks can be applied in a messy real-world environment.
- **Build up public understanding of digital issues** so that society is able to use these regulatory levers for accountability effectively, providing mechanisms for technology users to raise concerns through an ombudsman role.

This paper touches on some regulatory tools that an independent regulator *could* use to deliver on these overarching aims:

- Conduct in-depth market studies of emerging digital issues, identifying key risks and scoping out actions to address them.
- Establish an index of social harms associated with digital technologies
- Conduct horizon scanning and scenario planning to identify medium and long-term technological risks to society.
- Carry out independent auditing of the technical structures of technology, such as testing for algorithmic discrimination.
- Develop open design standards for aspects of technology, such as legibility and intelligibility for terms and conditions.
- Develop and carry out social impact assessments for technology developers to use at an early stage of a technology's lifecycle.
- Develop ethical codes of practice and establish a 'digital standards panel' to investigate and mediate on instances where ethical codes have been breached.
- Conduct research into the views and values of the public and other stakeholders around emerging technologies and leading public information campaigns on emerging digital issues
- Developing new agile regulation tools such as sandboxes for the digital space.
- Manage voluntary or non-voluntary transparency reporting for a range of issues - not just content.

- Establish a knowledge transfer network for sectoral regulators to share learnings on digital issues.

This list of regulatory activities is not exhaustive, and new innovative ways of working will be needed to build a UK regulatory system that thrives in a digital economy. In the next stage of this work Doteveryone will be exploring which of these tools and approaches can equip an independent regulator to meet this challenge. This paper represents the start of a conversation, and in June 2018 we will be inviting views on the consultation questions described in section 7. Following these discussions a White Paper will be released in July 2018 outlining our detailed vision for an independent internet regulator in the UK.