DIGITAL SOCIETY

REGULATING PRIVACY AND CONTENT ONLINE

GARFIELD BENJAMIN

SOLENT UNIVERSITY
SOUTHAMPTON

2020

ACKNOWLEDGEMENTS

This project was supported by Solent University, through the Research England evidence-based policy fund.

Surveys were conducted by YouGov.

Participants at the project workshop were representatives from academia, government, think tanks and advocacy groups. This included:

> Dr Elinor Carmi, Me and My Big Data, University of Liverpool
> Areeq Chowdhury, Director of WebRoots Democracy
> Harry Farmer, NESTA
> Ellen Judson, Researcher, Demos

We thank the participants for their insightful contributions to the discussion.

We would also like to thank Dr Elinor Carmi and Areeq Chowdhury for reviewing this report.

CONTENTS

Executive summary

Introduction

Privacy in and out

Review of existing recommendations

Survey

- Key observations
- Related evidence

Key issues

Recommendations

- 1 Regulate privacy, data and online content together
- 2 Build regulation on principles linked to rights
- 3 Provide a platform for representation
- 4 Give regulators meaningful powers and the resources to exercise them
- 5 Strengthen design-side regulation
- 6 Promote public understanding
- 7 Plan for future development

Concluding remarks

References

Appendix - survey results

EXECUTIVE SUMMARY

Society increasingly relies on digital platforms. But regulation of how we interact with social media, search engines or other online platforms has so far been unsuccessful in preventing harms, ensuring rights are upheld or empowering citizens to engage in digital society. Current laws tend to separate issues out into privacy and online content. This has the advantage of giving clear remits to regulators and focusing energy, resources and expertise on specific issues. But it also holds regulators and policy-makers back when it comes to tackling larger systemic issues.

This report argues for broader regulation that brings together the ways data about individuals goes out (privacy or data protection) and how the information they receive comes in (recommendations for online content, particularly when harmful and/or political). This currently spans multiple government departments and regulators in the UK, creating overlaps in some areas but leaving gaping holes in others. At a time when we are relying more and more on large platforms with huge amounts of power, it is essential to empower citizens, communities, smaller organisations, and government, to tip the balance away from a few big tech executives. Only by taking a more comprehensive and cohesive approach can regulation promote rights, justice and equity for a more positive digital society.

METHODS

This project builds on research into performative frameworks of rethinking online privacy. Understanding privacy as not just technical and legal systems but a whole array of individual and collective acts that shape and reinforce norms and expectations leads towards thinking in terms of identity, consent and collective action. This approach lends itself to also thinking about information “in” as well as information “out”, by assessing privacy and online content as part of the same wider issue. We highlight the expectations set by digital platforms and the algorithmic “back-end” which combines personal data and content recommendations. The approach emphasises the importance of context - how the sharing of information might be appropriate in one situation but not in others - and seeks ways to empower people with greater agency over the data they share, receive, and is collected about them.

The project began with reviewing existing recommendations for policy interventions to tackle issues around the regulation of online privacy and/or content, including targeted advertising and political content. We then conducted nationally representative surveys of UK adults to gain public perspectives on trust of major platforms, concern for privacy and online content including misinformation and advertising, risks and opportunities to individual identity and the integrity of society, and support for more comprehensive regulatory measures. The surveys were followed by a workshop with academia, advocacy groups/think tanks, funding foundations and government.

RESULTS

Our findings show that the public is highly concerned about information online. This is strongest around privacy, which suggests an opportunity to use increasing privacy regulation as a basis for more thorough regulation of and education about digital platforms more widely.

People feel relatively in control of what they see online, but express significant concerns with influence and decisions about online content and platforms. There is a large disparity between how the public perceives current influence over regulation (78% of people feel tech companies have a lot or a little influence, 40% for UK politicians, only 33% for users) and desired influence over regulation (57% tech companies, 61% for UK politicians, 75% for users).

The UK public strongly supports platforms being legally responsible for checking political adverts (80%, averaged across Google, Facebook and Twitter) as well as being required by law to regulate or check any content they provide to users (76%, averaged across Google, Facebook and Twitter). People place the responsibility for this on platforms, but support increased regulation by government and a range of methods punishing platforms that break the rules. There is widespread support for greater regulation of the use of personal data online (73%), fake news online (75%) and hate speech online (71%).

People do not trust major online platforms, and do not feel represented by the tech industry. But there is a feeling of even less representation in the press and UK politics. Existing proposals for greater regulation have public awareness and education as strong common themes. Working with different user groups and communities should be an important part of the work of UK regulators.

But people are optimistic about the potential for the Internet. While only 25% of people think the Internet currently reduces inequality, and there is widespread acknowledgement of the potential harms for individuals and different harms for different groups, 50% of respondents still felt that platforms could be designed in ways that reduce inequality. There is a strong desire for greater regulation of platforms, and 67% of people support regulating privacy and online content more cohesively.

CONCLUSIONS

There are a few key themes around the need for future regulation that have emerged through the project.

Inequality and politics : political advertising and fake news are important areas for regulation. There is also the need to improve representation in regulation. Trust is low and the impacts of shadowy back-end decisions and systems are very real. Power asymmetries need to be challenged to empower citizens to participate in digital society without being exploited by mutli-national corporations.

Design : there is often a lack of clarity surrounding how platforms actually collect and use data, particularly with automated decisions by algorithms. Improving regulation requires improving design-side influence of regulators and communities in order to support the desired principles of rights, equality and justice for digital society.

Combining regulators : there is strong support for bringing regulation together to tackle the larger systemic issues with digital platforms. But this requires sensitivity to the different approaches, expertise and resources necessary. There is resistance to any existing regulator taking on such as broad remit, so we propose a formal inter-regulator office to enable different existing powers to be brought together to tackle larger issues.

Awareness : education and critical digital skills are a significant challenge. This includes developing up to date integration with school curriculum across technical and social subjects, but should also take into account the intersectional barriers to digital participation such as age (at either extreme), class, and race. Tech industry workers are another group where better critical knowledge of sociotechnical issues could create better design practices and support the aims of public policy.

RECOMMENDATIONS

We propose the following measures for a more cohesive and coordinated approach to regulating privacy and content online:

1. Regulate privacy, data and content online together : by establishing an Office for Digital Society to act as a formal mouthpiece for combining the remit of the ICO, OfCom, ASA, CMA and others in tackling larger and systemic issues of privacy and content online.
2. Build regulation on principles linked to rights : equity, diversity, dignity and justice should be at the centre of future regulation to empower individuals and groups.
3. Provide a platform for representation : by involving affected communities in regulation is essential in resolving the massive power asymmetries currently held by digital platforms.
4. Give regulators meaningful powers and the resources to exercise them : by ensuring that financial and staff resources of constituent regulators are adequate to tackle the large number of cases, and that the Office for Digital Society can appropriately bring together regulators' powers to effect meaningful change.
5. Strengthen design-side regulation : by taking a more proactive approach not only to recommendations but for regulation and requirements, empowering regulators to take action earlier, and engagement more deeply with industry and civil society.
6. Promote public understanding : by expanding practical, critical and participatory skills not only in formal education but through promoting interdisciplinary engagement and understanding of societal issues within industry.
7. Plan for future development : build in mechanisms for sandboxing future regulations and a clear path for expanding the remit of the Office for Digital Society, up to and including a possible Department for Digital Society.

INTRODUCTION

INTRODUCTION

Much of life today occurs either online or is mediated by online platforms. The spread and vast power of platforms creates major social and regulatory challenges, with real consequences for individuals, communities and democratic structures. In particular, there are key points of regulation that intersect: privacy, the data we give out or is collected about us, and content, the information we receive. How decisions are made about the way information flows in different directions is often hidden in the "back-end" of platforms, algorithms and data centres. This can lead to confusion and a lack of agency not only for individuals but also for marginalised communities and even policy-makers and regulators.

Regulation of privacy and content online has come a long way. In the UK, the General Data Protection Regulation (GDPR) and 2018 Data Protection Act (DPA) have provided a useful first step towards empowering privacy rights, but remain plagued by issues of enforcement and lack of future scope. Similarly, the proposed Online Harms legislation and regulation offers improvements in recourse against discriminatory or otherwise harmful online content, but remains limited in proactive measures for improving justice.

Tackling structural issues for digital society requires a more comprehensive approach to the data, platforms, interfaces and algorithms that define life online. Privacy and content are inextricably intertwined, but this is not reflected in the current UK regulatory environment. This report proposes combining the many related areas of regulation to improve justice, agency and empowerment in digital society.

The report begins with the core concepts that underpin the proposal, drawing on new academic research into the social effects and structures of technology. This includes a performative critique and framework of privacy and content, building on interdisciplinary and intersectional work across fields.

We then review existing policy recommendations to draw out common approaches to more effective regulation of privacy and content, separately and together, in specific contexts and for society as a whole.

We present new survey data that provides a representative view of UK public opinion surrounding issues of privacy, identity, representation, data, algorithms, online content and their regulation.

We discuss key issues emerging from the surveys, policy review and a workshop held as part of the project. Attendees at this workshop included representatives from academia, government, policy and advocacy groups, and foundations, all working towards a better digital society. Through the workshop, experience and perspectives were shared and the results of the surveys discussed alongside broader issues in the regulation of online platforms.

Finally, we propose a set of seven recommendations for establishing a cross-regulator Office for Digital Society as a roadmap for tackling these issues.

PRIVACY IN AND OUT

PRIVACY IN AND OUT

Preventing online harms and improving the Internet as a public good is not just about being online, but about being together online and doing life online together. It is therefore not just about protecting ourselves online - which is inherently divisive and individualising - but about finding ways to empower citizens and communities through improving the integrity of our information and interactions online. This leads to two key questions:

Access : Who has access? What are the conditions for access?
Agency : What are the barriers to agency? How can we better empower everyone?

These issues cut both ways, and they predate the Internet. Loyalty schemes were used to promote specific products, special interest or client mailing lists were used to send targeted advertising, and helicopter photographs of our homes taken unsolicited and without consent appeared through our letterboxes available to purchase, all long before search engines and social media. But the new digital tools and platforms we now often use on a daily basis have escalated these practices - and, more importantly, the harms they can create - to such an extent that there is a need to radically rethink the way we govern the use of such technologies to increase the equity and justice of online society.

This project builds on research Benjamin2020 into how the culture of privacy influences the effects of technology on society. Privacy was chosen as the concept on which to focus as it is already in use across different fields - law, technology, social science, medicine - and, more widely, it means something to everyone. Each setting may have contextual differences in how it is defined, but it is a commonly used concept that everyone sees the value of in some situations (whether that is metadata about online activity, a private conversation, or going to the bathroom). But while it is an influential concept, it is also contested with different expectations. Understanding how these different ideas are embedded in our culture helps us to use them more positively across disciplines and settings. The work uses a few important concepts to understand these issues.

Contextual integrity : this means the appropriate flow of information Nissenbaum2010, a way of thinking about privacy that acknowledges that we may want to share a piece of information in one context (such as a photo of our children with close friends and family on social media) but not others (we wouldn't want it to be used to train a facial recognition system or in an advert by a company we dislike).

The networked self : this is the way our identity is developed in part through what we see and do online, and shows the importance of establishing legal and technical systems that empower its development Cohen2012. It is an active process rather than something fixed in stone. It is built through our relationships with information and with other people or communities.

The incomputable : there is always something that resists being converted to data Hildebrandt2019. Human relations are not only complex but also emotional and cultural. Appreciating this underpins the need for proportionate and contextual use of data (i.e. collecting only when necessary and using only when appropriate) to avoid misrepresentation in decision-making. This also means that there

is no single 'solution' to issues of privacy and data - what is needed are ongoing discussions and regular review for inclusive policy.

Performativity : this means that privacy is a social norm that is created and reinforced by the individual and collective acts we all participate in and how we see other people's actions. For example, social media sites may set up a community expectation that when we add a new 'friend' we should look into their history, likes, and other information to find out as much as we can about them, or it may be expected that we acknowledge such information exists without looking at it all. Performativity in this sense was originally applied to traditional social norms and roles, such as gender, by Judith Butler and Eve Kosofsky Sedgwick. In a performative framework, individual actions, collective actions and collective responses are all intertwined in establishing different norms and expectations.

This requires a shift in language. While protecting privacy is useful in legal, technical and regulatory context when thinking about, for example, recourse, it remains fundamentally reactive. Performing privacy becomes a more active, collective and preventative process. Other language shifts that have been proposed Costanza-Chock2020 DIgnazio&Klein2020 include moving from ethics (which in practice remains largely vague and voluntary) to justice, from fairness (which assumes an equal starting point) to equity, from accountability to co-liberation, from transparency to reflexivity, and from tackling bias in data to tackling the underlying structural oppression that leads to the creation of biased systems in the first place.

Emerging from the research are a few key principles of performing privacy:

> Privacy (and data) are something we do, not something we have;
> How we share and use information builds and reinforces expectations;
> Context is important;
> The flow of information should be visible;
> We should challenge uneven power structures that lead to discrimination;
> Identity, consent and collective action are core principles not just buzzwords;
> Shaping positive contexts means more emphasis should be placed on communities and collective action online and offline;
> We should strive to empower all users and communities online.

The same principles apply to online content.

Links between privacy and online content, or surveillance and manipulation, are well established Zarsky2006 Tufekci2014 SusserRoessler&Nissenbaum2019. This includes targeted political advertising, search engine recommendations, and news or misinformation. The relation between these different directions in which information flows has been labelled "epistemic inequality" Zuboff2019, the gap between what an individual can know and what is known about them. These are interconnected issues, with intersectional impact, including problems with representation (of, for example, womes, BAME people, trans people, those with disabilities, ...) in online content Noble2018 DIgnazio&Klein2020. How the underlying technical systems operate can lead to wider issues of algorithmic discrimination and the exclusion of some members of society from information and opportunities Benjamin2019.

Similar platform processes mediate and marginalise information going out (privacy) and information coming in (online content). This has been described as the rhythms of online media Carmi2020, the patterns that control how information flows in all directions. Privacy feeds into content (who we are determines what we are shown) and the two processes together tend to define who we can be and what we can do online. This more often than not heightens

and exacerbates existing inequalities. Something is always lost in reducing the diversity of society and human experience to computable categories that fit neatly into an algorithm for targeting content. The same problematic assumptions - a technological ideology - underpin both the serving of content and the creation of data that enable it.

The complex impact of the connections between privacy and online content on public policy has also been established Gandy2017. The need for robust privacy mechanisms to protect users from exploitation of their data in relation to what content they see online is also gaining traction in policy contexts ICO2019. But there is an extra level that is currently missing from the debate: using privacy as a concept and set of regulatory tools to directly tackle the problems of personalised content. This project sees privacy and content not just as interconnected issues but part of one and the same underlying issue, and proposes that they should therefore be regulated together in a more cohesive way.

REVIEW OF EXISTING REGULATIONS

REVIEW OF EXISTING RECOMMENDATIONS

As more and more of society and government has moved online, issues of privacy, personal and public data, and online content have spanned across many government departments. Government can often be a sprawling mass of bureaucracy and overlapping remits or jurisdictions, particularly in relation to the use and regulation of data and the Internet. Separate laws cover Human Rights, Data Protection, Freedom of Information, Digital Economy, Copyright and other related rights and regulations. DCMS, BEIS, DfE, DHSC and the Cabinet Office are but a few of the departments with key responsibilities, and many have dedicated digital branches, themes or teams. National Data Strategy, CDEI, Digital Economy, NHSX, Government Digital Services or NCSC/GCHQ, each one focuses on a specific aspect of digital society. Similarly, various oversight bodies have remit that covers these issues, including the ICO, OfCom, Children's Commissioner, EHRC, CMA, ASA, and the list is only increasing.

This organisational structure allows for multiple different approaches and foci of regulation, but it also risks inconsistency, gaps between regulations and implementations, and the need to ensure government itself is upholding best practices.

There are many recommendations for improving regulation around specific areas of privacy, online content, targeted advertising, digital politics and related issues. These have come from government entities, academic researchers, policy think tanks and advocacy groups. The recommendations often use different approaches and languages depending on the context, aims and priorities of the recommending organisations, but a few key themes emerge across these different recommendations.

Reviewing the current space of regulatory recommendations provides a key to developing more cohesive future regulation that brings together privacy and online content, and the full data-algorithm ecosystem.

Regulate data out to regulate data in

The primary way of linking the in/out rhythms and flows of data in regulation is to improve privacy rights in order to mitigate some of the harms of personalised or targeted content online. The impact and intersection of platforms gathering data about us and using it to target advertising, provide personalised content recommendations or filter out "undesirable" content [Carmi2020] - usually algorithmically - has been a long identified area of concern in terms of surveillance, representation and mediation of information. And yet it has remained largely unregulated, owing in part to the international nature of large online platforms such as Google and Facebook, in part due to the unprecedented social conditions these technologies have created, in part due to lobbying influence to protect the business models of these platforms, and in part simply due to the excess of power and control these platforms wield in the organisation of digital society. Regulation has been slow to catch up, but there have been several important steps (GDPR/DPA, Online Harms) and high profile policy recommendations relating to this problem.

The CDEI Review of Online Targeting: Final Report and Recommendations examined both targeted advertising and online content recommendations. The report highlighted the different regulators involved in this area but focused its recommendations on the new online harms regulator. The report's suggestions emphasised three areas: accountability, transparency and user empowerment. This included calling for a more coherent approach between the online harms regulator (OfCom) and other regulators such as ICO and CMA. However, in detail this refers largely to "sharing data science resources", which risks falling into promoting the language of platform domination and thereby entrenching targeting as a valid approach. We can instead call for a truly coordinated effort to tackle broader issues of data and online content. The CDEI report also emphasised the importance of information, including giving independent experts access to platform systems for audit and requiring explanations from platforms (reflecting the right to explanation of decisions made by algorithms under the GDPR/DPA). This is linked to transparency as well as user empowerment, focusing on design-side best practices and further information available for users around the funding of political adverts.

However, the CDEI report is symptomatic of how existing regulation is developed, in that it limits itself to the clear issue of online targeting - with a particular focus on advertising. This provides purpose and specificity, but also places a perceived limit of online harms to advertising products or influencing political opinions. These certainly are important areas, and are included throughout this report, but we also push further to acknowledge the broader flows of information that may influence or discriminate against different groups in society. The recommendations also risk maintaining current definitions or loopholes that enable large platforms to bypass the terms of regulation. The approach of "limiting harms and enabling beneficial uses of online targeting" could enable platforms to continue with ethics washing, voluntary codes of practice and an economic push for financial benefits over a commitment to rights and users. Further, advertising cannot be disentangled from wider flows of data to and from users - placing this limit will in turn always limit the effectiveness of regulation. Broader consideration of information users receive online is required to prevent the manipulation of labels to avoid due scrutiny, as well as to address the rights implications of the enormous power imbalances that users suffer in online platforms. The CDEI report is a hugely useful step in addressing some of these important issues, but the scale of the problems at hand - the sheer weight and scope of the largest platforms - requires much deeper integration of privacy and content for effective regulation.

The false trade-off between economic benefit, and user rights and empowerment, has been further questioned by recent findings by STER, the Dutch advertising agency for public broadcasts. STER found that tracking cookies have little to no provable benefit, and that in fact campaigns without such cookies are often more successful. The report acts as a call to avoid worsening the perception of 'clickbait' as a valid method, which has wider relevance to issues of information quality and citizen participation in online society. The importance of context and collective audience emerges again as STER proposes contextual advertising as the more effective alternative, preserving privacy while pushing for greater relevance and quality of content or ads.

A concept brought up in the CDEI report that resonates with other policy work is the idea of "data intermediaries". A data intermediary would be a third-party entity that represents a user's interests in how data flows between them and platforms. This echoes what the 2018 CMA Online Platforms and Digital Advertising Market Study (Appendix H) identified as "intermediation" in the business interface side of advertising platforms and the companies who use them, by creating a more substantial platform for user negotiations in how data is used. Similar concepts also appear in Ada Lovelace Institute's project Rethinking Data as "data stewardship", focused on data for public bodies, and in the broader legal concept of "data trusts" Delacroix&Lawrence2019 as potential

entities that could have the legal status to safeguard users' interests. But all these approaches share some common limitations. Firstly, they continue the idea that data is property to be traded. Given the broader inequalities and injustices of our economic context, this is likely to keep too much power beyond regulation and in the hands of monopolising platforms. A rights, dignity and agency based approach to privacy is much more effective in trying to combat systemic injustices. Secondly, this form of consolidating data mediation still requires significant support, explanation and additional trust. Adding a further layer of interaction risks further obscuring the back-end of data flows to users. Data intermediaries or similar would still require a highly engaged user base. More direct regulation to enforce community representation in decision-making and data ecosystems, along with more robust complaints procedures and regulator powers, is more likely to be effective in enhancing user agency.

This "back-end" of online content and decision-making was highlighted in the Privacy International submission to the House of Lords Select Committee on Democracy and Digital Technology. The submission emphasises how design choices, algorithms, data, etc. interact to define what content is seen by different people, as well as the issues of automating these processes and gatekeeping by a few large tech companies. Privacy International suggest caution in overstepping and limiting freedom of expression without using it as a fallback excuse for inaction (as it is often mobilised by tech platforms themselves based on a wilful misreading of the US Constitution). Emphasis is instead placed on taking more seriously the principles of existing privacy regulation such as GDPR to allow for greater regulation. Proper enforcement of existing privacy regulation would go a long way towards limiting harmful or manipulative online content, as many of these harms are based on practices that are fundamentally non-compliant with the law. This includes design as well as default settings, another important focus of regulatory recommendations that take a more holistic approach Costanza-Chock2020 Carmi2020. Increasing the effectiveness of existing privacy and advertising regulation is an important first step in establishing a more integrated regulatory environment for privacy, data and content online.

Awareness and clarity

A persistent issue that is the focus of both existing regulation and recommendations for future policy is an increase in awareness and understanding. For example, the 2019 ICO Update Report into Adtech and Real Time Bidding called for greater understanding by businesses engaged in processing data - particularly its use in targeted advertising - as well as the need for greater clarity and simplicity of privacy terms and other information for users. This shows the importance of greater understanding on all sides of data systems, and the need to remove the obfuscation and mystification that places too much power in the hands of the platforms designing the technologies.

However, it is not simply that the public isn't aware, and certainly not that the public do not care deeply about these issues. The Carnegie UK Trust report Data Privacy From Attitudes to Action provided evidence of the privacy paradox - in which users know the risks and harms but do not necessarily change their behaviours accordingly (from changing privacy settings to choosing which platform to use). This was found even more extremely in recent research HindsWilliams&Joinson2020 that uncovered a pervading attitude of "it wouldn't happen to me" and sense of immunity to targeting even in the wake of the Facebook-Cambridge Analytica scandal. Awareness leading to action is further complicated by a study that showed how viewing news items about surveillance actually led to users creating less secure passwords Mamonov&Koufaris2016. The Carnegie UK Trust report showed the need for greater awareness of both practical and regulatory methods, and a current lack of consensus over terms and definitions. Clarity in platform terminology and regulatory rights are essential for users to convert concern into action, in order to overcome the twin feelings of hopelessness

and invincibility. The Carnegie UK Trust report also highlighted the importance of context, to which we can add the need for tech companies themselves to develop greater understanding of the role they play and the different needs of the different individuals and communities who use their platforms.

One of the main works in identifying and remedying these problems has come from the Me and My Big Data Report 2020. This project emphasises the need for awareness of how the full systems, business models and consent mechanisms of data interact. It details the individual and collective skills required to use, think about and participate with technology, and to support others in our communities. The Me and My Big Data report separates "data doing" digital literacy skills (the more practical behaviours such as using social media and search engines effectively, or adjusting privacy settings) from both "data thinking" and "data participating". These two additional skillsets are of vital importance in promoting awareness and critical thinking about how data is generated, shared and used, as well as how this translates into supporting others and other forms of positive and proactive social and political engagement. This form of data literacy supports individuals and communities.

The project assessed different user groups, highlighting the pre-existing and intersectional disadvantages often at play, such as the combination of lower education and socio-economic position in both younger and older people contributing to disadvantages in access, skills and a supportive community. The findings also emphasised the need for increased awareness about the interconnectedness of systems and issues, and the fact that today people are never fully online or offline but a flexible and shifting mix. This supports the idea of privacy, data and life online as an active and ongoing process that is contextually dependent and in which collective empowerment is key. It suggests the need for broad regulation that acknowledges the reach of online data and content as well as its impact across other areas of society.

Regulation and regulators

To enable and enforce the recommendations required to improve privacy, data and content online, much attention is given to the regulatory environment and the specific regulators involved. This is an increasingly complex area with overlapping priorities and concerns, potentially leaving much to fall through the cracks in terms of enforcing larger scale issues or providing users with clarity on how to resolve problems. A representative view of this landscape is shown in Figure1 - it is non-exhaustive but highlights the key interactions and overlaps of existing regulation:

The most prominent existing regulator in the area so far has been the ICO. But the wider issues and intersecting remits place limits on the effectiveness of regulation. For example, the ICO's Age Appropriate Design: A Code of Practice for Online Services provides a positive example of design-side regulation. But its recommendations push enforcement beyond the limits of ICO. This is a common problem: regulators such as the ICO are doing important work and providing recommendations and best practices on a wide range of interconnected issues, but the enforcement remains lacking as it inherently spans different regulators and large scale coordinated action has not yet been achieved. The current powers and scope are also largely reactive - often requiring a data breach to have occurred. There is more work to do to promote positive interventions to prevent the harms from occurring in the first place, particularly in the case of children. More broadly the use of these clear extra considerations for children could be used to promote better design for all users. There is a clear need to extend these practices to support vulnerable adults and those with accessibility needs, but it should also include ways to avoid e.g. racial or gender discrimination in design. More coordination is needed between regulators to push out better practices and greater understanding of these increasingly complex issues to ensure no communities are being pushed aside by tech companies or forgotten by policy-makers and regulators.

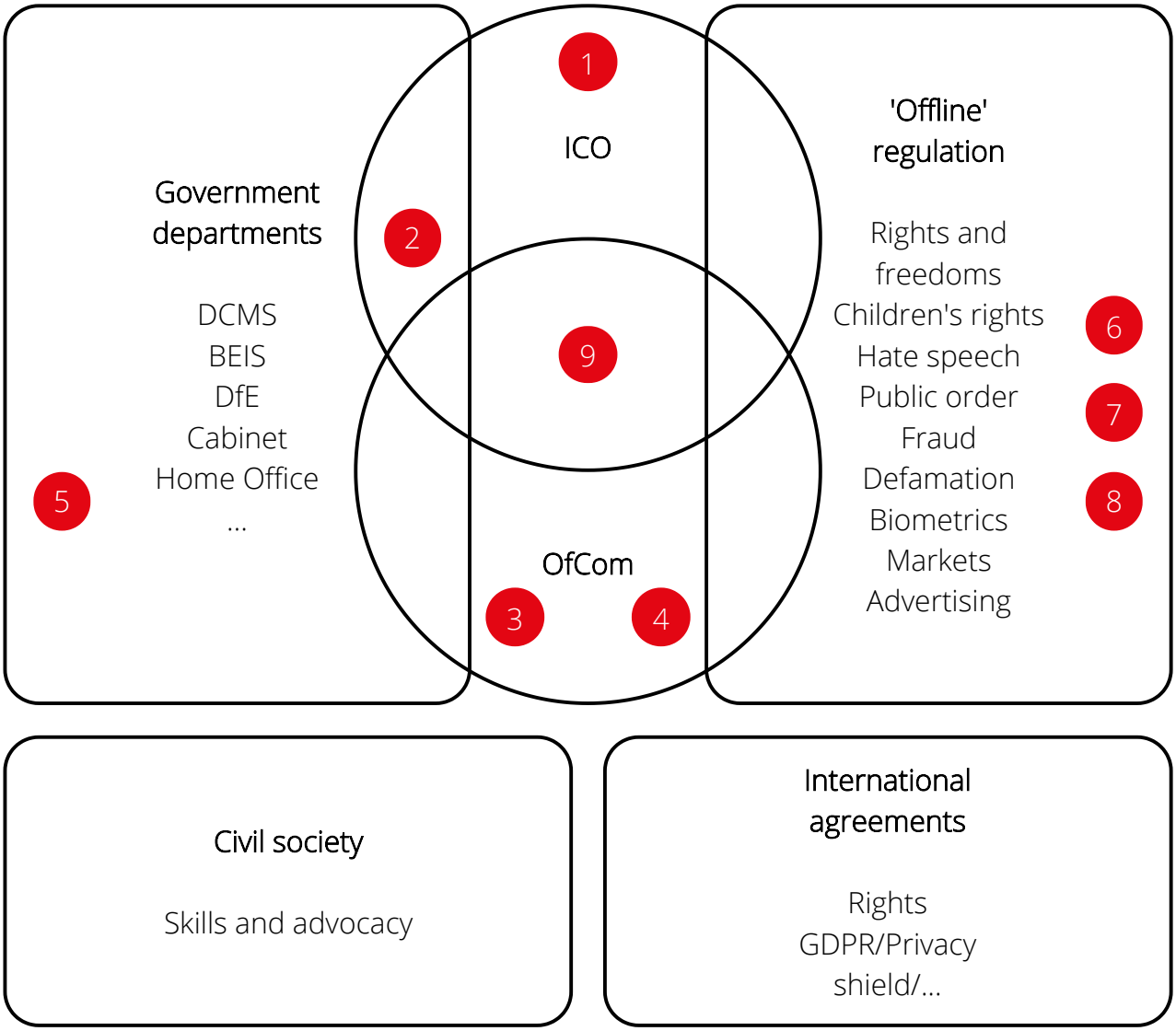


Figure1 : Current regulatory environment for privacy, data and content online.

1. ICO has been main source of regulation of privacy and use of data so far;
2. ICO is separate from but sponsored by DCMS;
3. Calls for regulating tech companies as traditional media companies (Noble&Roberts2017) are echoed in the new powers for OfCom to regulate online harms - but there are also much broader issues at stake;
4. OfCom itself was created as a consolidation of existing related regulators, showing a trend towards regulating more cohesively and at greater scale with greater powers and resources;
5. Many government departments have responsibilities relevant to privacy, data and online content, including DCMS (national data strategy, creative economy), BEIS (skills, economy), DfE (skills and access) and the Cabinet Office (data in government);
6. The Children's Commissioner has also been particularly active in advocating for regulation and public awareness of privacy and use of data, echoing specific additional regulation for children in legislation;
7. Existing non-digital regulation should also apply, though it is seldom exercised in practice - including anti-social behaviour, hate speech, etc.;
8. Facial recognition, while more about privacy than content at the moment, spans other regulators such as the Biometrics Commissioner or the CCTV Commissioner - this applies to targeted content in, for example, public advertising screens like Piccadilly Circus;
9. This is the target area for development - the intersection of privacy and content - it is also the area that draws in many other areas, regulations and departments.

The Online Harms White Paper by DCMS and the Home Office pushes further into inter-departmental regulation of online content, although it remains focused on explicitly political content and advertising. The recommendations align with the extension of OfCom's remit to cover regulation of (some forms of) online content. The White Paper built on research supported by both ICO and OfCom on Internet Users' Experience of Harm Online, highlighting the inter-regulator approach required. The Online Harms White Paper acknowledged the asymmetric power relation between regulators and companies but ascribes this to knowledge of the relevant technologies. This misdirection is furthered by undermining its potential impact by emphasising principles that limit the regulator's powers, such as the "protecting innovation" priority that entrenches tech companies' ability to develop new systems and uses of data always ahead of reactive regulation. However, the White Paper does emphasise the need for increased responsibilities for companies, including embedding processes beyond simply responding to liability or signing up piecemeal to voluntary codes of practice (such as the ICO Age Appropriate Design). But it remains to be seen how the inclusion of this new remit within OfCom, and the significant overlap with ICO, will play out in practice.

Following the Online Harms White Paper, the House of Lords Select Committee on Democracy and Digital Technologies Digital Technology and the Resurrection of Trust provided a wide range of evidence from experts in many related areas, with the main recommendation of implementing the Online Harms Bill quickly and with appropriate powers. The Committee's report gave detailed recommendations on issues of accountability, including audit, transparency, digital democracy and education. Following these recommendations would cement the powers for OfCom for regulating platforms for harmful content, but the definition of these harms remained incredibly vague in the report. We propose instead that the focus on harms is somewhat reactive, and that effective regulation of systemic issues would need a more proactive approach based on core principles such as justice, rights, equity and dignity. An issue raised through the course of the report was that no existing regulator wanted to cover online content within its remit, echoed by the ICO's evidence and response to the Online Harms White Paper which included a suggestion of an inter-regulator committee (in the style of their AI group or existing collaborations between Ombudsman). This would allow cases to be brought from multiple regulators together, which is an essential step in tackling larger issues of content that span the specific remits of different Offices. However, the suggestion (which was emphasised in the House of Lords report) remains largely limited to responding to specific complaints. To tackle the pervasive and systemic issues of platforms, this concept requires pushing further into a more comprehensive coordination of wider regulators (beyond the few involved in a specific case) that is able to also target design-side regulation and education.

An alternative approach to wider coordination of regulation that appears across many policy recommendations is the establishing of a new regulator. While the powers are in practice likely to be added to OfCom, this underpinned the CDEI proposal for a new online harms regulator focused on accountability, transparency and user empowerment. A key mechanism of this regulator would be to use codes of practice in order to stay future proof, while the duties explicitly include protection of privacy and freedom of expression, a remit covering all online content not just advertising, and a coherent landscape with formal coordination. This is a significant commitment to resolving some of the core tensions - mainly negotiating privacy against freedom of expression, and inter-regulator cooperation - while expanding the scope of what is covered. However, these measures will amount to little without adequate powers and resources. This is particularly the case with codes of practice which, while allowing adaptability, have yet to be appropriately enforced. Design-side regulation is a persistent problem, and voluntary codes of practice often leave too much room for interpretation or simply being ignored, particularly by larger organisations with opaque internal review processes.

Nevertheless, while language such as accountability and transparency remain problematic and limited in their assumptions, the aims of regulators are approaching the necessary scope and space in which coordinated improvements can take place.

Other work from outside government pushes this idea even further. Doteveryone's Regulating for Responsible Tech Report proposed an Office for Responsible Technology. This would have an even broader remit, sitting above existing regulators to empower them. The weight such a regulator could carry would enable an even more authoritative voice as both a source of evidence for future policy and research, and as a means to inform the public about the interconnected issues that emerge with new online technologies. It also emphasises accountability, but uses a broad scope to better support the public to find redress by bringing together and further enabling the powers of existing regulators.

Similarly, stemming from the Kinder, Gentler Politics report focused on the impact of online platforms in the democratic process, WebRoots Democracy proposed an Office for Social Media Regulation. While this appears more specific in its guiding issues, the regulator would focus on monitoring the platforms themselves, to take a more active role in promoting robust, clear and anti-discriminatory practices for the mediation of content online, with powers up to and including the ability to suspend platforms. The impact of such a regulator would be far reaching in terms of wider online harms and the availability of meaningful information not only during, for example, elections but across all social media.

These proposals all start from a specific concern - online harm, responsibility, damage to the political process - but the push for wider regulators with more far-reaching powers highlights a common theme: there is a clear need for more cohesive regulation of online platforms, data, privacy and the increasingly broad collection of intersecting rights and dangers.

Political content, political process

Political processes and events are a key point of concern with online content, data and privacy. The Electoral Commission report on the 2019 UK general election found that changes to the way campaigns are being run online present one of the most significant challenges to confidence in the democratic process and outcome of the election - almost one in five were not confident it was well run, often citing media campaign issues as the cause - and raised concerns over transparency of digital campaigns (less than one third of people agreed that they could find out who was responsible for creating a political advert - the Commission warned that these misleading techniques risk undermining trust) as well as online abuse of politicians (also addressed in the WebRoots Democracy report Kinder, Gentler Politics). Recommendations by the Electoral Commission include increased responsibility of campaigns and legislation to support an informed public, as well as protections and support for candidates suffering intimidation or harassment. Responsibility for this last point rests across parties, government and platforms.

The impact of privacy, targeting and quality of content online has far-reaching and important implications for the political process. In 2019, Sophia Ignatidou produced a report for Chatham House on AI-driven Personalization in Digital Media: Political and Societal Implications. There are big issues involving data, tech companies and society, including discrimination, agency, autonomy, identity, and the dignity of individuals and groups. Also important to consider is the more general impact on social cohesion and polarisation, and how we might promote positive and constructive discourse. The report highlights the potential for normative and ethical approaches, for example following established journalistic codes of practice. This adds another justification for regulating online information platforms as media companies. The report raises the importance of taking into account how content is recommended (by, e.g. search engine or social media news feed algorithms) as well as the specific case of

targeted adverts. Ignatidou recommends making personalisation clear across all media, extending the power of OfCom (as is currently happening for online harms), and funding more research into HCI as well as into accountability between platforms, technologies and systems. The report emphasises that this is a global effort that will need coordination not only between UK regulators but with international counterparts. It also adds another voice calling for increased data literacy for citizens, as well as ethics training for engineers of the future.

Similar issues have been identified, and recommendations proposed, by other related bodies and reports. A Law Commission PROJECT, as well as an Electoral Commission REPORT, called for increased transparency through clearer labelling of political ads and the requirement for 'digital imprints' including funding sources. The Privacy International REPORT ON EUROPEAN PARLIAMENT ELECTIONS also emphasised the need for transparency and the importance of language in how a given company defines "social issue-based" advertising. The Coalition for Reform in Political Advertising report ILLEGAL, INDECENT, DISHONEST AND UNTRUTHFUL highlighted the need for greater inter-regulator cooperation in this context. By proposing a "special extension" to the ASA to cover political advertising, the report includes recommendations for the involvement of the Electoral Commission and ICO in some capacity. It also echoes the electoral commission in emphasising the need for political parties to actively engage in improving.

Involvement by political parties includes avoiding the push towards personalisation. A recent REPORT by the ORG highlighted the excessive information that parties hold over the electorate, as well as the lack of meaningful value from personalisation. This reiterates the findings of the STER report on advertising cookies. As a matter if trust and integrity for political organisations, political process and digital society more generally, political parties should urgently take a more active role in demonstrating better practices.

On a related topic, the Demos report WARRING SONGS, on information operations, highlights the reinforcing connections between privacy and security which are particularly important in democratic processes. The report showed the breadth of the threat and the need to look across all different types of information. It also emphasised the need to consider not just untruthful information (fake news or disinformation) but also the manipulation of how truthful content is presented. This can include how partial information is selectively amplified or differently framed to promote a particular political narrative.

Demos identified the use of discrimination, such as Islamaphobia, to mobilise information warfare by exacerbating existing biases through polarisation ad victimisation, leading to the purposeful breakdown in social cohesion. These concerns were echoed in WebRoots Democracy's KINDER GENTLER POLITICS report, which emphasised the need for action to prevent discrimination and the delegitimisation of the political process, leaning on existing anti-social behaviour and abuse legislation. The longer term solutions proposed by Demos combine regulation and platform architectures. This highlights a common theme: the need for urgent meaningful regulation at a necessary scale, as well as intervening to establish more socially positive design-side norms with the platforms themselves.

Contexts and perspectives

An important, and perhaps more difficult, recurrent area of concern is improving representation and inclusion, and acknowledging different contexts and perspectives in regulation and technical systems. This is a deep and systemic issue that requires improvements beyond privacy and content, but it should be central to any policy concerning data and platforms.

The Carnegie UK Trust REPORT highlighted the importance of context. For example, there may be widespread acceptance of data sharing in established contexts such as health or retail loyalty cards, but it is not the case for other areas such as social media or smart meters. This is perhaps due to the perception of those

areas as new and therefore invading once private or personal spaces and activities. It could also be due to perceived automation and disempowerment rather than necessarily a direct result of privacy concerns.

It is possible to build platforms and data systems differently. They can be more inclusive of different communities by, for example, involving different voices in the design process Costanza-Chock2020. This goes beyond consulting user groups in a market research or testing capacity. It involves changing representation in regulators and senior positions of platforms in order to improve agency for marginalised groups. In this regard, the Ada Lovelace project Rethinking Data proposes a method of changing narratives, changing practices and changing regulations together.

To support this, regulation should set up clear contextual boundaries to empower existing communities and the new, potentially fluid, communities that emerge online. Rights, dignity and justice are the guiding principles across the literature in this area. But more systemic change must include a switch from corporate to public interests in the discourses that surround and inform technology and its regulation.

Information platforms are a public service, having largely displaced (and thereby privatised) the role of, for example, public libraries Noble2018. The public service rhetoric appears across government and industry to justify systems (often subsumed within what are in practice largely economic "potential benefits"). But this is seldom carried through in practice at the level of the treatment of users, interface design, structures and architectures or decision-making interests. If technology and data are to benefit society (other than making a few people more wealthy) then it needs to be regulated as such. Social, public and community contexts need to be foregrounded as guiding principles that are followed through with specific interventions and enforcement. Engaging earlier and more deeply with social research into technology will be essential for any overarching regulator.

SURVEY

SURVEY RESULTS

To support the analytical work of the project, we conducted surveys of public opinion relating to privacy, data and online content. Widespread support for regulation would empower policy-makers to make more radical changes, while increased public interest and engagement in these issues would help regulators more effectively promote new practices and greater awareness.

The surveys were conducted online by YouGov Plc. Survey 1 was undertaken between 22nd and 23rd January 2020, with a total sample size of 2,014 adults. Survey 2 was undertaken between 17th and 18th Februrary 2020, with a total sample size of 2,026 adults. The figures have been weighted and are representative of all GB adults (aged 18+).

The purpose of the surveys was in part to gauge public support for regulation of information online, but also to assess perceptions of privacy, online content, platforms and how they are regulated, as well as gauging the importance of underlying principles such as trust.

Survey 1 focused on concern for privacy and content online. This included trust in platforms across core issues, the general state of regulation in the UK, whether platforms and regulation do enough to tackle problems, and how different types of data are used to define what content we see online. It also gauged overall support for increased regulation and controls over, for example, political advertising compared to general content online.

Survey 2 examined issues of identity and agency online. This included how people perceive the influence of information online, how represented people feel in current regulation, how decisions are made about regulation and technology, and how much control they have over information. The survey also asked about broader perceptions of technology and society as well as support for specific regulatory measures.

Full results can be found in the APPENDIX.

KEY OBSERVATIONS

People are more concerned with privacy than with content, and less trusting of platforms with their information than with the content they receive. This could suggest that the already increasing privacy regulations could usefully be leveraged to support more equitable and representative content. People are also more concerned with how their information is used than with sharing it in the first place, which suggests an underlying support for a performative and contextual view of privacy, and a greater role for establishing better systems of data use and platform responsibility.

Across most issues, female respondents were more concerned and less trusting of platforms, and had stronger calls for increased checking of content and regulation of platforms. Similarly, older respondents were less trusting about platforms, although post-millenials (those under 25) were generally less positive than millennials, suggesting a trend towards more critical perspectives for those who have

had to deal with life on social media at a younger age. This trend was echoed in how represented different age groups felt within the tech industry: generally less feeling of representation as respondents got older, except for the under 25 group who felt less represented than their millennial counterparts.

Platforms, trust and influence

Over half of people thought that Google and Facebook are doing too little to protect people's data or combat misinformation. Facebook consistently received the least trust, possibly due to the visibility of the Cambridge Analytica scandal and other privacy and political advertising in the press.

There is a lack of agency for users and citizens when it comes to online platforms. This is particularly strong when it comes to regulation, although fairly even across how it is regulated and who makes decisions about how it is regulated. The same balance exists between how personal data is used and who decides how it is used. However, when it comes to what content we see online, people feel relatively in control of what they see but much less in control of who influences what they see. This is purely based on public perceptions, but it focuses public interest on a need for regulation of how and why specific online content is provided.

There is also a massive disparity between perceived current influence over regulation (tech companies at 78%, users at 33%) and desired influence over regulation (tech companies at 57%, users at 75%) but this is interestingly not a complete swap. People still think that tech companies should have significant influence over regulation, and are only just edged out by UK politicians for desired influence (61% to 57%). However, this still highlights an awareness of massive disparities in current influence over regulation, and the desire for a much more strongly user- and community-focused approach.

Content and responsibility

People are massively in favour of platforms having tighter controls over political adverts and fact-checking political content, but they are also almost equally in favour of platforms regulating and checking any content (though less strongly). Interestingly, this is more pronounced (more overall support and/or stronger support) in social class C2DE compared to ABC1. This was echoed to some extent in respondents from social class C2DE feeling less represented in the tech industry, despite being more supportive of tech companies' influence over content and regulation. Intersectional issues of exclusion should be taken into account, and greater representation promoted in industry.

People placed responsibility for checking the integrity of information online largely on platforms as well as content creators. In the workshop there was some surprise that government responsibility was so low as they receive a lot of pressure to tackle the issue. But the problem of potential censorship was raised, and the results also showed generally high support for regulation. This could be due to the perception that it should be platforms' responsibility, but in the absence of appropriate action on their part the government needs to step in with regulation.

Regulatory measures

Support for specific regulatory action tends towards clear punitive measures such as fines (68% for privacy, 65% for misinformation) but also more extreme measures such as banning platforms (53%) as well as a desire for better complaints procedures (56%). Around half of respondents supported giving users various forms of increased control over their privacy, personalisation and content, and there was also support for regulating platforms in the same way as media companies (51%).

There was some surprise at the workshop at the lack of support for specific user-focused regulation, given the general support for user control. This could highlight the need for

design-side regulation that targets default settings. We suggest that support for increased user agency as a general principle but less so for specific measures shows the need for more design-side regulation of default settings and a shift in the assumptions that platforms make about data collection. This would echo, for example, NCSC's push for SECURE BY DEFAULT with "privacy by default".

Measures receiving less support included those that centralised control over data or content, suggesting a lack of trust in any single place and the need for integrated responses. This calls into question potential support for "data intermediaries", "data trusts" or similar concepts, at least without increasing public awareness and ensuring concrete protections for collective user agency.

Other measures with less support were active interventions in content, making personalisation "opt in" and breaking up big tech companies. This could represent a general acceptance of big tech structures, but given the overwhelming support for generalised increases in regulation across all areas of privacy and content, it more likely highlights the potential gaps in knowledge about how algorithmic recommendations work and how they feed into legislation and business models. A theme at the workshop was the issue of how to read through public opinion data to uncover where understanding was obscured by opaque systems. Public understanding continues to be an important part of any regulator's remit.

Perception

The issue of perception was also raised in terms of the visibility of corporate ethics committees and advisory boards that, while seldom exercising meaningful powers, may give the impression of at least a faster response by platforms than government has been able to provide. A positive example was cited in the DCMS gesture of having an empty nametag for Mark Zuckerberg when Facebook refused to appear for questioning, demonstrating the importance of government challenging platforms in public view.

There were large disparities in how people perceived the effects of online content on identity. People felt that their own identity was not influenced by what they see online (only 15% felt it was), but that other people's identities were (59% thought it was). Similarly, people thought they themselves could identify false (74%) or biased (86%) information online but that others were less likely to be able to (23% and 26%). The impression that users could safely identify biased content even more so than false content echoes the lower level of concern for biased content.

This is particularly worrying given the work of, for example, Demos, in identifying the harmful effects of semi-truthful information that may bypass our assessment of believable content. The disparities in perception were more pronounced in older users, who also perceived identity as less fluid and less active. While a performative framework of privacy and content is a useful analytical tool for all contexts, it is embodied particularly strongly in younger users who are more inclined to embrace such an understanding of the networked self and collective acts on social media.

Potential for online media

Respondents acknowledged the potentially harmful effects of online content to individuals, as well as how these harms might affect different groups in different ways. And yet people were largely still positive about the potential for the Internet. While only 34% believe the Internet encourages democracy, a plurality of 49% think it encourages diversity, and 72% believe it encourages participation. Unsurprisingly, only 25% of respondents felt the Internet currently reduces inequality (though we may question why even that many do), but 50% said that it could be used to reduce inequality. This further supports the strong overall support for regulation to bring out the societal potential for online media.

Overall, while people tended to see privacy and content, and action and decision-making, as separate issues, there was support (67%) for regulating online privacy and content by the

same set of laws and oversight bodies. This perhaps highlights a need for greater understanding of the opaque back-end of how platforms operate in connected ways. But it shows a general awareness of and clear support for the need to tackle online problems more cohesively.

RELATED EVIDENCE

Previous surveys on related topics by other projects and organisations support these findings. For example, the People, Power, Tech 2020 survey by Doteveryone found that only 40% of people were concerned about facial recognition technology, whereas 73% were concerned about disinformation and 84% concerned about children accessing inappropriate content. This supports our findings that differential concerns across related topics could guide the language of regulation. The survey also found that over half (58%) of the public feel the tech sector is regulated too little. Interestingly, 81% of people said the Internet has made life a lot or a little better for 'people like me', but only 58% said it has had a very positive or fairly positive impact on society overall. This highlights the findings from our study of a large disparity in perception of benefits and harms between individuals, other people and society as a whole. Bridging these divides should be an important part of any collective response to the challenges of life online and performing a more positive digital society together.

The recent Polis and the Political Process report by Demos and ORG found that 61% of the UK public thought profiling based on online data should be illegal, and 88% felt that the same rules for political advertising should apply online as offline. Interestingly, 90% of respondents thought information from political campaigns should be verified, but 52% thought authorities shouldn't control what politicians say, which highlights the importance of how the issue is phrased, and the competing and interwoven rhetorics of integrity and censorship. The report found a general lack of worry around political campaigns - not on principle but under the assumption that people can and do make up their own minds. This coincides with the findings of this report that people hold a much high opinion of their own ability to determine the validity of information.

A study by The Guardian and Reveal Reality, tracking a small sample of smartphone users' browsing activities ahead of the 2019 UK general election, highlighted the interconnectedness of news and entertainment practices on social media in how people find, read and share political content and news about politicians. This adds another level of support to treating online platforms as media companies at the intersection of news and entertainment. The study also highlighted casual trolling behaviour between friends to create drama on social media - despite reading balanced news sources - suggesting more attention and action is needed around the contextual boundaries between humour and harm.

A survey by the Coalition for Reform in Political Advertising found that an overwhelming majority (87%) of the UK public want platforms to have a legal requirement to control claims in online targeted ads. This emphasises the need for political discourse as a particularly relevant use case for increased regulation, and a potential area for development of better practices that could be rolled out more widely.

In a health setting, a report by Understanding Patient Data showed that 74% of people thought the public should be involved in NHS decisions about how patient data is used. However, 63% of respondents were unaware that third parties gained access to NHS data. The strong support (82%) for greater transparency is clearly an important step in broadening public understanding of the ways data is collected, shared and used.

The Me and My Big Data PROJECT found that only 54% of people believe it is acceptable for companies to use personal data to personalise their experience of apps and websites. The researchers highlighted how, given the prevailing business models based on this assumption, the finding potentially shows a lack of understanding about how these issues are connected and deeply embedded in our online lives. The project also found that there was increasing distrust of traditional media (82% don't trust offline media) but high UK trust for government. This supports regulation as a key tool for change, as well as showing the need for a clear and cohesive voice from which positive policies and practices can be established. Of particular interest are the Social and Media users and the Limited users groups the project identifies. Echoing the perceptions found in this project, the intersection of very young or old users with lower social class and education presents a significant area of concern for awareness, skills and representation.

Clean Up the Internet released a report on anonymity and social media harms which found that 83% of the British public thinks anonymity makes people ruder online. While anonymity in practice is more complicated, the poll highlights a potential limit of public opinion to guide understanding and instead act as a measure of perception and which areas need greater awareness and increased literacy. But the report also shows the opinions of support for remedial action. For example, a large majority (80%) were found to support large fines for social media companies, while a plurality short of half (43%) supported shutting down such companies for failing to tackle online abuse. Similarly, around half (52%) of the public believe the bosses of social media companies who do not take enough action to combat abuse should face criminal charges, highlighting a general support for accountability of platforms. This was compared to only 17% who opposed the proposal, and support was found to be higher among Conservative voters. The survey found that older respondents support criminal charges more than their younger counterparts whilst women are more supportive of these measures than men. However, as a practical measure this is limited. Issues raised in the workshop included the fact that some types of sites have no clear boss or even address, while many exist outside of UK jurisdiction. There is also the issue for big tech companies of where in a complex corporate structure the blame should lie (including parent companies or national offices), and what loopholes, excuses or scapegoats might be used to defer responsibility.

In the specific case of children receiving harmful content online, the 2020 REPORT of the EU Kids Online project, involving researchers at LSE, found that six different types of harmful content were experienced by an average of 10% of children (age 12-16) at least once a month. The study found that 79% of EU children (age 9-16) know how to change their privacy settings. But the privacy paradox is still there in terms of behaviours following incidents, and only 59% know how to check information they see online. This suggests that using privacy concerns to support better online content could also extend to skills and design - a potential role for UK regulators to push industry to include better informational controls alongside privacy controls in more empowering interfaces. This echoes and furthers the ICO report on age appropriate design.

Similar results can be found across the world. For example, a Consumer Champion SURVEY found that Americans would not be willing to sell their data for profit. 63% (with a relatively even gender split) would never sell their browsing history for profit, while of the 3.5% who would, two thirds were male. This and many other related surveys in the US back up the findings in this report that women tend to show more concern and less trust of technology companies and sharing information online, largely due to widely acknowledged higher rates of abuse towards women online. This echoes WebRoots Democracy's work into online abuse on the basis of gender (including women and trans people), race, religion, disability and other forms of discrimination in the political process.

Another survey from the US, for Columbia Journalism Review, examined views on disinformation. The study found highly polarised and partisan mistrust of different media and news sources, as well as a widely acknowledged impact of social media and disinformation on election outcomes.

More widely, Amnesty International conducted surveys on personal data and regulation of big tech across nine countries (Brazil, Denmark, Egypt, France, Germany, India, Norway, South Africa and the USA). Across these countries, 71% of people worry about how tech companies collect and use their personal data and 77% worry about tech companies profiling users. Brazil, India, USA and SA show the highest level of worry for collection and use of data, and overall privacy is the main cause for concern, closely followed by a loss of control. The main causes of worry for profiling are privacy, influencing political opinions and controlling what people see online (all over 50%). 73% of people in those countries want their governments to do more to regulate tech companies, with most support coming from Brazil, SA and France.

A European Commission review of two years of GDPR has shown problematic disparities in how regulation is enforced, as well as an excessive burden falling on SMEs rather than large platforms. The findings suggest more attention to enforcement and empowerment of regulators is required, as is a more comprehensive set of design-side advice for smaller companies. This was echoed in the workshop, where it was shared that SMEs show a willingness to engage in better practices and often proactively seek advice from government but require more support.

There is increasing evidence that not only is regulation necessary but also holds a high level of support from the public. And these problems are global. There is an opportunity for the UK to lead the way in terms of effective regulation and coordination with overseas counterparts.

KEY ISSUES

KEY ISSUES

Any policy recommendation has limitations, as does public opinion in defining policy. Sometimes this is due to narrow focus, other times due to balancing competing priorities. Sometimes it is a practical decision to make incremental improvements, but sometimes it is simply due to the scale of the issues at hand. These are structural and ingrained, and often predate the Internet. But tackling these problems is an essential part of reducing online harms and ensuring a more equitable, empowering and just digital society.

Underlying inequalities

Online platforms tend to perform, perpetuate and escalate existing inequalities. This is seen across the collection of data about, and the targeting of content to, individuals and groups. It is usually those already marginalised who suffer the most.

This report has already highlighted the important academic work being undertaken on issues of race Benjamin2019, gender DIgnazio&Klein2020 and specific intersectional concerns Noble2018, but the problems are widespread across disability, age, education, social class, region and other divisions of marginalisation. The digital divides are many, with decisions affecting access and education often resulting in the "digital redlining" of marginalised groups Gilliard&Culik2016.

The ICO adtech report found that existing or in-development industry initiatives presented no compelling evidence that they would adequately resolve these underlying issues. This adds further weight to the need for much more extensive external regulation on the design side. Similarly, a NATO STRATCOM Centre of Excellence report on social media companies found the platforms severely wanting when it came to tackling inauthentic behaviour online (such as manipulation-as-a-service providers), with Facebook appearing the worst.

If regulation is to move beyond voluntary self-governing ethics towards data justice and human rights, then these problems need addressing urgently and deeply. 71% of our survey respondents thought that regulation should be based on principles such as equality, rights and justice, carrying the same weight as demonstrable problems that have already occurred. The unchecked development of online platforms has led to massive rights issues, identified throughout the academic research already cited but also in Amnesty International's Surveillance Giants report. Policy-makers need to take these issues seriously, and be prepared to take radical measures, to undo the entrenching of discrimination that currently plagues life online for many people.

The need for design-side regulation

Design is an active process. It is never neutral. Equitable and just design needs to involve affected communities to ensure representation in how socially and politically important systems are constructed Costanza-Chock2020. Design and regulation should centre those most affected by any technology or policy. A limitation of using existing privacy regulation is that it can often be individualising, which is why a performative framework emphasises representation, inclusion and collective action. Life online is relational - it is something that happens in the things we do together - and should be regulated as such to empower all users.

Proposed regulators often have a strong focus on the public finding redress. This is important, but often too late when it comes to the systemic harms to individuals and groups. It also fails to take into account any unknown harms, particularly with the impact of, for example, search engine bias or monopolisation of different data types. And yet public support is strongest for punitive measures. This could be due to a commitment to lack of interference with private companies and what can often be portrayed as prioritising innovation. But it could also be because complaints, fines and bans are the easiest to regulate and most commonly seen in the public eye.

Design-side regulation can be much more difficult, and much more opaque, particularly in the translation of (often textual and wordy) policy recommendations to practical technical and visual design. There is a need to strike a balance between enforceable regulations and voluntary design best practices. Neither on its own will suffice. Regulators must work with industry to develop better practices. But this should not just be limited to prominent figures or senior managers who already hold significant power and tend to embody business interests above all else. The international community of tech workers has been a source of change from within large platforms. Regulators should seek ways to better empower those designing and building systems "on the ground" in terms of whistleblowing but also establishing more positive norms for developing more equitable technology.

There is a role for regulators in interrogating the language used by platforms, as well as the funding streams and lobbying by platforms to manipulate areas of regulation. For example, the flip of how cookies are considered from private (the space of the personal device on which they are stored) to public (and therefore exploitable for extracting data and targeting content) created the basis for targeted advertising Carmi2020. Similarly, IP laws have been repeatedly used to keep the backend of platforms and algorithms opaque not only to users but to regulators.

Technologies change quickly and platforms are often in control of the language used to describe them, thereby shaping public perceptions and the terms of debate. A greater role for regulators on the design side is necessary. For example, consent is an important concept for privacy, and yet often does not translate in practice to a meaningful choice. Current consent mechanisms have been criticised for their "cosmetic treatment" of manipulation Carmi2018 leading to a normative emptiness in failing to improve rights and behaviours Bietti2020. If the Internet is to be an equitable tool for participation in digital society, if platforms are to take on the role of a public service in providing legitimate information, then meaningful choice should always include the right to refusal - we should always have the option to say no without being excluded Cifor&Garcia2019.

A radical proposal by Safiya Noble is the need for an FDA style approval mechanism for algorithms that can cause real harm Noble2020, and when considering the potential for harm this could be very far reaching. This can be extended to bad practices in interface design - the "dark patterns" that not only manipulate users but shift the platform-user relationship from embodying user values to assigning value to users. There is also the need to find new ways to capture the different contexts of how and why information is collected or recommended, taking into account that these may change over time.

Consolidating regulation

There is clear need, across existing policy research and in the public view, for more cohesive regulation of data flows online including privacy and content. But this comes with certain issues. It is difficult to bring together disparate regulations and regulators within ever expanding government bureaucracies. It is particularly difficult to create a new regulator - especially one with the required broad scope and weight of enforcement powers. There are two current main routes to creating a more cohesive regulatory environment:

Combine existing laws/regulators : this has been the trend so far, particularly with OfCom both in its inception and with the new online harms powers. However, regulators often prefer clear existing remits, such as the ASA staying within its clear focus and limits, and thereby avoiding taking on political advertising in a substantial way. Regulators must manage their own explicit mission with the broader principles they are seeking to uphold and the wider issues and interactions with related areas, all while avoiding the perception of seeking to expand their power beyond what policy-makers have approved. Combining regulators risks expanding scope without expanding resources, as has been the fear for the merger of the Biometrics and Surveillance Camera Commissioners. This also highlights the importance of preserving different areas of expertise. For example, in regulating privacy and content it is essential to bring together both the media platform experience of OfCom and the data protection expertise from ICO. Shifting some or all of one regulator's remit onto another risks creating unnecessary hierarchies between bodies that are currently taking steps to work more closely together. There is no clear way to simply add privacy and content powers to a single existing regulator.

Create a new overarching regulator for the Internet : this builds on many existing policy recommendations, acknowledging the need for a wider remit across data, privacy and content. Tackling these intersecting issues that span regulators and the division between them (or potential conflicts) requires careful management. A new umbrella regulator could resolve some of these issues, offer increased coordination and mediation, and fill in some of the gaps between existing regulators. However, creating new regulators often meets resistance from inside government, and we wish to avoid bloating the already complex landscape. Establishing another new regulator with clear powers and scope also leaves the risk of new problems emerging that still fall outside its remit. More flexibility is required.

Given the potential difficulties in drawing responsibilities away from established regulators - particularly considering the potential benefits of leveraging longstanding 'physical world' regulations to tackle digital issues - our recommendations propose a third approach that brings together existing regulators in a more formal way while maintaining the separate expertise and focus areas. This builds on the ICO proposal for legislation around further regulator cooperation, but pushes the concept beyond tackling individual inter-regulator cases towards a more comprehensive platform for tackling systemic issues with platforms online.

Consolidating regulation provides an opportunity to better empower regulators who are currently often under-resourced. For example, the Irish DPA has seen a large rise in staff numbers, and yet still only manages to process around 6% of cases. The European Commission review of the GDPR explicitly includes an action for member states to provide sufficient funding for data regulators. But empowerment is more than financial support. The Irish DPA showed that it had sufficient weight and support (from government and the public) to block a new Facebook dating app launch due to non-compliance with data regulations. Our survey shows that the UK public supports more extreme measures such as these, but we have yet to see regulators use such support to gain suitable empowerment to effect larger scale systemic or preventative change. This includes future-proofing and adapting regulation as well as anticipating new socio-technical developments, which can be addressed by, for example, "sandboxing" extensions of current strategy McDougall2020. Bringing together a wider scope of regulators - as well as perspectives from industry, academia and communities - is essential in this process.

Public awareness

A consistently identified issue is the need to increase public awareness. Its appearance in almost all academic literature and policy recommendations suggests this is not only an important but also a difficult task, made even more so when converting awareness and attitudes into positive behaviours. This is the challenge of a performative framework of

privacy - improving individual actions together in order to establish more positive collective norms.

But this burden should not be placed solely on users. Critical skills are an essential part of digital society and supporting their development and enactment should be built into regulation, particularly in line with the findings of, for example, the Me and My Big Data and EU Kids Online projects. Improving literacies and understanding also includes ensuring that users are advocated for in debates, and that complaints are handled promptly and equitably, so that exercising rights is seen as empowering and effective.

The issue goes even deeper. There are too many shadowy processes, and lack of clarity surrounding complex regulation and complaints procedures. The ICO adtech report shows how few people outside the industry know that real-time bidding exists or how it works, and the findings of this project's survey suggests that the important back-end mechanisms are kept opaque from users, part of the corporate design of platforms. Even where users are aware of and concerned about the issues (particularly surrounding privacy), there remains a lack of clear information and built-in accessible tools- and therefore lack of empowerment - for practical methods.

A discussion that came up in the project workshop focused on the perception of content recommendation algorithms as less biased - on the industry-led marketing that the decisions are based in data and therefore lay claim to objectivity. People rarely actually know what goes on behind the scenes, and may not be able to find out what lies beneath the closely guarded secrets of proprietary algorithms. Public awareness must include broader sociotechnical knowledge of, for example, the business models, and the flows of data and money, that promote content recommendations. There is also the issue that often people may not be aware of - or, worse, may not be able to take - other choices.

As the number of roles that interact with privacy, data, online content, algorithms, advertising or related issues on a regular basis continues to increase, it will become ever more important that these skills are developed throughout society. Reports such as the House of Lords Select Committee often contain detailed proposals for including digital literacy in a range of existing topics (such as computing or relationship education) but more is needed to embed sociotechnical issues within the computing curriculum and education should not stop after school. Existing approaches to adult education also tend to focus on making things clearer to users, further shifting the burden of responsibility away from government and platforms. A suggestion that came out of the workshop was a computing version of what medical, legal and accounting practice have well established: a charter or enforceable code of conduct accompanied by a register from which bad practitioners could be struck off. This would undoubtedly receive significant backlash from the industry, but more radical measures such as this highlight the need to target understanding back from use to design and education in how platforms are built and operated with society at the heart.

There are also problems with perception in multiple directions. Power asymmetries extend to the opacity of systems and business models to the public, often defined by corporate PR rather than revealing sociotechnical realities. SImilarly, within government there is a politics of openness around who decides what is collected or shared (and why), and what is made transparent in government or public data Birchall2018. In the workshop, an issue was raised around a habit in government to assume a certain level of skill or access, which could obscure digital divides that lead to exclusion and marginalisation. Resolving these issues is a continual and non-"solvable" process. The implications of these issues rapidly escalate and intersect. Wider understanding of the connectedness of privacy, data, content, platforms and politics are required at all levels. Online platforms need to be built with user understanding in mind to enable empowerment-by-default.

RECOMMENDATIONS

RECOMMENDATIONS

Built on the findings of this project, we propose the following recommendations for more cohesive and effective regulation of privacy, data and content online. These recommendations include changes to regulation today, changes to the narratives around these issues, and a roadmap or framework for changes over time.

1 Regulate privacy, data and online content together

This report has shown the need for a move towards consolidating the regulation of privacy and online content (including algorithmic curation, misinformation, platform responsibility and tackling hate speech/radicalisation).

We recommend an inter-regulator Office for Digital Society to act as the face of the government's response to these problems, manage cases with overlap or conflict between regulators, and provide a clear voice for guiding policy and industry guidelines.

The Office would draw on a team from across existing regulators - for example, one senior and one junior member seconded from each participating regulator - to ensure an appropriate breadth of expertise and promote skills building through inter-regulator knowledge exchange.

This cements the collaborative work already being done by providing broader coordination and making space for future development. It builds on the ICO proposal for increased cooperation but moves further into a more permanent and inclusive committee of regulators such as ICO, OfCom, CMA, ASA, EHRC, Electoral Commission, Children's Commissioner and others as appropriate.

The Office could be set up informally in the first instance to gather evidence on effectiveness and provide detailed policy recommendations for formalisation.

The permanent Office would not necessarily require regulatory powers of its own. Instead, it would act as a formal "collective mouthpiece" for bringing together the powers of existing regulators to tackle larger, more systemic and cross-regulator cases.

The Office for Digital Society would act as a "one-stop shop" for people and businesses seeking to find out information or make a complaint, directing people to the relevant more specific bodies as appropriate.

With more formal powers, the Office could act as a combined regulator with the power to arbitrate between other bodies, adding to mechanisms of robust oversight for individual regulators and finding a space for voices of unity in policies that balance competing rights or interests.

The Office would also coordinate broader socio-technical research funding by UKRI as well as working with other foundations and funders.

The Office would interface with international regulatory counterparts and industry bodies for cross-jurisdictional rights and platforms. This is particularly important to ensure the existing steps of the GDPR and European cooperation are not lost in future developments of the DPA.

The Office for Digital Society would act as a point of coordination and cohesion in resolving current issues and guiding future regulation.

2 Build regulation on principles linked to rights

Any overarching regulation and regulator must be based on codified principles that empower rights, justice, equity, diversity and dignity - online and offline. These principles are the foundation of research into the societal effects of platforms, and have strong public support as a basis for regulation.

Placing principles first requires deciding what society wants from digital technologies. The Office for Digital Society should establish inclusive methods of debate around future policy (see point 3 on representation).

Building on existing “offline" rights and legislation, the Office membership should include representatives from, for example, the Equality and Human Rights Commission or the Medical Research Council. These could be permanent, associate or temporary assignments depending on the specific focus of a given activity or meeting.

An inclusive approach to rights potentially affected by online media acknowledges the specific and varied aspects and the different expertise and priorities of different regulators.

The Office for Digital Society, bringing together different regulators, would provide a platform for overcoming the conflicts between rights, such as the online harms vs censorship debate, in a way that more directly and restoratively tackles issues such as discrimination.

Robust principles can lead to robust processes of cooperation and oversight to manage conflicting principles and prioritise the public good. The Office for Digital Society should set out these principles and how they link to practical measures, which in turn would establish the terms of reference for independent review.

3 Provide a platform for representation

A key aim for an overarching regulator should be for more inclusive, representative and equitable regulation and policy-making.

The wider remit of the Office for Digital Society should be addressing the power asymmetries of platforms and systems.

The activities of the Office should involve diverse communities and advocates in decision-making, this includes engaging with researchers working on specific relevant inequalities as well as advocacy groups, community leaders and members of the public.

The Office should include guest members from different communities as well as academia, and should consider the use of, for example, citizens’ assemblies. This would help ensure marginalised voices are heard before policies are made, as well as afterwards to uncover issues and inconsistencies in enforcement.

A particular mission of the Office should be regulating and educating to empower political and social participation and inclusion.

This method could include, for example, use of cross-Whitehall groups (x-WH), particularly when developing new policies to tackle specific issues with online platforms, by bringing in expertise from across the civil service. This should include not only different regulators and departments but devolved Parliaments and Assemblies to ensure representation from across the UK.

4 Give regulators meaningful powers and the resources to exercise them

It is essential that regulators are effectively empowered to enforce legislation and rights, including appropriate powers and adequate resources.

Enforcement measures should be sufficient to promote behavioural change (e.g. significant increase in fine size, the ability to ban social media platforms or privacy-invasive products, and links to broader skills and practices).

Appropriate powers may include the ability to break up big tech monopolies where the size of such companies renders them essentially unable to be effectively regulated.

The Office for Digital Society should provide analysis of existing powers of constituent regulators, and provide recommendations for further empowerment to more effectively perform their duties.

Innovation is not an excuse - regulators should be able to interrogate the use of language such as “innovation" for future policies that might allow loopholes of oversight for new and emerging technologies.

The Office should include independent external oversight with real powers, building on inclusive representation (see point 3) by involving experts, advocates and members of affected communities.

Part of supporting regulators is robust and clear funding. The Office should receive additional direct funding to support the work of its constituent regulators and wider research.

Possible sources of funding include sponsorship by the Departments whose remit the Office covers (particularly DCMS, BEIS, Cabinet Office), funds raised by ICO and OfCom fines (although this would have to be balanced with perception of fines for income undermining independence), and direct taxes for platforms, tech companies and political advertising.

Platform tax is a preferred method as it highlights the importance of the issue and establishes a firmer grounding of public good for regulation and research. This reprioritises the emphasis of direct corporate funding of, for example, research by channelling funds through the public Office.

Issues of funding also include the remit of digital procurement across government and other public services such as health or law enforcement. Given the power of platforms, access to data provided by government contracts, and the rise of algorithmic governance, proactive interventions in contracts and the ability to block discriminatory technologies in public services would improve equity and integrity in government systems.

5 Strengthen design-side regulation

To take a more proactive approach, the Office for Digital Society should move collective narratives from protecting towards performing privacy, data and content.

The Office should promote interdisciplinarity in platform design, and provide advice and best practices to companies - particularly SMEs - as well as constructively in the regulation of big tech for societal benefit.

The Office should promote and enforce the most stringent practices as a minimum rather than as an optional extra. For example, age appropriate and accessible design should be applied throughout, and expanded to cover anti-discriminatory design practices for interfaces, databases and platforms.

Design-side regulation should take a more inclusive and proactive approach to, for example, audits. This should include not only access to training data but also to platforms’ audit data as this is another area that entrenches and obscures bias. The full decision-making and technical system should be taken into account.

The Office should provide specific advice to government departments and their own digital teams, to establish better practices within public procurement and raise expectations of public bodies as examples of upholding justice and prioritising the public good.

The Office should also maintain a responsive and active approach to evolving technical and

social systems. This is essential for public scrutiny and to ensure decisions about the future of digital society are made in conjunction with the UK government and public.

6 Promote public understanding

An important activity for the Office for Digital Society is to promote public understanding of issues, of skills, of rights and of methods of collective action. This includes greater critical awareness of how different systems are connected.

The aim should be for all people to be empowered as active participants in life online, for mutual benefit, also supporting point 3 on representation.

The Office will support a comprehensive programme of critical skills across all ages, communities and types of user groups by engaging with researchers and those groups to assess needs.

This programme Includes interventions in education, communities, industry, research and government.

The Office should work with DfE and researchers to include practical understanding of social, economic and political factors within, for example, the secondary computing curriculum.

With its wider remit and scope, the Office would expand existing work for, e.g., children as part of the more comprehensive programme, including filling in the gaps for those who may have so far been excluded from such knowledge and skills.

7 Plan for future development

The speed of new technologies requires regulators to leave room for regular and rapid updating of specific regulations and strategies in conjunction with independent review to respond to new platforms and societal impacts.

The formation of the Office for Digital Society from across existing regulators acknowledges the scale of problems while retaining contextual specificity, and seeks to overcome the limited effectiveness of blanket rules to date.

The Office would work closely with the new Regulatory Horizons Council to identify areas for future reform, including sandboxing possible regulations in conjunction with relevant research, industry and community groups.

The remit for the Office would almost certainly need to expand over time to more explicitly cover data, algorithms, machine learning, artificial intelligence and other related technologies not only online but in wider use.

It is likely that in the near future the Office for Digital Society would need to expand into a full government Department for Digital Society, bringing together the overlapping remits of, for example, DCMS, BEIS and others in a more cohesive way to lead for a more equitable digital future.

CONCLUDING REMARKS

Digital society is not separate from physical society, and regulation should be further integrated with new areas. The issues are embedded throughout our society and require contextual consideration that is regularly reassessed and updated. This report has shown research, policy, and public opinion in support of more cohesive and comprehensive underpinning regulation around the use of data and the Internet. It brings together many existing currents in policy, advocacy and research to support a more cohesive and systemic approach. The report has provided a set of recommendations to enable this and to enhance the work of existing regulators across relevant areas.

Many of the principles and recommendations in this report are also directly applicable to related areas such as machine learning and artificial intelligence. It is anticipated that these areas would also have to be regulated together in the near future. It is anticipated that the Office for Digital Society would provide a blueprint and evidence for such regulation.

Regulating privacy, data, content and platforms more cohesively is about changing the “default settings" of digital society. We can perform the Internet differently together for collective benefit. This is in many ways a drive towards greater access: to skills, to justice, to agency, to communities. New narratives are needed to shift the “default settings" of digital society. Creating a more positive experience of life online and offline - a digital society we can take pride in - requires systems, platforms, policies and regulation that embody:

> Privacy-by-default
> Rights-by-default
> Inclusion-by-default
> Dignity-by-default
> Empowerment-by-default

END MATTER

REFERENCES

Ada Lovelace Institute. 2020. Rethinking Data. Ada Lovelace Institute.

Amnesty International. 2019. New poll reveals 7 in 10 people want governments to regulate Big Tech over personal data fears. Amnesty International.

Amnesty International. 2019. Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights. Amnesty International.

Garfield **Benjamin**. 2020. From protecting to performing privacy. Journal of Sociotechnical Critique 1(1), 1-30.

Ruha **Benjamin**. 2019. Race After Technology: Abolitionist Tools for the New Jim Code. Polity.

Elettra **Bietti**. 2020. Consent as a Free Pass: Platform Power and the Limits of the Informational Turn. Pace Law Review 40(307).

Clare **Birchall**. 2018. Shareveillance: The Dangers of Openly Sharing and Covertly Collecting Data. University of Minnesota Press.

Carolyn **Black**, Lucy **Setterfield** and Rachel **Warren**. 2018. Online Data Privacy from Attitudes to Action: an evidence review. Carnegie UK Trust.

Harry **Brignall**. 2010. Dark Patterns.

Elinor **Carmi**. 2018. Do you agree?: What #MeToo can teach us about digital consent. Open Democracy.

Elinor **Carmi**. 2020. Media Distortions: Understanding the power behind spam, noise and other deviant media. Peter Lang.

CDEI. 2020. Review of online targeting: Final report and recommendations. CDEI.

Marika **Cifor**, Patricia **Garcia**, TL **Cowan**, Jasmine **Rault**, Tonia **Sutherland**, Anita Say **Chan**, Jennifer **Rode**, Anna Lauren **Hoffmann**, Niloufar **Salehi**, Lisa **Nakamura**. 2019. Feminist Data Manifest-No.

Clean Up the Internet. 2020. New opinion poll: 83% of Brits think anonymity makes people ruder online. Clean Up the Internet.

CMA. 2020. Online platforms and digital advertising market study: Appendix H. CMA.

The Coalition for Reform in Political Advertising. 2019. Illegal, Indecent, Dishonest and Untruthful: How Political Advertising in the 2019 General Election let us down. The Coalition for Reform in Political Advertising.

Julie **Cohen**. 2012. Configuring the Networked Self: Law, Code and the Play of Everyday Practice. Yale University Press.

Columbia Journalism Review. 2019. How We See Disinformation. Columbia Journalism Review.

Consumer Chamption. 2016. Would You Sell Your Online Data For Profit? (Survey Results). Consumer Champion.

Sasha **Costanza-Chock**. 2020. Design Justice: Community-Led Practices to Build the Worlds We Need. MIT Press.

DCMS and **Home Office**. 2019. Online Harms White Paper. HM Government.

Sylvie **Delacroix** and Neil **Lawrence**. 2019. Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance. International Data Privacy Law 9(4), 236-252.

Catherine **D'Ignazio** and Lauren **Klein**. 2020. Data Feminism. MIT Press.

Doteveryone. 2018. Regulating for Responsible Technology. Doteveryone.

Doteveryone. 2020. People, Power and Technology: The 2020 Digital Attitudes Report. Doteveryone.

Electoral Commission. 2018. Report: Digital campaigning - increasing transparency for voters. Electoral Commission.

Electoral Commission. 2020. Report overview: 2019 UK Parliamentary general election. Electoral Commission.

European Commission. 2020. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. Communication from the Commission to the European Parliament and the Council.

Oscar **Gandy**. 2017. Surveillance and the Formation of Public Policy. Surveillance & Society 15(1), 158-171.

Chris **Gilliard** and Hugh **Culik**. 2016. Digital Redlining, Access, and Privacy. Common Sense Education.

Mireille **Hildebrandt**. 2019. Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. Theoretical Inquiries in Law 20(1), 83-121.

Joanne Hinds, Emma Williams and Adam Joinson. 2020. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies.

House of Lords Select Committee on Democracy and Digital Technologies Digital Technology and the Resurrection of Trust. 2020. Select Committee on Democracy and Digital Technologies Digital Technology and the Resurrection of Trust Report of Session 2019-21. Parliament UK.

Henrietta Hopkins, Suzannah Kinsella and Anita van Mil. 2020. Foundations of fairness: views on uses of NHS patients' data and NHS operational data. Understanding Patient Data.

ICO. 2019. The Information Commissioner's response to the Department for Digital, Culture, Media & Sport consultation on the Online Harms White Paper. ICO.

ICO. 2019. Update report into adtech and real time bidding. ICO.

ICO. 2020. Age appropriate design: a code of practice for online services. ICO.

Sophia Ignatidou. 2019. AI-driven Personalization in Digital Media: Political and Societal Implications. Chatham House.

Alex Krasodomski-Jones, Josh Smith, Elliot Jones, Ellen Judson and Carl Miller. 2019. Warring Songs: Information Operations in the Digital Age. Demos.

Law Commission and Scottish Law Commission. 2020. Electoral Law: A joint final report. Law Commission.

Stanislav Mamonov and Marios Koufaris. 2016. The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. Journal of Information Privacy and Security 12(2), 56-67.

Simon McDougall. 2020. AI, Research and Regulation. Panel, 8 June 2020. CogX2020.

Me and My Big Data. 2020. Me and My Big Data Report 2020: Understanding citizens' data literacies: thinking, doing & participating with our data. University of Liverpool.

NATO STRATCOM COE. 2019. How Social Media Companies are Failing to Combat Inauthentic Behaviour Online. NATO STRATCOM.

NCSC. 2018. Secure by Default. NCSC.

Helen Nissenbaum. 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

Safiya Noble. 2018. Algorithms of Oppression. NYU Press.

Safiya Noble. 2020. What does 'good' look like in technosociety? Keynote, 8 June 2020. CogX2020.

Safiya Noble and Sarah Roberts. 2017. Engine Failure: Safiya Umoja Noble and Sarah T. Roberts on the Problems of Platform Capitalism. Logic 3 Justice.

Ofcom and ICO. 2018. Internet users' experience of harm online. OfCom.

ORG. 2020. Who do they think we are? Political parties, political profiling, and the law. ORG.

Privacy International. 2019. European Parliament elections – protecting our data to protect us against manipulation. Privacy International.

Privacy International. 2019. Submission to the House of Lords Select Committee on Democracy and Digital Technologies. PI.

David Smahel, Hana Machackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson, Sonia Livingstone and Uwe Hasebrink. 2020. EU Kids Online 2020: Survey results from 19 countries. EU Kids Online.

Josh Smith, Toby O'Brien, Harry Carr, Pascal Crowe and Matthew Rice. 2020. Polis & the Political Process: Mapping public attitudes regarding data driven political campaigning and an exploration of polis as a democratic innovation. Demos and ORG.

STER. 2020. Een Toekomst Zonder Advertentiecookies? STER.

Daniel Susser, Beate Roesslerand Helen Nissenbaum, 2019. Online Manipulation: Hidden Influences in a Digital World. Georgetown Law Technology Review 4(1), 1-45.

Zeynep Tufekci. 2014. Engineering the public: Big data, surveillance and computational politics. First Monday 19(7).

Jim Waterson for The Guardian and Reveal Reality. 2019. Uncovered: reality of how smartphones turned election news into chaos. The Guardian.

WebRoots Democracy. 2018. Kinder, Gentler Politics. WebRoots Democracy.

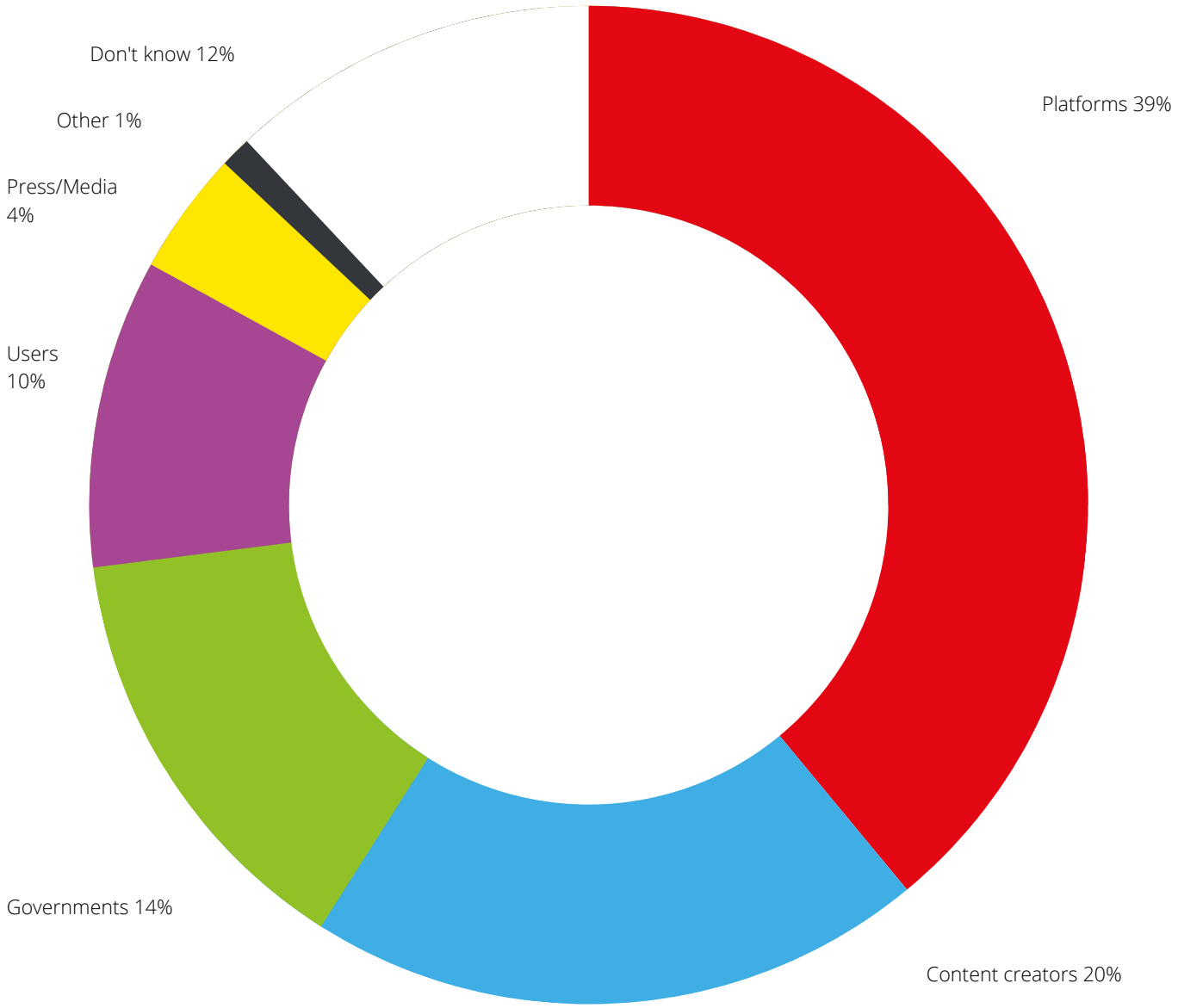
Tal Zarsky. 2006. Online Privacy, Tailoring, and Persuasion. In Katherine J. Strandburg and Daniela Stan Raicu (editors). Privacy and Technologies of Identity: A Cross Disciplinary Conversation. Springer, 209-224.

Shoshanna Zuboff. 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books.

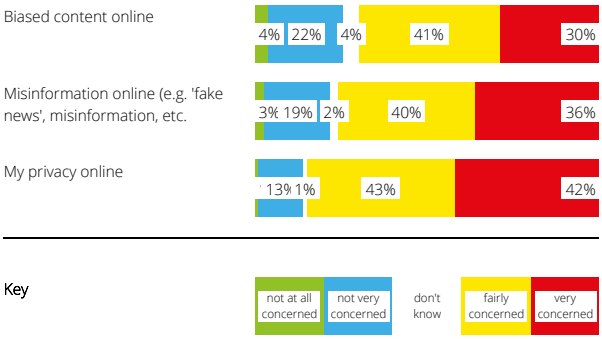
SURVEY 1

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 2,014 adults. Fieldwork was undertaken between 22nd - 23rd January 2020. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18).

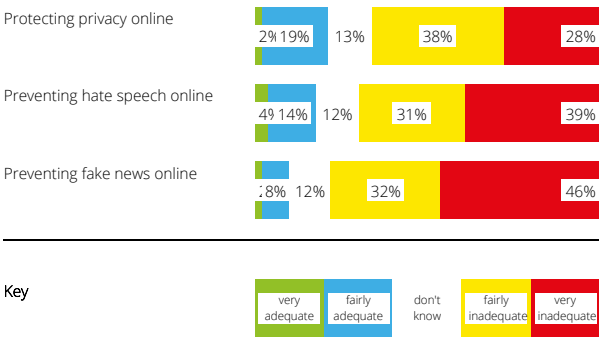
For the following question, by "integrity of information online", we mean ensuring the data is real, accurate and safeguarded from unauthorised users.
In general, whose responsibility do you think it MAINLY is to protect the integrity of information online? (Please select the option that best applies)



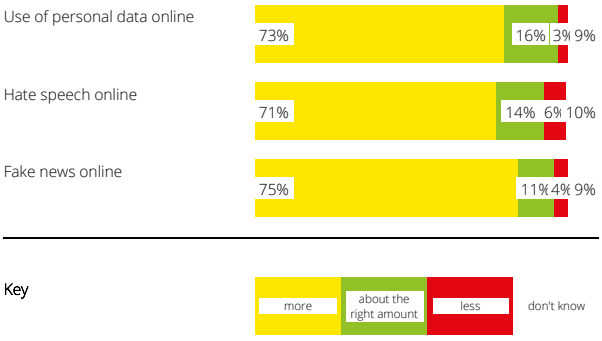
To what extent if at all, would you say you are concerned about each of the following? (Please select one option on each row)



How adequate or inadequate would you say current UK legislation is at addressing each of the following? (Please select one option on each row)

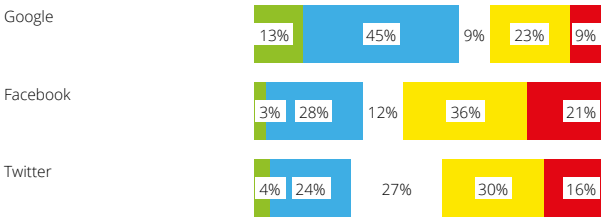


Do you think the following should be more or less tightly regulated by UK law, or is the current level of regulation about right? (Please select one option on each row)

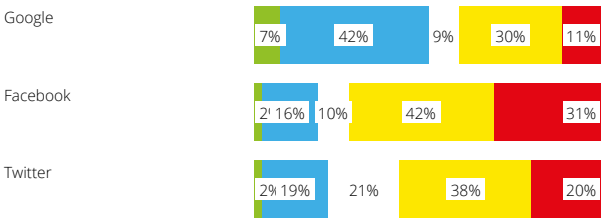


How much, if at all, do you trust the following (Please select one option on each row) ...

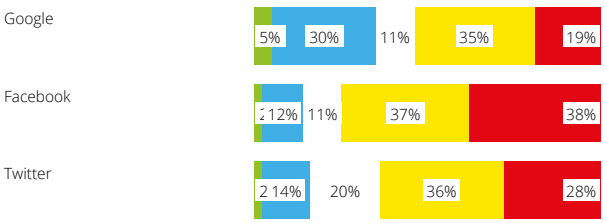
...to provide you with content relevant to you (e.g. search results, news items, adverts, etc.)?



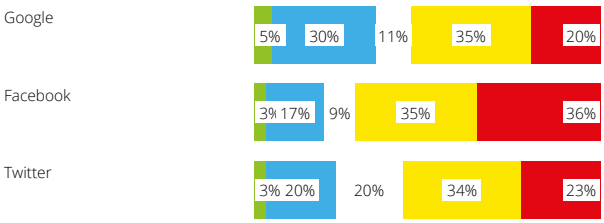
...to provide you with truthful content (e.g. search results, news items, adverts, etc.)?



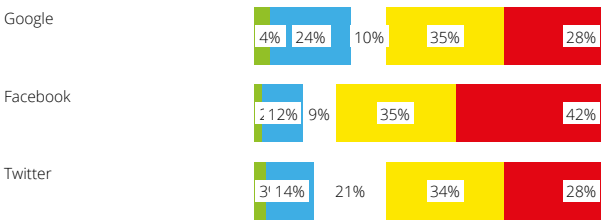
...to provide you with unbiased content (e.g. search results, news items, adverts, etc.)?



...with protecting its users' personal data?

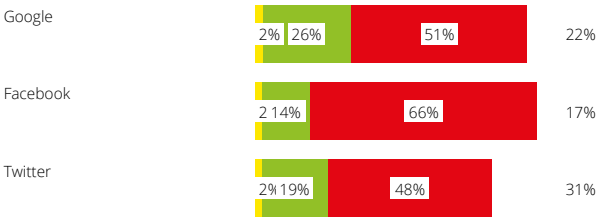


...with how they use personal data (e.g. name, location, search history, images)?

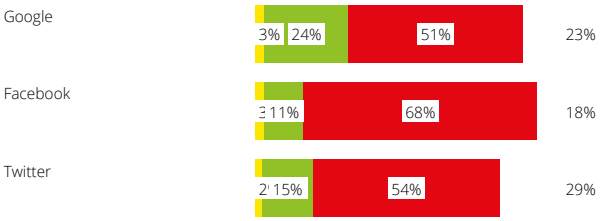


In your opinion, are the following doing too much, too little, or about the right amount to...

...protect their users' personal data (e.g. name, location, search history, images)? (Please select one option on each row)

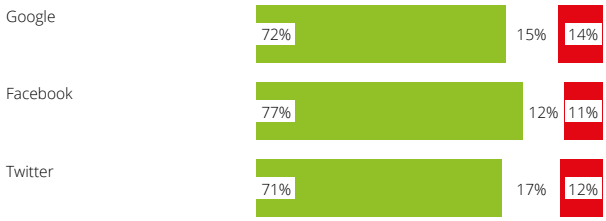


...combat misinformation on their platforms (e.g. fake news, deep fakes, etc.)? (Please select one option on each row)



Key

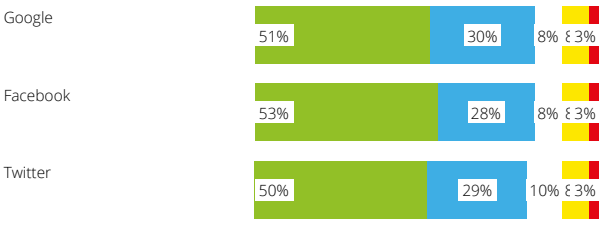
Do you think that the following should have tighter controls over political advertising on their platforms? (Please select one option on each row)



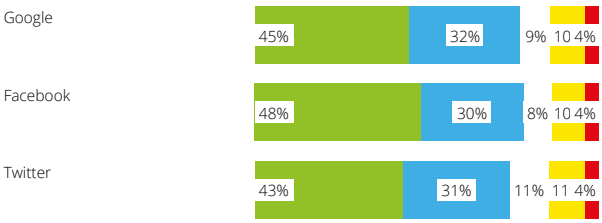
Key

To what extent do you agree or disagree that the following sites should be...

...legally responsible for fact checking political advertising that appears on their platforms? (Please select one option on each row)

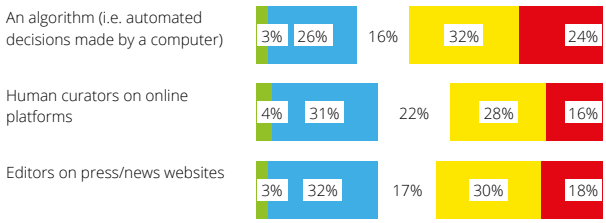


...required by law to to regulate and check ANY content (e.g. posts, news items, adverts, etc.) they provide to their users? (Please select one option on each row)



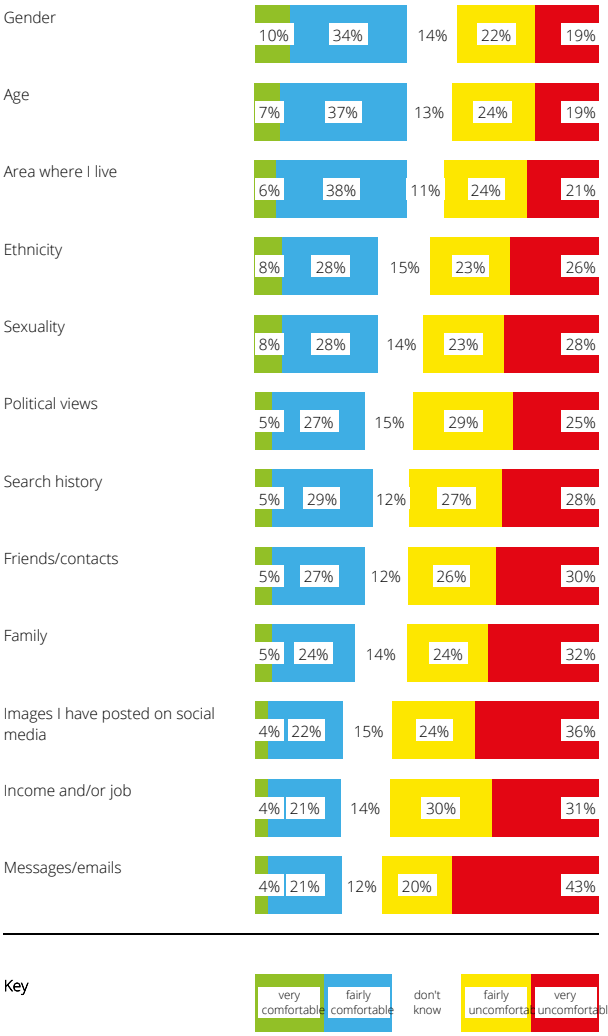
Key

How comfortable or uncomfortable would you say you are with each of the following deciding what content (e.g. search results, news items, adverts, etc.) you see online? (Please select one option on each row)

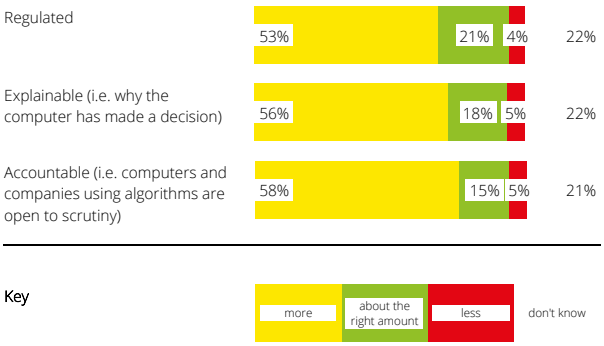


Key

How comfortable or uncomfortable would you say you are with the following information about you deciding what content (e.g. search results, news items, adverts, etc.) you see online? (Please select one option on each row)



Thinking about the use of algorithms (i.e. automated decisions made by a computer) in deciding what online content a person sees...
Do you think the use of algorithms by online platforms should be more or less of each of the following, or is it about the right amount? (Please select one option on each row))

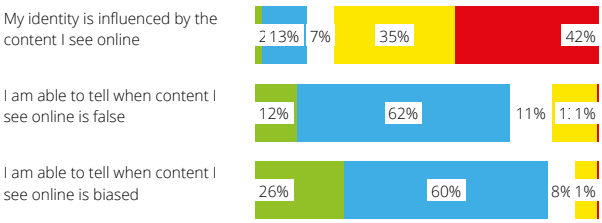


SURVEY 2

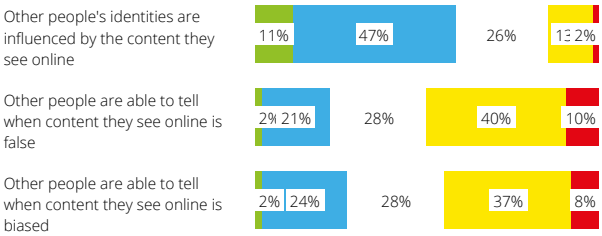
All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 2026 adults. Fieldwork was undertaken between 17th - 18th February 2020. The survey was carried out online. The figures have been weighted and are representative of all GB adults online (aged 18+).

For the following questions, by 'content', we mean any type of text or multimedia content (e.g. news items, articles, social media posts, streamed videos, adverts etc.) you consume online. By 'identity', we mean all aspects that make a person who they are (e.g. characteristics, attitudes, behaviours, etc.).

Thinking generally about yourself...
To what extent do you agree or disagree with each of the following statements? (Please select one option on each row)

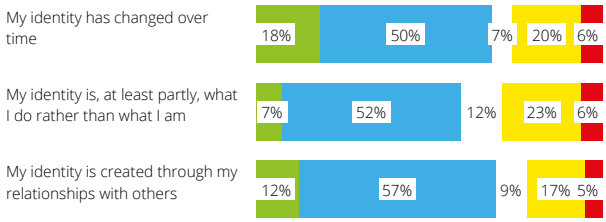


Now thinking generally about other people...
To what extent do you agree or disagree with each of the following statements? (Please select one option on each row)

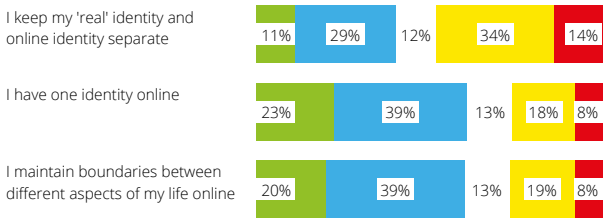


To what extent do you agree or disagree with each of the following statements about...

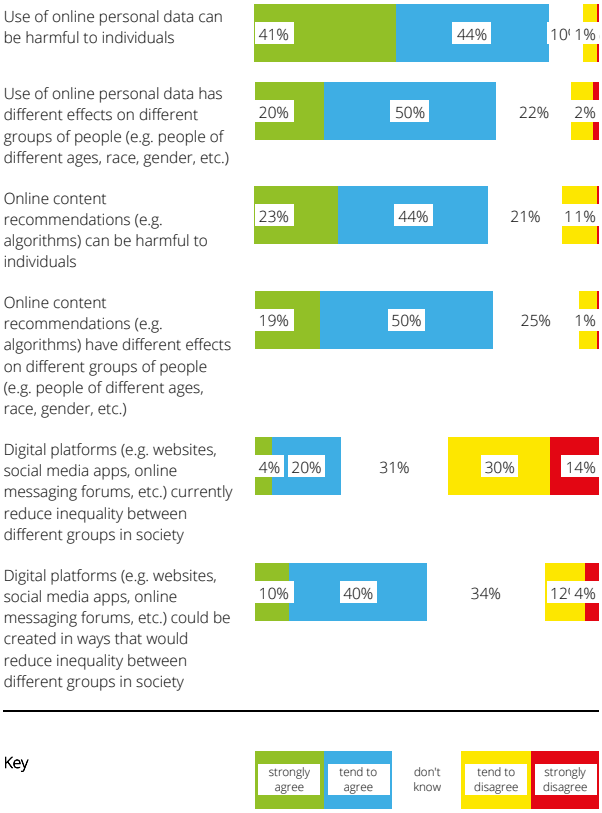
...your identity? (Please select one option on each row)



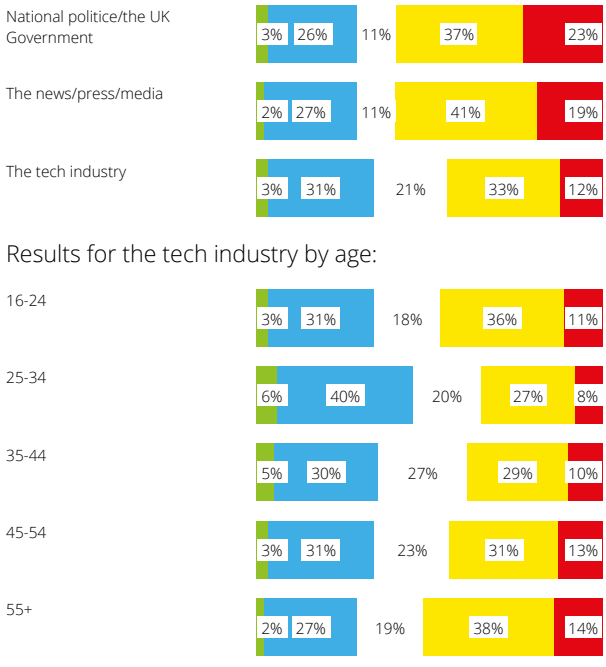
...your online identity? (Please select one option on each row)



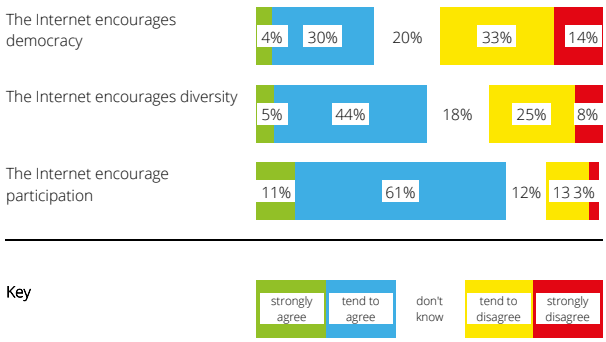
As a reminder, by 'content', we mean any type of text or multimedia content (e.g. news items, articles, social media posts, streamed videos, adverts etc.) you consume online. By 'online personal data', we mean any personal information (e.g. your age, location, ethnicity, income, friends, search history, etc.) collected or stored online. To what extent do you agree or disagree with each of the following statements on how online data is used (e.g. by platforms, governments etc.) and how content is recommended to users? (Please select one option on each row)



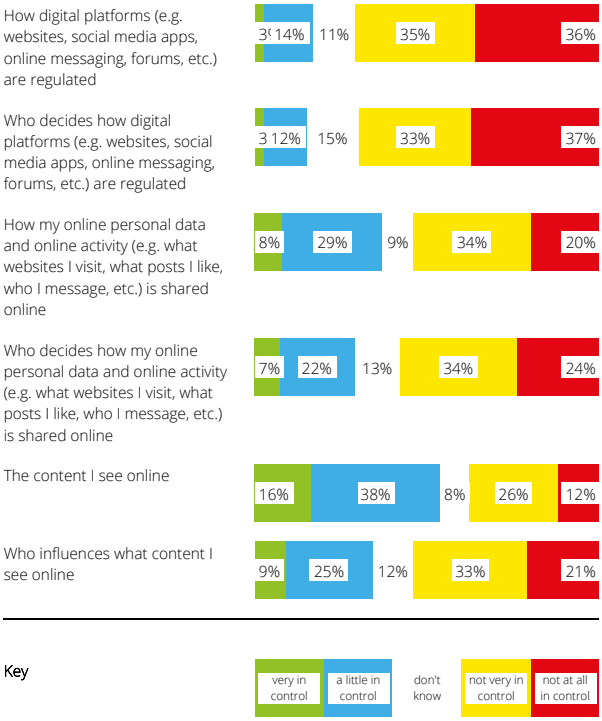
How represented, if at all, do you feel your own opinions and/ or interests are by each of the following? (Please select the option that best applies on each row)



In general, to what extent do you agree or disagree with each of the following statements about the Internet (e.g. websites, content, news articles, search engines, social media, etc.)? (Please select one option on each row)

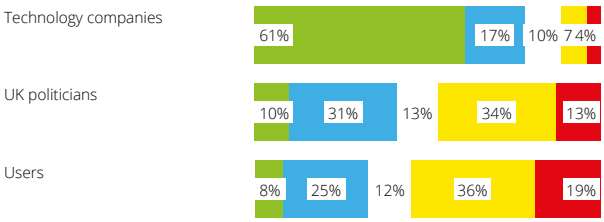


As a reminder, by 'content', we mean any type of text or multimedia content (e.g. news items, articles, social media posts, streamed videos, adverts etc.) you consume online.By 'online personal data', we mean any personal information (e.g. your age, location, ethnicity, income, friends, search history, etc.) collected or stored online. How in control, if at all, do you feel over each of the following? (Please select the option that best applies on each row)

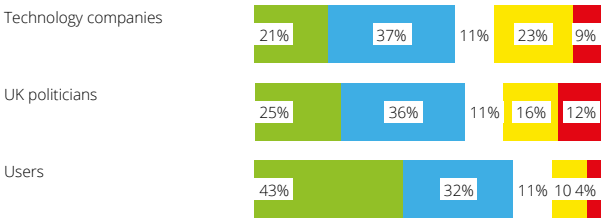


How much influence, if any, do you think each of the following groups...

...CURRENTLY have over the regulation of digital platforms (e.g. websites, social media apps, online messaging, forums, etc.)? (Please select one option on each row)

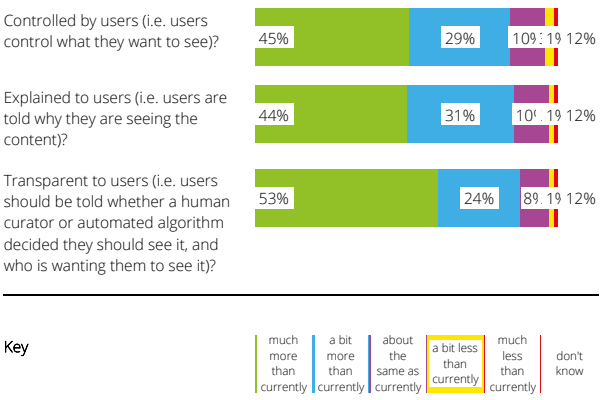


...SHOULD have over the regulation of digital platforms (e.g. websites, social media apps, online messaging, forums, etc.)? (Please select one option on each row)

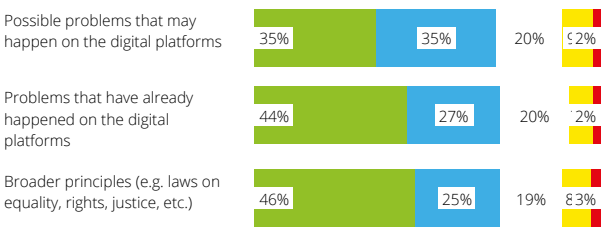


Key

How much more or less do you think the decisions about what content is shown online should be...

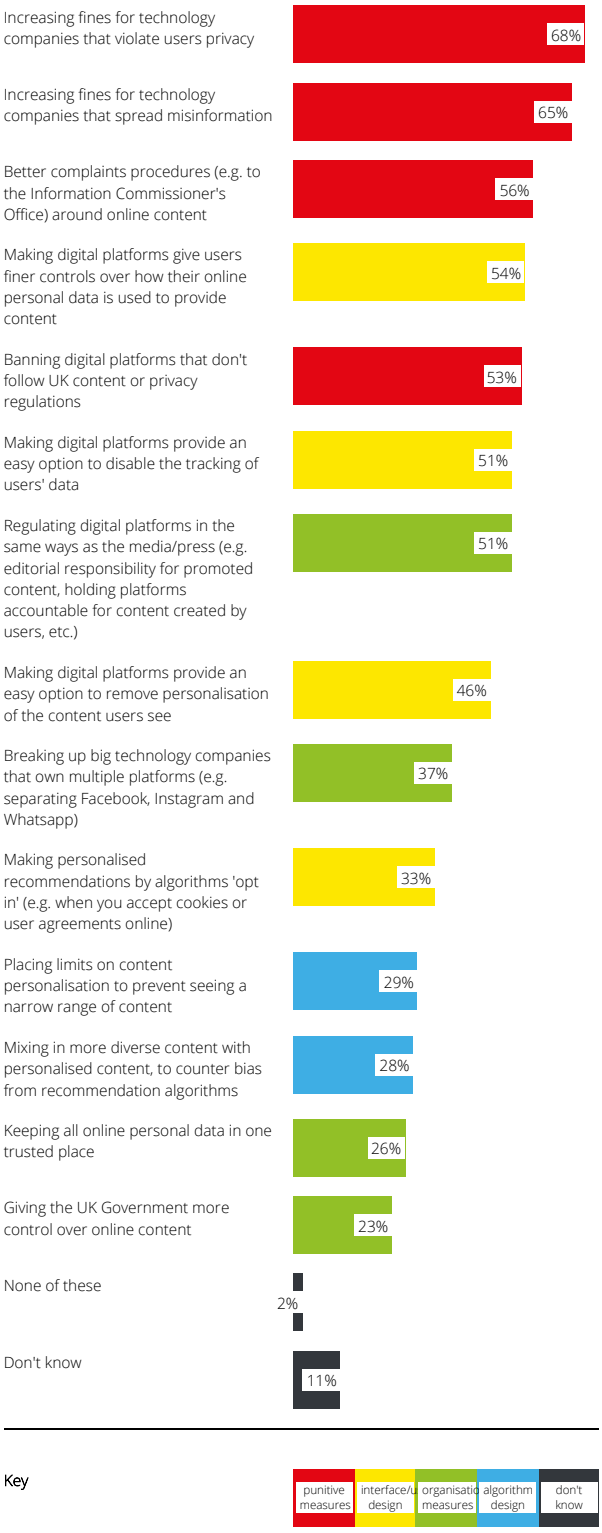


To what extent, if at all, do you think each of the following should be used to decide how digital platforms (e.g. websites, social media apps, online messaging forums, etc.) are regulated? (Please select the option that best applies on each row)

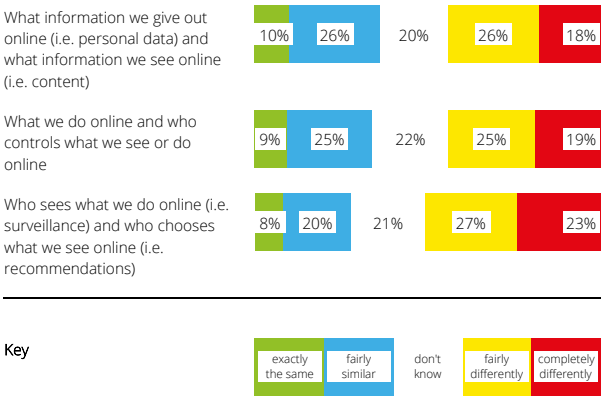


Key

Thinking in general about the regulation of digital platforms (e.g. websites, social media apps, online messaging forums, etc.)....
Which, if any, of the following regulatory measures would you support? (Please select all that apply)



In terms of how we generally think about, interact with and regulate each of the following...
To what extent, do you think each of the following should be treated similarly or differently? (Please select the option that best applies)



Currently, online privacy (i.e. what information users give out) and online content (i.e. what information users receive) are regulated by a mix of different laws and oversight bodies.

To what extent do you support or oppose regulating online privacy and content by the same set of laws and oversight bodies?