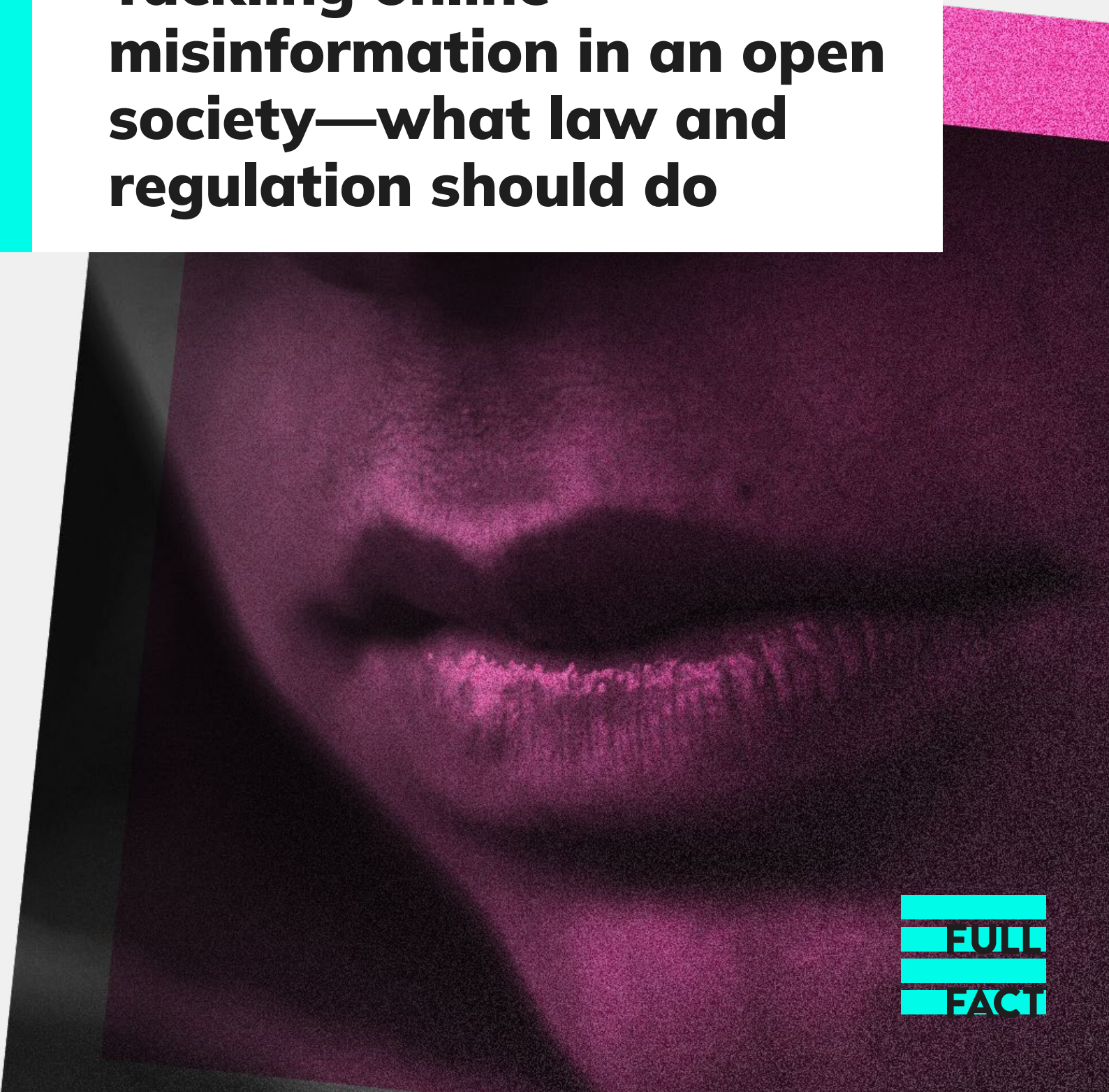
FEBRUARY 2022

Full Fact Report 2022

Tackling online misinformation in an open society—what law and regulation should do



About this report

Full Fact fights bad information. We do this in four main ways. We fact check claims made by politicians, public institutions, in the press and online. We then follow up on these, to stop and reduce the spread of specific claims. We campaign for systems changes to help make bad information rarer and less harmful, and advocate for higher standards in public debate.

This report explores how the online UK information environment can be improved to tackle bad information in the context of the Online Safety Bill and how harmful misinformation can best be addressed under new law and regulation. It follows on from our 2021 report, Fighting a pandemic needs good information[1] which considered how good information, communicated well, can benefit both individuals and society. Our 2020 report, Fighting the causes and consequences of bad information[2], looked at the evidence we had built up over ten years' of Full Fact's work to address misinformation and the harms it poses to democratic society. This 2022 report is the third report that we are able to produce thanks to the support of the Nuffield Foundation.

The Nuffield Foundation is an independent charitable trust with a mission to advance social well-being. It funds research that informs social policy, primarily in Education, Welfare, and Justice. It also funds student programmes that provide opportunities for young people to develop skills in quantitative and scientific methods. The Nuffield Foundation is the founder and co-funder of the Nuffield Council on Bioethics, the Ada Lovelace Institute and the Nuffield Family Justice Observatory. The Foundation has funded this project, but the views expressed are those of the authors and not necessarily the Foundation. Visit www.nuffieldfoundation.org

This report was written by staff at Full Fact and the contents are the responsibility of the Chief Executive. They may or may not reflect the views of members of Full Fact's cross-party Board of Trustees.

We would like to extend our warmest thanks to Peter Cunliffe-Jones, Anand Menon, Gavin Freeguard, Poppy Wood, Jenny Brennan and Mark Franks for their comments on an earlier version of this report.

[1] The Full Fact Report 2021: Fighting a pandemic needs good information, January 2021 https://fullfact.org/about/policy/reports/full-fact-report-2021/

[2] 'The Full Fact Report 2020: Fighting the Causes and Consequences of Bad Information', April 2020 https://fullfact.org/blog/2020/apr/full-fact-report-2020/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

In addition, we thank our other supporters, our trustees and other volunteers of Full Fact. Full details of our funding are available at fullfact.org/about/funding.

We would welcome any thoughts or comments to our Head of Policy and Advocacy and lead author Glen Tarman, at glen.tarman@fullfact.org.

Full Fact, 2022

Nuffield Foundation

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Summary

In the coming weeks the Online Safety Bill will be introduced to Parliament. This is overdue but essential legislation that will impact each one of us. There is only a short window of time to ensure that the Bill effectively addresses online harms, while enhancing our public debate and rights as citizens.

Full Fact exists to fight bad information. For over a decade our team has challenged false and misleading claims, encouraged prominent politicians and the media to correct themselves when they get things wrong, and worked with internet companies to provide good, reliable information on their platforms.

During this time we have seen the harm that online information can do. Bad information has and continues to ruin lives, divide communities and undermine trust in our shared institutions.

The Online Safety Bill is an opportunity to rework the systems that have too often failed in the face of harmful misinformation and disinformation.

MPs in the House of Commons and peers in the House of Lords will soon be examining, discussing and amending the Bill, updated after pre-legislative scrutiny.

In doing so Parliament will finally debate fundamental questions about our online environment in the UK that up until now have effectively been delegated to internet companies without independent scrutiny and transparency. Protection of UK internet users' freedom of expression must rest with the British Parliament rather than be controlled by internet companies overseas.

At present, the draft Bill is a missed opportunity. As the government puts forward further proposals to tackle criminal content and online activity, it must also ensure that the Bill increases democratic scrutiny of the way the internet companies approach their systems and design, and provide better ways to hold them accountable for tackling harm while protecting freedom of expression.

The Bill must have a clearer focus on proportionately but effectively addressing such harm, including that from misinformation and disinformation. That will require:

- a robust and transparent regulatory regime, that expressly recognises both the harms caused by the dissemination of misinformation and disinformation and the importance of protecting freedom of expression;

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

- better promotion of good quality, accurate information and other alternatives to content restriction or 'take down';
- A more proactive role for an independent Ofcom, as both a strategic and a day-to-day regulator with responsibility for identifying and addressing harmful misinformation issues.

Without better, more focused law and regulation, the Online Safety Bill risks continued harms to individuals and communities, undermining public health, and unintentional, long-term damage to public debate. In this report, made possible through the Nuffield Foundation, we set out ten ways that the Online Safety Bill can live up to its promise. We urge the Government and Parliament to deliver legislation in line with these imperatives.

1. **Create stronger media literacy as the first line of defence:** build the resilience to misinformation and disinformation of all UK citizens with media and information literacy at the scale needed
2. **Prioritise promoting good information over restricting content:** restrict information only as a last resort
3. **Make Ofcom responsible for understanding harms caused by misinformation and disinformation:** the regulator should fill knowledge gaps with an enhanced research responsibility and an additional evidence centre should be established
4. **Actively look for harmful information vacuums and fill them:** ensure reliable information from authoritative sources is available
5. **Identify and coordinate responses to information incidents openly:** emergency procedures should be open and transparent
6. **Prioritise tackling specific harmful deceptive behaviour over restricting content:** amend the draft Online Safety Bill to cover regulated content and activity
7. **Make government interventions in content moderation transparent:** limit 'censorship-by-proxy' where government pressures internet companies to restrict content that parliament would not
8. **Require independent testing of algorithms which restrict or promote what people can see and share:** Online Safety Bill should grant Ofcom powers and independent researchers access to algorithms
9. **Secure public confidence in how elections are protected through transparency:** the Online Safety Bill must strengthen democracy and a public protocol put in place for elections

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

10. **Continue to ensure the supply of high quality news:**
    the law should require a minimum supply of high quality news on the largest online internet platforms (Category 1 internet services)

We are all at risk without proportionate action against online harms, and we are all at risk without careful democratic oversight of the government's actions in this area.

Full Fact will scrutinise the updated Online Safety Bill as it progresses through Parliament, and update our recommendations accordingly.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Introduction

Tackling online misinformation in an open society - what law and regulation should do

False and misleading information has circulated online for decades, causing real harms including to public health, public debate and public trust. We have described this in detail in previous reports[3], including the first year of the pandemic which made harmful misinformation apparent to all. Online misinformation is affecting everyone, whether they use social media platforms or not. It has negatively impacted so many people's lives and livelihoods and far too many lives have been lost in some part due to it.

In recent years it has become ever more clear that social media platforms and search engines are part of the problem when it comes to bad information and harms within our information environment. The days of self-regulation are over. The Online Safety Bill in the UK is one result of that.

The UK government, after some delay, finally published the Online Safety Bill in draft form in May last year. The legislation will impose greater regulation on the internet companies in what the Government say will 'make the UK the safest place in the world to be online while defending free expression'.

The Bill covers internet services that offer user-generated content as well as search engines and is intended to make those services safer by placing responsibilities on providers in relation to content that is illegal and/or harmful to children or adults. Misinformation and disinformation largely falls within what the Bill sets out in relation to requirements on what is harmful to adults.

The challenge now is what good law and regulation of social media looks like to address the harms from misinformation and disinformation and how that is brought about, so action is proportionate, and rights to freedom of expression are upheld.

---

[3] Full Fact, 'Tackling Misinformation in an Open Society', 2018 https://fullfact.org/media/uploads/full_fact_tackling_misinformation_in_an_open_society.pdf
'The Full Fact Report 2020: Fighting the Causes and Consequences of Bad Information', April 2020, https://fullfact.org/media/uploads/fullfactreport2020.pdf.
'The Full Fact Report 2021:Fighting a pandemic needs good information', January 2021, https://fullfact.org/media/uploads/full-fact-report-2021.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

The government has stated that disinformation and misinformation that could cause significant harm to an individual are within scope of the duty of care of the Online Safety Bill. It has also been promised that types of disinformation and misinformation are likely to be proposed in secondary legislation as categories of priority harm that companies must address in their terms and conditions.

The legislation will also introduce other provisions to address disinformation and misinformation such as specific transparency requirements and the institutional architecture of the new regime, which will see an expert working group on disinformation and misinformation established as part of the drive to tackle bad information that creates harms.

It isn't possible in a single report to provide a fully comprehensive examination of online misinformation in the UK or to set out all the ways the eventual Online Safety Act should tackle it given the complexity of the draft legislation. As such, in this report we explore a few key areas that are vital for properly addressing bad information now and in years to come.

The extensive material submitted during pre-legislative scrutiny and the growing debate and backdrop of revelations around online misinformation and disinformation have shown just how important this legislation is, but also how critical it is that the UK Government and our lawmakers make changes so that the draft Bill is improved before and during its passage through parliament.

The main objective of this report is to support good outcomes in the Online Safety Bill and its implementation by proposing a set of recommendations to be adopted in law, regulation and practice by policy makers and actors in the new regulatory regime and wider online misinformation policy ecosystem.

This report is published in the light of the Online Safety Bill Joint Committee's scrutiny report on the Bill published on 14 December 2021. Where relevant this report references the Joint Committee's work and recommendations.

This version of the Full Fact Report 2022 is published prior to the updated Online Safety Bill being introduced into Parliament. Soon after the revised Bill is published Full Fact intends to release an updated version of this report.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 1: Create stronger media literacy as the first line of defence

Build the resilience to misinformation and disinformation of all UK citizens with media and information literacy at the scale needed

Recommendation The government and Parliament's ambition for online media literacy in the Online Safety Bill should be strengthened, as a key part of citizen-supporting methods of tackling the problems in our information environment. Greater resources must be leveraged and the regulator Ofcom must massively step up its efforts on citizen media and information literacy.

Address the vast literacy skills and knowledge gap that leaves a population and society at risk of harms in the digital era

Media and information literacy can strengthen the public's defences against the harms of online misinformation and disinformation. Empowering citizens to access, evaluate, and use information critically includes knowledge and technical skills as well as general attitudes needed to recognise reliable information, retrieve it, and produce it in an ethical manner.

Such media and information literacy can make the difference between decisions based on sound evidence, and decisions based on poorly informed opinions that can harm personal health and wellbeing, social cohesion, and democracy.

Yet these competencies are not anywhere near the levels they need to be. In news and current affairs content alone, Full Fact research in 2021 showed one in three UK adults find it difficult to distinguish true information from false information[4]. More widely, Ofcom found 40% of UK adult internet users do not have the skills to critically assess online content. Just 2% of children in the UK have the critical thinking skills needed to tell fact from fiction online[5].

[4] Full Fact, 14 October 2021, UK public as concerned by the spread of misinformation as immigration and Brexit and the EU, https://fullfact.org/blog/2021/oct/uk-public-concerned-spread-misinformation/
[5] National Literacy Trust, 11 June 2018, Fake News and Critical Literacy, https://literacytrust.org.uk/research-services/research-reports/fake-news-and-critical-literacy-final-report/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

This UK media and information literacy deficit is in a context where Ofcom's own research shows misinformation is one of the most prevalent harms experienced by the public[6]. This leaves a population of citizens inadequately protected against the harms of misinformation. However successful the Online Safety Act eventually is in making the UK 'the safest place in the world to be online', the rollout of the new regime is going to take many years.

The Joint Committee on the draft Online Safety Bill notes (paragraph 102) that in removing societal harms from mis- and disinformation from the draft Online Safety Bill (although it had earlier been set out as planned in the White Paper), 'the Government instead aims to tackle the problem of disinformation through strengthened media literacy'. Whilst Full Fact and others want the Online Safety Bill to better address the White Paper's promise of tackling the "harms that have the greatest impact on individuals or wider society", it is clear that media and information literacy should play a very significant role for citizens in the UK. The big question is whether that ambition is set out clearly and can be realised both through the Bill and otherwise.

This matters because a very significant level of online misinformation is inevitable in a globally connected democracy.

Individuals, whilst having a responsibility for their own literacy and in their online actions and behaviours, need an enabling environment where all actors with the power to do so build media and information literacy skills. This should work alongside other efforts to address harmful misinformation and disinformation and the risks to the welfare of citizens, democracy and national security that arise from it. This includes robust law and regulation, government and regulatory commitment, and internet platforms that take on - or are compelled - to play their full part.

Accelerate action on the Online Media Literacy Strategy

The UK Online Media Literacy Strategy[7], published by DCMS in July 2021, rightly gives significant prominence to misinformation and disinformation. It calls information literacy, the subset of media literacy that supports users' critical thinking skills and understanding of how online content is generated the journalistic process,

[6] Ofcom, Pilot Online Harms Survey 2020/21, accessed 31 January 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0014/220622/online-harms-survey-waves-1-4-2021.pdf

[7] The Department for Digital, Culture, Media and Sport, July 2021, Online Media Literacy Strategy, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004233/DCMS_Media_Literacy_Report_Roll_Out_Accessible_PDF.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

'one of the key tools that governments have to tackle misinformation and disinformation'.

As the Online Media Literacy Strategy underlines, research shows UK internet users 'lack the critical thinking skills required to spot online falsehoods' and that there is a clear need to upskill users with information literacy about the real world harm online misinformation and disinformation can have. This has been made even more evident during the pandemic.

Not only is there a pressing need, there is also an unmet demand from citizens. Ipsos MORI and Google research[8] on media literacy related to misinformation and disinformation found that 55% of UK users want to learn more about how to use tools to distinguish between true and false information online. Two-thirds of users believed internet and technology companies should provide training to improve the critical thinking of those using their services.

Building audience resilience to misinformation and disinformation using media literacy as a tool to reduce the harm of misinformation and disinformation is one of six challenges the government has committed to addressing. The Online Media Literacy Strategy sets out important principles to this end, each with actions online platforms can take, as well as the user skills and knowledge needed. Overall, the Online Media Literacy Strategy is relatively strong on diagnoses, but more comprehensive action plans in 2022/23, 2023/24 and beyond are required for its positive elements to be realised and media literacy be an effective tool to reduce the harm of misinformation and disinformation. Without that it will remain weak on cure.

Reflect the need for more and better media literacy than in the draft Online Safety Bill

Given that the purpose of the Online Safety Bill is to make provision about both the regulation of internet companies by Ofcom and the regulator's role in media literacy, the new regime presents a huge opportunity to transform media literacy in the UK in the digital era. At present that ambition is not sufficiently clear.

The draft Online Safety Bill gives Ofcom the power to require service providers to set out (in the new annual transparency reports) what they are doing to improve the media literacy of their users and how they are evaluating the effectiveness of such

[8] IPSOS Mori, 15 March 2021, Online media literacy: Across the world, demand for training is going unmet, https://www.ipsos.com/ipsos-mori/en-uk/online-media-literacy-across-world-demand-training-going-unmet

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

action. Ofcom will also need to publish guidance on how those companies should evaluate any such efforts. Some additional transparency on what platforms are doing, plus this guidance, do not amount to a massive step change and could mean just more of the same: platforms reporting a lot of activity without much evidence that such efforts are solutions commensurate with the problems including in reducing harms from bad information.

The draft Online Safety Bill also requires Ofcom to 'carry out, commission or encourage educational initiatives designed to improve the media literacy of members of the public'. Again, either through its own action, or what it leverages and inspires from others, it is unclear if what Ofcom will do will be of a scale needed and whether it will play its full part including making sure what others do is effective and sufficient.

The Joint Committee has made a number of important recommendations and wider calls on media literacy in its report. This includes that Ofcom 'should require that media literacy is built into risk assessments as a mitigation measure and require service providers to provide evidence of taking this mitigation measure where relevant'[9]. We agree that this should be a requirement not least because service providers have direct access to UK citizens as users of their services, but primarily also as internet companies would need to then deliver literacy efforts at least as a mitigation measure, and preferably more if done well (see also below, including minimum standards).

The Joint Committee also recommends that 'Clause 103(11) is amended to state that Ofcom's media literacy duties relate to "the public" rather than "members of the public"', and that the definition of media literacy is updated to incorporate learning about being a good digital citizen and about platform design, data collection and the business models and operation of digital services more broadly.'[10] Full Fact agrees that the definition of media literacy should be strengthened along these lines. The draft Online Safety Bill definition of media literacy[11] is an improvement on the

[9] Joint Committee on the Draft Online Safety Bill, 14 December 2021, Draft Online Safety Bill, Paragraph 386 Recommendation 96
https://committees.parliament.uk/publications/8206/documents/84092/default/
[10] Joint Committee on the Draft Online Safety Bill, 14 December 2021, Draft Online Safety Bill, Paragraph 388 Recommendation 94
https://committees.parliament.uk/publications/8206/documents/84092/default/
[11] The Department for Digital, Culture, Media and Sport, May 2021, Draft Online Safety Bill, Part 4, Chapter 8,
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Communications Act 2003 and extends Ofcom's remit and duty including around the 'reliability and accuracy' of online material, but can be strengthened further. People in the UK, as elsewhere, are citizens and active communicators, not mere users of services. Understanding how those platforms and services operate is also key to literacy and tackling harmful misinformation (see also an article on this by the LSE's Lee Edwards[12]).

The Joint Committee has also recommended that Ofcom be made responsible for setting minimum standards for media literacy initiatives as part of the UK's media literacy to reduce online harms[13]. We agree that this should be the case for the regulated services. It should be noted, however, that most actors presently working to improve media literacy in the UK are non-profits, many of which are under-resourced, and far too few are working in literacy related to false information.

The Joint Committee has recommended that the Online Safety Bill be updated so that Codes of Practice are binding on providers, and that a Code of Practice on digital literacy be included in a list of Codes put on the face of the Bill. It has also called on Ofcom to start work on this and other Codes of Practice, so they are ready for enforcement as soon as the Bill becomes law. Full Fact supports this recommendation.

The Joint Committee also recommends a 'whole of government' approach to media literacy. The Department for Education has a long way to go on online media literacy including around harmful misinformation and disinformation[14]. In this area, it must also be recognised that the great majority of UK adults are not in formal education. Cross-government action is therefore required. It is also imperative that there is a whole of society approach to harmful misinformation and information and that law and regulation reflects that.

---

[12] Lee Edwards, 9 November 2021, LSE, 'Media literacy in the Online Safety Bill: Sacrificing citizenship for resilience?', https://blogs.lse.ac.uk/medialse/2021/11/09/media-literacy-in-the-online-safety-bill-sacrificing-citizenship-for-resilience/

[13] Joint Committee on the Draft Online Safety Bill, 14 December 2021, Draft Online Safety Bill, Paragraphs 381 and 382, Recommendations 93 and 94 https://committees.parliament.uk/publications/8206/documents/84092/default/

[14] The Department for Digital, Culture, Media and Sport, July 2021, Online Media Literacy Strategy, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004233/DCMS_Media_Literacy_Report_Roll_Out_Accessible_PDF.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Strengthen Ofcom's future role on media literacy as part of a whole of society approach

Will Ofcom's actions, either directly or through leveraging and inspiring others, be of a scale needed? The pandemic has reminded us again that providing good information proactively is an effective way to limit the damage bad information can do. With audiences fragmenting, our public bodies need to gear up to do this at a much larger scale than in the past.

Ofcom does very good work on media literacy[15], yet to date it has been limited in impact. Its research on the state of play and what works is very useful, but Ofcom's direct and indirect action needs to translate into accelerated progress—real world difference—and that means resources and initiatives which move the dial when it comes to online media literacy around misinformation.

Ofcom's media literacy activity is presently focused on generating an evidence base of UK adults' and children's understanding and use of electronic media and sharing that evidence base internally and with external stakeholders. The Bill needs to clarify the extent to which Ofcom's media literacy research should play a role in shaping public policy, or providing other organisations and agencies with evidence to inform their initiatives. That would also make it easier to envisage what will or needs to be different under the eventual Online Safety Act regime.

Ofcom's research must go beyond the state of play to far more of what works and setting out a concrete action agenda. For example, if Ofcom's research released in April this year tells us 24% of UK adults did not consider the potential trustworthiness of online information at all, this is important to know. But even more important would be Ofcom's informed recommendations, for example, about what the internet platforms it will soon regulate could, or indeed should, do to change that, alongside action by others.

There are many areas in the media literacy provisions requiring scrutiny, deliberation and changes on the face of the Online Safety Bill. Overall, the duty to "Promote" and "Improve" media literacy is insufficiently clear about the outcomes being sought, or how they should be measured.

[15] Through its duty to promote media literacy via the 2003 Communications Act, Ofcom established the 'Making Sense of Media' programme to improve coordination within the UK media literacy landscape. Full Fact sits on the advisory panel of this programme.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Without clear ambition from government and authorities such as the regulator it is not apparent what the shared project is. Taking the same Ofcom research figure above, that 24% of UK adults did not consider the potential trustworthiness of online information, what might be the target ambition? Should the UK not have a target that all UK adults consider the trustworthiness of online information by a certain date or is another target level warranted? As things stand, there is no target ambition for a collective effort to help people on this or any other measure.

In December 2021, Ofcom released its new approach to online media literacy[16]. The document details Ofcom's priorities across five pillars. The regulator has a base of work in three of these areas to build on: in research (on the state of media literacy and the evidence base); on engagement with the online media literacy sector across the UK and adding value to it; and, in evaluation where it has attempted to position itself to help those that run media literacy programmes assess effectiveness. Ofcom has identified two further priority areas which are much newer for the regulator: working with platforms and supporting underserved users.

Ofcom intends to establish best practice design principles for media literacy, encouraging platforms to look at how their design affects what their users see and to work around enabling users to control what they see. It sees this work as a prelude to its duties under the eventual Online Safety Act. Of underserved users, Ofcom intends to support the sector by commissioning initiatives to serve those having particular media literacy needs, including on critical thinking online.

Ofcom says it has relaunched its online media literacy programme, 'using our existing powers', with the goal of promoting people's ability to participate effectively and stay safe online. It has set out its priority activities for the next 12 months largely in this frame with some anticipation of its future role. There are a lot of activities underway which may contribute to impact in future, but KPIs and measures of success appear absent.

We would like to see a further relaunch by Ofcom on media literacy in a year's time under the Online Safety Act with the necessary plan of action commensurate with the new role and the challenge of reducing harm from misinformation and disinformation (along with related challenges in its linked and wider literacy remit). In particular, Ofcom's work in relation to online platforms will need to change

[16] Ofcom, 6 December 2021, Ofcom's approach to online media literacy, https://www.ofcom.org.uk/__data/assets/pdf_file/0015/229002/approach-to-online-media-literacy.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

dramatically. The regulator will need to move from a focus on a limited set of outputs to outcomes.

Ofcom's proposed plan of work[17] states that the regulator will deepen organisational preparations for its new regulatory responsibilities as the Online Safety Bill proceeds through parliament as a major focus in 2022/23. By June 2022 Ofcom has said it will publish a document setting out its plans for taking on these new responsibilities. Ofcom's plan should be explicit on how it intends to improve media and information literacy in the UK in relation to building the resilience to misinformation and disinformation of all UK citizens.

Mobilise increased resources for literacy and leverage action from social media platforms

Media literacy needs a very significant uplift in resourcing if need and demand are to be met and swathes of the population not left at unnecessary risks of harm. The current Online Media Literacy Strategy expenditure by the government is not credible. The first year (2021/22) includes an action plan with a budget of just £340,000 - a significant part which is focused on vulnerable internet users and hard-to-reach audiences.

Both Ofcom and government funding for online media literacy need a very significant increase if they are each to fulfil their distinct roles in improving online media literacy. Leveraging or inspiring action by others will not be enough (and must be well resourced in itself), but appropriate investment in online media literacy will enable Ofcom to do what is needed, and will enable whole of society support to develop.

It is difficult to envisage internet platforms playing a full part in media literacy without a clear direction of travel at a national level: of what media literacy levels are being worked towards. The Online Safety Bill and the future annual plans of the Online Media Literacy Strategy could change that. In addition, at present there is very little substance on what Ofcom's guidance on media literacy is likely to mean in practice.

The Online Safety Bill is not currently ambitious enough on media literacy in the digital era. This risks a situation developing where Ofcom has insufficient ambition, will or leverage to actually improve the nation's media, digital and misinformation

[17] Ofcom, 15 December 2021, Ofcom's proposed plan of work 2022/23, https://www.ofcom.org.uk/__data/assets/pdf_file/0023/229640/Consultation-Ofcoms-proposed-plan-of-work-2022-23.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

literacy. Whilst much of this does not need to be in legislation, some changes are warranted to make sure real progress is made over time.

Strengthening media literacy in the Bill would also support freedom of expression by supporting citizens to be part of tackle the problems in our information environment: whether navigating the everyday misinformation that comes with living in a democracy or more harmful misinformation.

Action for government

- Amend the draft Online Safety Bill in line with the Joint Committee recommendations on media literacy.
- In order to ensure progress and accountability, amend the Online Safety Bill to require Ofcom to produce a strategy setting out how it intends to meet its new duty to improve the media literacy of the public (including any steps it will require or recommend service providers to take) and how progress will be measured. The regulator should also be required to publicly report on the progress it makes.
- Increase the resourcing available for online media literacy including digital and information literacy across government departments as well as Ofcom's settlement and ability to raise sufficient funds for improving literacy from regulated service fees.

Action for the regulator Ofcom should accelerate its work in online media literacy commensurate with the extended obligations the Online Safety Bill sets out especially in relation to maximising leverage towards regulated entities on their effective action. Plans should be based on intended outcomes and progress towards better literacy rates including around harmful misinformation and disinformation with commensurate expenditure and revenue raising.

Action for platforms Ahead of and under the new regulatory regime ramp up digital literacy initiatives to UK audiences on owned platforms and beyond based on the latest evidence of what works, sharing further learning with others, and ensuring these efforts are in line with the UK Online Media Literacy Strategy.

Action for civil society Civil society organisations should explore the role they can play in supporting their constituency around online misinformation and literacy related to their mission and press for more and better action by government and others.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 2: Prioritise promoting good information over restricting content

Restrict information only as a last resort

Recommendation The government should: adopt the recommendations of the Joint Committee to strengthen the Online Safety Bill in ways that protect freedom of expression and address harmful misinformation and disinformation through compatible approaches compatible; avoid unintended consequences damaging to freedom of expression around any new false information measures; and, step up efforts (through law, regulation and practice) to ensure users have access to good information.

Make freedom of expression the starting point for any action on a piece of content

An open society should aim to inform people's decisions, not control them. Proportionate action is needed from internet platforms to address clearly identified harms from bad information. But action on specific pieces of content should take freedom of expression as the starting point, and policies addressing harmful misinformation and disinformation should support the right to freedom of expression.

As we said in our 2018 publication Tackling misinformation in an open society[18], 'misinformation and disinformation are sensitive topics intimately connected with individuals' free speech'. With fundamental rights at stake, it is no surprise that free speech has been a key issue in debates about the draft Online Safety Bill. UK legislation is necessary to address bad information and end the era of the internet companies making decisions on online misinformation from offices in California without independent scrutiny and transparency.

We do not believe that an internet company, or anybody else, should take action just because somebody says something which isn't true. Freedom of expression includes the freedom to be wrong. When action is taken on specific content that is both false and harmful or malicious, this should begin with giving users information from non-partisan, authoritative sources that helps them make up their own minds about

[18] Full Fact, 2018, Tackling Misinformation in an Open Society, https://fullfact.org/media/uploads/full_fact_tackling_misinformation_in_an_open_society.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

whether to trust what they are seeing, in preference to more restrictive measures. This is not the status quo, as outlined below.

We believe the Online Safety Bill must be strengthened to include measures that counter dangerous false information, while protecting – and enhancing – freedom of expression. Parliamentarians must be satisfied it does so as the Bill makes its passage towards Royal Assent.

Protect freedom of expression from internet company overreach

Internet companies can overreach on their own initiative in many ways, whether in their policies, by human moderation or in the use of algorithms. A well-known case in point is Facebook's decision to remove posts discussing whether Covid-19 may have come from a lab. This decision was later reversed, because the company would "no longer remove the claim that Covid-19 is man-made" in response to the US government announcing that it was evaluating that possibility.[19]

What is known about the internet companies' choices to restrict information is likely to be the tip of the iceberg. Their decisions can powerfully enhance our ability to impart and receive information, or they can infringe on our freedom of expression. At present, the control of what we see, hear and can say online ultimately rests too often ultimately with companies whose decision-makers are in Silicon Valley.

While companies hide information about the details and tradeoffs of their choices and resist independent evaluation, no parliament should rest easy. The only way to protect freedom of expression from the internet companies themselves is to legislate for oversight of their content moderation choices.

The draft Online Safety Bill, however, appears to let in-scope companies 'mark their own homework' when it comes to adhering to what is required, and this includes how freedom of expression features. Such a system will not work without independent quality control. There needs to be a stronger emphasis on Ofcom being able to set out directions for impact assessments and steps required, along with a duty to comply with any direction from Ofcom. We also believe that the Bill could set out the requirement for proportionate responses more clearly and enforceably.

Critics who think that non-illegal content should not be in the scope of the Bill argue that it would threaten freedom of expression for platforms to take steps to reduce the risks associated with such content when it gives rise to harm. This is a valid concern,

[19] Politico, 27 May 2021, Facebook no longer treating 'man-made' Covid as a crackpot idea, https://www.politico.com/news/2021/05/26/facebook-ban-covid-man-made-491053

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

but staying with the status quo leaves platforms - private corporations - with the responsibility to determine freedom of expression online and leaves harms unaddressed when freedom of expression approaches are available.

Adopt ways of tackling harmful misinformation that leave people free to say what they want

From provision of proactive information (such as the Covid-19 information centres Facebook and others have) to friction-introducing initiatives (such as read-before-you-share prompts introduced by Twitter) and highlighting independent fact checking, there is a growing number of resources and methods that can be used online which mean restricting content should rarely be necessary. We believe that, in principle, these kinds of responses are preferable to those that restrict freedom of expression and are likely to be proportionate in a wider range of circumstances.

The obligation in the draft Online Safety Bill which requires Category 1 service providers to carry out, publish and keep up to date an assessment of the impact of each company's policies on freedom of expression (as well as privacy) is an important requirement. We welcome the fact that details will be publicly available about how a regulated company intends to protect users' right to freedom of expression within the law. We think that this is one area where freedom of expression approaches to harmful false and misleading information could be positively proliferated at a much greater scale than is presently the case.

Build on effective responses to misinformation that respect freedom of expression

There is an existing evidence base which shows that it is possible to balance responses to misinformation and disinformation with protections for freedom of expression. The study that sets this out most comprehensively is the UNESCO and ITU sponsored report Balancing Act: Countering Digital Disinformation while respecting Freedom of Expression[20], which is an action-oriented framework covering the 'life cycle' of online misinformation and disinformation from production to transmission, reception and reproduction.

Not only are freedom of expression approaches available, but there is an evidence base of research that demonstrates such responses to misinformation and

[20] UNESCO, September 2020, Balancing Act: Countering Digital Disinformation while respecting Freedom of Expression, https://en.unesco.org/publications/balanceact

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

disinformation are effective at reducing its harmful effects and spread. Given such responses do not infringe on freedom of expression rights, law, regulation and practice should prioritise them.

A groundbreaking study published in Proceedings of the National Academy of Sciences[21] in 2021 found that, on average, fact checks reduced belief in misinformation. This was true in the UK and all other countries in the research[22]. It showed that people who were presented with fact checks retained factual information for weeks afterwards. And fact checking increased accurate beliefs regardless of political affiliation: a trend that held firm regardless of the topic's political salience (including Covid-19). This study is one of many showing the difference fact checking can make: more people are able to recognise false claims and make decisions based on good, reliable information.

As we set out in Chapter 1, a very significant uplift in online media and information literacy is also required as part of the set of responses.

Many companies that will sit within Category 1 in the UK Online Safety regime are falling far short in their policies and action. A recent open letter to YouTube's CEO Susan Wojcicki from the world's fact-checkers[23] pointed to its status as 'one of the major conduits of online disinformation and misinformation worldwide'. Urging effective action against disinformation and harmful misinformation, over 80 of the world's independent, non-partisan fact-checking organisations (including Full Fact), are calling on YouTube to stop the framing the matter as a false dichotomy of deleting or not deleting content[24]. By doing this, the company is avoiding the possibility of doing what has been proven to work[25]: surfacing fact-checked

[21] Ethan Porter and Thomas J. Wood, 14 September 2021, The global effectiveness of fact-checking: Evidence from simultaneous experiments in Argentina, Nigeria, South Africa, and the United Kingdom, https://www.pnas.org/content/118/37/e2104235118

[22] Full Fact was one of the organisations studied in this research and we cooperated with the researchers on it. The design of the research was pre-registered before analysis was carried out.

[23] Full Fact, 12 January 2022, 80 fact checkers publish open letter to YouTube demanding effective action against disinformation, https://fullfact.org/blog/2022/jan/80-fact-checkers-publish-open-letter-youtube-demanding-effective-action-against-disinformation/

[24] YouTube, 15 August 2021, Perspective: Tackling Misinformation on YouTube, https://blog.youtube/inside-youtube/tackling-misinfo/

[25] Full Fact, November 2019, Fact checking in the 2019 election: research recommendations, https://fullfact.org/media/uploads/election-factcheck-briefing.pdf; Ullrich K. H. Ecker, et al., 2020, The effectiveness of short-format refutational fact-checks, British Journal of Psychology, 111, 36–54, https://bpspsychub.onlinelibrary.wiley.com/doi/pdf/10.1111/bjop.12383; Rebecca K Helm and Hitoshi Nasu, June 2021, Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation, Human Rights Law Review, 21(2), 302–328, https://doi.org/10.1093/hrlr/ngaa060

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

information is more effective than deleting content and it also preserves freedom of expression while acknowledging the need for additional information to mitigate the risks of harm to life, health, safety and democratic processes.

Beyond any necessity to remove content for legal compliance there are often ways to provide context, debunks and other techniques to provide good information in response to harmful misinformation. This is not to argue that good information alone will be enough. As in the YouTube example above, fact checkers also propose other accompanying solutions to reduce the dissemination of disinformation and misinformation: from meaningful transparency about disinformation on a platform; support for independent research; and the publication of a moderation policy on disinformation and misinformation, including the use of artificial intelligence (see also Chapter 8). Platforms and users should not be profiting from promoting disinformation and misinformation that could cause harm.

We welcome the Joint Committee's recommendation that Ofcom be required to issue a mandatory code of practice to service providers on how they reduce harm, including from disinformation. Such a code should include use of fact checking in proportion to reach and risk, along with other forms of mitigation compatible with freedom of expression that should be part of that code, including user control over their curation and better human moderation.

Through adopting this in the Online Safety Bill, the government can place Ofcom in a better place to address harmful misinformation and disinformation by promoting proven interventions that qualify online speech but do not restrict it.

Responses to harmful misinformation and disinformation must be proportionate

In line with the European Convention on Human Rights (ECHR) and Article 10 of the Human Rights Act (1998)[26], legislative and regulatory responses to harmful false and misleading information online should only impinge on or limit freedom of expression in certain circumstances and, even when the situation can justify such an intervention, that right should only be interfered with in a narrowly-defined, necessary, proportionate and time limited way[27]. This and other international human

[26] UK Government, 1998, Human Rights Act 1998, https://www.legislation.gov.uk/ukpga/1998/42/schedule/1
[27] Equality and Human Rights Commission, 3 June 2021, Article 10: Freedom of expression https://www.equalityhumanrights.com/en/human-rights-act/article-10-freedom-expression

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

rights instruments the UK has signed up to should protect the right of everyone in the country to freedom of expression and information.

The government has said that it 'recognises that any legislation addressing user-generated content has the potential to affect users' freedom of expression', and as a result, has put in place 'safeguards to ensure that service providers are required to interpret their duties in a way that minimises any interference with their users' right to freedom of expression'.[28]

Under the draft Online Safety Bill, all in-scope service providers must take into account the need to protect freedom of expression when they decide on and implement their safety policies and procedures. In addition, Ofcom has to ensure that all its codes of practice protect the right of users and interested persons to freedom of expression and include in them the steps that regulated companies must take to comply with their safety duties.

Notwithstanding the fact that the Human Right Act only imposes obligations in relation to freedom of expression on public bodies, and private companies are free to decide what content should and should not be on their platforms, the draft Online Safety Bill does require user-to-user services to have regard to freedom of expression. We believe that it flows from this that platforms will need to prioritise promoting good information over restricting content as one of the best ways of mitigating harms and risks. A related method is for service providers to take part in identifying and filling information vacuums (covered in Chapter 3).

The Joint Committee noted that 'the provisions in the draft Bill on content that is harmful to adults could have a "chilling effect" on freedom of expression and give too much power to service providers'. It has recommended that Clause 11 of the draft Bill be removed for a 'statutory requirement on providers to have in place proportionate systems and processes to identify and mitigate reasonably foreseeable risks of harm', among other measures to make this work effectively. The Joint Committee also sees this as a way to be clearer about the 'legitimate grounds for interference in freedom of expression'. It further calls for the objective to safeguard freedom of expression to be one of Bill's core objectives at the start of the Bill.

Full Fact is largely supportive of the Joint Committee's report and its recommendations. However, we do not think the recommendations go far enough in this space. The increasing importance of this issue means that the Bill that returns to

[28] Minister for Technology and the Digital Economy, Chris Philp, 13 October 2021, Written evidence https://committees.parliament.uk/writtenevidence/41326/pdf/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Parliament should be recalibrated so that it has, more clearly at the core of its objectives, a focus on countering the harms arising from the dissemination of misinformation and disinformation online while protecting freedom of expression. We look forward to considering the Government's response in this area and what improvements may have been made when the Bill is introduced to Parliament.

In its report The Draft Online Safety Bill and the legal but harmful debate[29], the House of Commons Digital, Culture, Media and Sport Committee recommended the Bill should include a 'non-exhaustive, illustrative lists of preventative and remedial measures beyond takedowns... proportionate to the risk and severity of harm, to reflect a structured approach to content. This could include tagging or labelling, covering, redacting, factchecking, deprioritising, nudging, promoting counter speech, restricting or disabling specific engagement and/or promotional functionalities (such as likes and intra- and cross-platform sharing) and so on' (Recommendation 9, Paragraph 21). Defining a list of approaches like this in the primary legislation may be difficult, and flexibility is important, but we agree with the Committee's point that there is a need to more fully embed a focus on measures beyond simply taking down content in this way.

We are also concerned about the Law Commission's proposed new anti-harassment offence of sending knowingly false communications which intentionally cause non-trivial emotional, psychological, or physical harm. The false communications offence may work in specific cases of harassment but we cannot see how this vague definition can work at internet scale.. We set out our concerns in evidence to the Law Commission consultation on the proposed changes to communications offences[30], including that it will encourage inappropriate takedowns of content. In February, the government confirmed it will be accepting the recommended false communications offence as laid out by the Law Commission and will bring it into law through the Online Safety Bill.[31]

Any UK vision for reducing the harms of misinformation and disinformation must be based on the promotion of pluralism of information and opinion, and open and

[29] House of Commons Digital, Culture, Media and Sport Committee, January 2022, The Draft Online Safety Bill and the legal but harmful debate, https://committees.parliament.uk/publications/8609/documents/86961/default/

[30] Full Fact, January 2021, Full Fact - response to the consultation on communications offences, https://fullfact.org/media/uploads/full_fact_for_the_law_commission.pdf

[31] House of Commons Written Statement, Update on the Law Commission's Review of Modernising Communications Offences Statement, 4 February 2022

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

ongoing debate on online policy. Everyone should be able to access reliable, credible, independently verifiable information. Facts matter, and with them people can make their own decisions for themselves, for those around them and for wider society.

Action for government: Ensure the Online Safety Bill is amended and strengthened, taking into account the recommendations of the Joint Committee, to ensure that the Bill has, more clearly at the core of its objectives, a focus on countering the harms arising from misinformation and disinformation while protecting freedom of expression.

Carefully consider whether the Law Commission's proposed offence of sending knowingly false communications can work effectively at internet scale.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 3: Make Ofcom responsible for understanding harms caused by misinformation and disinformation

The regulator should fill knowledge gaps with an enhanced research responsibility and an additional evidence centre should be established

Recommendation The Online Safety Bill should be amended to give Ofcom a responsibility for researching the harms caused by misinformation and disinformation. The powers of the advisory committee on disinformation and misinformation should be amended for it to advise Ofcom on such research. Ofcom and the Department for Digital, Culture, Media and Sport (DCMS) should also explore establishing an independent evidence centre on online harms.

Ofcom must be granted a remit to research harms caused by misinformation and disinformation

To be able to implement and regulate the new Online Safety regime in a proportionate, risk-based way, Ofcom requires the best possible evidence and intelligence.

Several initiatives are already underway (or proposed) within government to improve evidence on online harms in general and on misinformation and disinformation specifically. These include:

- The Online Safety Data Initiative: a project 'designed to test methodologies to facilitate better access to higher quality data to support the development of technology to identify and remove harmful and illegal content from the internet'. It is led by a consortium of experts from government, the Online Safety Tech Industry Association (OSTIA), Faculty Science, and PUBLIC[32],

[32] The Department for Digital, Culture, Media and Sport, About the Online Safety Data Initiative, Online Safety Data Initiative blog, accessed 8 December 2021, https://onlinesafetydata.blog.gov.uk/about-us/

A registered charity (no. 1158683) and a non-profit company (no. 6975984) limited by guarantee and registered in England and Wales

overseen by the Online Harms Expert Group, and convened by the Centre for Data Ethics and Innovation.[33]

- Research by DCMS on online harms.[34] The Impact Assessment published alongside the Draft Online Safety Bill says 'DCMS is funding a two stage project investigating the feasibility of research to assess the drivers and impact of online harms and then leading to specific research to assess child online safety and online abuse (including anonymous abuse) in more detail'. This aims to provide Ofcom with 'a more robust evidence baseline of online harms' to support its implementation of the regime.[35]
- The Counter-Disinformation Data Platform, led by DCMS, which 'will develop universal taxonomies for online harms data which should improve the evidence base in the future'.[36] It 'seeks to improve the government's sharing and analysis of data to build a deeper understanding of disinformation and related risks to the information environment, supporting the development of future responses'[37] and 'create a commonly understood information picture of disinformation'.[38]
- The Draft Online Safety Bill proposes requiring Ofcom to arrange for research into UK users' opinions and experiences of regulated services, including how

[33] The Department for Digital, Culture, Media and Sport, 2 July 2021, CDEI convenes expert group to advise on Online Safety Data Initiative project, Online Safety Data Initiative blog, https://onlinesafetydata.blog.gov.uk/2021/07/02/cdei-convenes-expert-group-to-advise-on-online-safety-data-initiative-project/

[34] The Department for Digital, Culture, Media and Sport, 26 June 2019, Online harms research publications, https://www.gov.uk/government/collections/online-harms-research-publications

[35] The Department for Digital, Culture, Media and Sport, May 2021, Draft Online Safety Bill, Impact Assessment, Paragraph 54 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985283/Draft_Online_Safety_Bill_-_Impact_Assessment_Web_Accessible.pdf

[36] The Department for Digital, Culture, Media and Sport, May 2021, Draft Online Safety Bill, Impact Assessment, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985283/Draft_Online_Safety_Bill_-_Impact_Assessment_Web_Accessible.pdf

[37] HM Treasury, 27 October 2021, Shared Outcomes Fund Round 2: Pilot Project Summaries, https://www.gov.uk/government/publications/shared-outcomes-fund-round-two

[38] The Department for Digital, Culture, Media and Sport, 26 August 2021, *C*ounter Disinformation Data Platform Digital /Technical Project Management Team, Digital Marketplace, https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/15487?utm_id=20210827

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

their complaints are handled, and to publish a statement about this in their annual report.[39]

These initiatives show that the government is aware of the importance of further research on (and coordination in tackling) online harms. But it is vital that such research is brought together and continues at a time when online technology and our understanding of online harms is fast-evolving. Research must be developed in a sustainable way that can be of practical, operational use to Ofcom and other regulators and actors in the UK working to address harmful misinformation and disinformation, as well as international partners, particularly in other democracies.

The Online Safety Bill should therefore be amended to place a new duty on Ofcom to lead, publish and support research on online harms, and in particular the harms caused by misinformation and disinformation (Ofcom already has a responsibility to undertake consumer research under the Communications Act 2003). The wording on Ofcom's powers to gather information (from clause 70) could be clarified and strengthened to support this.

But this is no substitute for the need for Ofcom to be able to request and access information relevant to their research regularly and frequently, in real time where necessary. The wording should ensure Ofcom can work in partnership with other bodies, including other regulators: its chief executive has told parliament that Ofcom would be keen to work with partners, including other regulators in the Digital Regulation Cooperation Forum.[40]

The government also needs to ensure that Ofcom has sufficient funding and flexibility to build on its existing world class research capability and recruit the necessary people and skills to fulfil these new functions. Ofcom should be able to undertake, share and support research based on its own assessment and in consultation with others on what is needed to build the evidence base.

The advisory committee on disinformation and misinformation should be given a role in harms research

The draft Online Safety Bill creates a new advisory committee on disinformation and misinformation (clause 98). Its chair would be selected by Ofcom, and its members drawn from three groups: those representing providers of regulated services, those

[39] The Department for Digital, Culture, Media and Sport, May 2021, Draft Online Safety Bill, Clause 99, https://www.gov.uk/government/publications/draft-online-safety-bill
[40] Ofcom, 1 November 2021, oral evidence to the Joint Committee on the Draft Online Safety Bill, https://committees.parliament.uk/oralevidence/2934/pdf/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

representing the interests of users of regulated services, and experts on the prevention or handling of disinformation and misinformation online. It is required to advise Ofcom on three things: how regulated services deal with disinformation and misinformation; transparency reporting requirements around disinformation and misinformation; and how Ofcom should promote media literacy around disinformation and misinformation.

Clause 99 of the Bill should be amended to give the advisory committee a fourth role: advising and overseeing Ofcom's research on the harms caused by disinformation and misinformation.

In addition, Ofcom should look to establish a citizen panel with civil society partners – to ensure that the views of the public on harms in a disinformation/misinformation context are available to it directly and not only through qualitative and quantitative research. Such a citizen panel should have a connection to the advisory committee on disinformation and misinformation. The responsibility of the committee could be extended to considering the views of the public on harms in a disinformation/misinformation context and incorporating that insight into the committee's advice to Ofcom.

Government and Ofcom should explore the creation of an independent evidence centre on harms and misinformation and disinformation

It is critical that Ofcom conducts its own research and builds an evidence base on the harms caused by disinformation and misinformation. But Ofcom and the government should also explore whether a separate, independent evidence centre could be of value.

Questions around online harms and the impact of disinformation and misinformation are very unlikely to go away – it may therefore be worth investing in an institution, something more permanent than a research stream or programme, as part of the wider evidence ecosystem on online harms. A separate institution could be in a stronger position to tell the regulator challenging truths than its own research team and draw upon wider expertise.

Models for such a centre already exist. The government's What Works Network comprises several centres – on subjects including education policy, policing, ageing, clinical excellence, homelessness and wellbeing – which aim 'to improve the way government and other public sector organisations create, share and use (or

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

'generate, translate and adopt') high quality evidence in decision-making. If evidence is not available, decision-makers should use high quality methods to find out what works.'[41] They collate existing evidence; produce reports and reviews and commission trials and evaluations where there may be gaps; assess the effectiveness of policies; and share their findings and support policymakers and practitioners to use evidence to inform their decisions.[42]

There are other similar bodies in the UK and elsewhere, such as the Economic Statistics Centre of Excellence (ESCoE), supported by the Office for National Statistics, which aims to be 'an international point of reference for measurement research',[43] or the Organisation for Economic Co-operation and Development (OECD) Observatory of Public Sector Innovation, which aims to 'uncover emerging practice and identify what's next, turn the new into the normal and provide trusted advice' around innovation in the public sector.[44]

Whilst there has been one centre set up around online harms, the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN)[45], an UKRI Research Centre of Excellence, it has a focus on privacy, data and cybersecurity threats with only limited exploration of some forms of related disinformation.

There is a strong case for an independent evidence centre to be established with a primary focus on disinformation and misinformation. This could be as part of wider work on online harms more generally, or internet regulation and standards; or include broader, related subjects, such as digital competition and other policy challenges relating to information and data. A world class evidence centre on these emerging issues could support the UK government's wider ambitions around regulatory diplomacy and becoming a data and digital hub globally.[46] It is imperative that there is a mobilisation of a high-quality evidence base of research, data and evaluations to

[41] The Cabinet Office, 22 October 2019, 'What Works Network', https://www.gov.uk/guidance/what-works-network
[42] Nesta, 3 June 2020, A Practical Guide for Establishing an Evidence Centre, https://www.nesta.org.uk/report/practical-guide-establishing-evidence-centre/
[43] Economic Statistics Centre of Excellence, About ESCoE, accessed 8 December 2021, https://www.escoe.ac.uk/about-escoe/
[44] Observatory for Public Sector Innovation, About OPSI, accessed 8 December 2021, https://www.oecd-opsi.org/about-observatory-of-public-sector-innovation/
[45] National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN), accessed 31 January 2022, https://www.rephrain.ac.uk/.
[46] The Cabinet Office, 16 March 2021, Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

help the regulator, policymakers, practitioners and others to achieve the objective of reducing harm from misinformation and disinformation in the UK through effective regulation and voluntary action.

Action for government Amend the draft Online Safety Bill to place a duty on Ofcom to research harms caused by misinformation and disinformation, and grant the advisory committee on disinformation and information a role in advising and overseeing Ofcom on such research; ensure Ofcom has the necessary powers and resources for such a role; with Ofcom, explore the option of setting up an independent evidence centre.

Action for the regulator With the government, explore the option of setting up an independent evidence centre.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 4: Actively look for information vacuums and fill them

Ensure reliable information from authoritative information is available

Recommendation The Online Safety Bill and resulting regime should include provisions to incentivise the proliferation of authoritative information; Ofcom as regulator should ensure it is providing an enabling environment and proper direction on information vacuums and data deficits; and, all actors with the ability to address information vacuums and associated problems should proactively improve their interventions.

Address the conditions where harmful content and behaviour is allowed to flourish

Where there is a lack of quality information on topics of public concern, online discussion about these topics can be quickly dominated by speculation, low quality or partial information, and misinformation or disinformation.

There has been plenty of research and discussion about the prevalence, format, spread and effects of misinformation and disinformation in recent years. However, there has been less about addressing the conditions which allow harmful content and behaviour to develop, such as information vacuums or algorithms which promote emotive content more favourably than factual information.

Some organisations have made steps towards considering what is needed to tackle information vacuums. This includes increased capacity for social listening to identify high volumes of questions or confusion about a certain topic, or analysing search trends to identify where content creators can be encouraged to meet demand for content about particular topics.[47]

[47] First Draft, 28 September 2020, Data deficits: why we need to monitor the demand and supply of information in real time, https://firstdraftnews.org/long-form-article/data-deficits/; Tina D. Purnat, et al., 2021, Infodemic Signal Detection During the COVID-19 Pandemic: Development of a Methodology for Identifying Potential Information Voids in Online Conversations, JMIR Infodemiology 1, pag.https://www.semanticscholar.org/paper/Infodemic-Signal-Detection-During-the-COVID-19-of-a-Purnat-Vacca/55e6c012de70a15788b35cdd74c39b65ebf50676; Data and Society, 29 October 2019,

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Discourse around the Online Safety Bill when it comes to harms around misinformation and disinformation has largely focused on addressing problematic content and the systems that spread it. We believe that addressing scenarios where a lack of accurate information generates an information vacuum should also be high priority – both across government and the wider institutional landscape, as well as by the internet platforms. As well as considering existing harm and platform systems, the Online Safety Bill needs to address the conditions under which harmful content and behaviour is allowed to flourish.

Help users access good information so they can make good decisions

In times of heightened uncertainty people try to make sense of what is happening and what they should do. Social media is now part of a process referred to as 'collective sensemaking' whereby individuals connect with others to assemble a picture of the situation so they can decide on the action they need to take. Questions and speculation mount. In that mix there can be misinformation which, if used to make a decision, can result in harm to that individual and possibly also near and distant others.

Rumours can be both helpful and harmful but, in the era of social media, the scale, speed and the sheer volume of information have changed the dynamics. Working out what information can and cannot be trusted is a challenge every day. In times of an information incident or crisis, this is even more difficult and charged with greater anxiety (which in itself can lead to any one us being part of the spread of bad information).

Whilst the Online Safety Bill has different categories for 'user-to-user services' and 'search services', the former (i.e. social media platforms) are also places where people look to find information (not just the search services). This can lead to 'engagement deficits': where high quality information exists, but there is low engagement on social media ('user-to-user services'). This low engagement on social media demonstrates that there is still a problem of supply; because high-quality information content fails to compete with other more emotive content, or because high-quality content is poorly promoted. This illustrates that it is not enough for good information to be

---

Data Voids, Where Missing Data Can Easily Be Exploited, https://datasociety.net/library/data-voids/; Google, Question Hub, Accessed 31 January 2022, https://questionhub.withgoogle.com/intl/en/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

created: it must be shared to reach those that would find it useful in their decision-making.[48]

The Covid-19 pandemic has given glimpses of how governments, health authorities and internet companies can work effectively together to proactively push out high quality information to pre-empt or mitigate information vacuums. However, this is a significantly untapped area, where much-needed interventions must be developed by multiple actors.

This phenomenon was illustrated mostly widely and clearly at the start of the Covid-19 pandemic (see case study). Whilst hugely challenging, the pandemic demonstrated that key actors understood the need to address information vacuums and a great deal of learning has been generated as a result.

Our monitoring and fact checking over the past eighteen months revealed several information vacuums. On the pandemic, for example, the initial lack of information about the safety of vaccines for pregnant women and effects on fertility has had lasting effects, with both women and vaccination centres receiving mixed messages, and pregnant women not being given second doses or thinking they need to start their course again[49].

Outside of Covid-19, we saw vacuums on issues such as fuel stocks, when low fuel levels led to panic buying. Taking an exceptional decision to publish the figures on, say, a daily basis, may have eased some of the panic; however the Department for Business, Energy and Industrial Strategy (BEIS) said that it would not be changing its monthly publication schedule.[50] The lack of government data may also have led to the media relying more heavily on reports from industry organisations warning about the number of petrol stations which were closed.

---

[48] First Draft, 28 September 2020, Data deficits: why we need to monitor the demand and supply of information in real time, https://firstdraftnews.org/long-form-article/data-deficits/

[49] Full Fact, 8 December 2020, No evidence Pfizer Covid-19 vaccine affects women's fertility, https://fullfact.org/health/vaccine-covid-fertility/; Full Fact 22 December 2020, There's no evidence the Pfizer vaccine interferes with the placenta, https://fullfact.org/online/placenta-protein-vaccine/; Full Fact, 8 October 2021, What do we know about the AstraZeneca vaccine in pregnancy?, https://fullfact.org/pregnant-then-screwed/AZ-vaccine-pregnancy/; Full Fact, 25 August 2021, PHE says no need to restart vaccination course in pregnancy after second dose delay, https://fullfact.org/health/vaccine-second-dose/; Full Fact, 22 September 2021, Do pregnant women get Covid-19 booster vaccines?, https://fullfact.org/pregnant-then-screwed/boosters-in-pregnancy/; Full Fact, 29 October 2021, Why can you mix and match booster jabs in pregnancy?, https://fullfact.org/health/health-pregnant-then-screwed-booster-mix-and-match/

[50] Twitter user @EdConwaySky, 29 September 2021, https://twitter.com/EdConwaySky/status/1443261242651590663

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Public authorities need to be proactive and cooperate to meet information needs

In an information environment where harm can be caused by a lack of good information allowing bad information to spread unchallenged, it is critical that public authorities have the capability to proactively address information vacuums and to cooperate effectively in doing so. From our fact checking we see this need in a wide range of sectors from public health and food safety and from trading standards to public infrastructure.

The need extends beyond public authorities to industry and business (see the 5G case study where the telecoms industry could have worked with public authorities in ways that better addressed the information need). We have also seen situations where the fast-moving consumer goods (FMCG) sector needed to be far more active in the information environment in relation to panic buying.

Capacity to identify and monitor information gaps exists already. Some service providers already monitor data deficits; others have not made this a public commitment, but clearly have the data and resources to do so. Therefore, we believe the provisions in the Online Safety Bill should direct service providers to support Ofcom in its role of understanding the harms done by misinformation and disinformation by regularly reporting where information vacuums and engagement deficits exist and whether, for example, there are information vacuums among particular demographic groups.

The Department for Digital, Culture, Media & Sport (DCMS) is currently building a disinformation dashboard to be used by different stakeholders, although these stakeholders and their needs are not yet clear. DCMS should build information vacuum detection into this dashboard as part of a regular monitoring programme. DCMS could also develop key indicators for information demand that could be used as a shared reference point for all UK actors involved in identifying information vacuums.

Full Fact has long advocated for the UK's official information producers to develop a horizon scanning function in relation to information that the public needs to make informed decisions during elections[51]. The pandemic has shown the need for horizon

[51] Full Fact, October 2020, Written Evidence, https://committees.parliament.uk/writtenevidence/13559/pdf/; Full Fact, 2021, The Full Fact Report 2021, Fighting a pandemic needs good information,

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

scanning for likely future information needs during information incidents such as public health emergencies or agricultural crises. Horizon scanning would not necessarily stop information vacuums from occurring, but would significantly improve the preparedness of the various bodies involved in producing and disseminating public information that is used in online conversations.

Full Fact's fact checking often reveals confusion and information vacuums, and we take action to try and ensure these gaps are filled. This can be a short-term problem and/or a long-term problem or set of problems that need to be addressed. In our experience, even with the feedback we provide, action is often not taken quickly enough to prevent the problems arising from information vacuums occurring, such as speculation or the introduction of low-quality or partial information to online discussions.

For example, in May 2021 Full Fact wrote to the Medicines and Healthcare products Regulatory Agency (MHRA) pointing out that the presentation of its Yellow Card scheme data was becoming a vector for misinformation about vaccine safety: people were presenting reports of suspected reactions to Covid-19 vaccines as official government statistics. This led to speculation and questions from online users about the safety of the vaccines, and exacerbated the existing information vacuum surrounding vaccines. However, it took several months before any significant action was taken: in the meantime, Full Fact saw numerous other examples of continued confusion from concerned internet users.

As detailed in the case study below, Full Fact sounded the alarm on an information gap around the safety of 5G which was not acted upon by the government or public health authorities in time, allowing the information vacuum to be filled by harmful conspiracy theories during the pandemic.

The regulatory framework that emerges from the Online Safety Bill needs to ensure that information producers and authorities work rapidly when they are warned about an information vacuum, before it is filled by harmful information. Ofcom will need to have capability in this area and ensure the requirements on in-scope companies address the risk of harm emerging in this way. If this is not set out clearly regulated companies could focus only on, for example, safety by design on content and

---

https://fullfact.org/media/uploads/full-fact-report-2021.pdf; Civil Service World, 1 February 2021, Government comms 'need overhaul' after Covid-19 blunders and spin, https://www.civilserviceworld.com/professions/article/government-comms-need-overhaul-after-covid19-blunders; Full Fact, 2020, The Full Fact Report 2020, Fighting the causes and consequences of bad information, https://www.pdpjournals.com/docs/888060.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

interaction that could create harm to their users and not on the absence of information that allows harmful misinformation to emerge. The regime set out in law and regulation will need to reflect this and work with a wider landscape of actors that should and/or can provide good information that platforms can set before their users. Health actors are the most obvious example, but as set out here, many other sectors and bodies have a key role to play in this regard.

Make factual information engaging

Under Facebook's Third-Party Fact-Checking Programme[52], fact checks are connected to false claims that online users have seen or engaged with. In the same way, high quality information needs to be connected up with information gaps, whether through algorithms, targeted advertising support or other methods. Government and public authorities cannot simply press publish and then forget about the information vacuum. Proactive promotion and continued monitoring of the information vacuum is an equally important part of the picture.

Unfortunately, it is not enough for high quality factual information to exist. It must compete with emotive and entertaining content against which it will almost always lose the race in terms of views, engagement and salience. This has been termed an 'engagement deficit' and tackling it should be an important part of measures to address information vacuums.[53] Academics, researchers, service providers and others have been aware of this phenomenon for some time. However, there is not yet a consensus on how to tackle the problem of emotive or speculative content performing better than factual information.[54]

We recommend that service providers identify and explain how they are tackling, and will tackle, engagement deficits in the risk assessments provided to Ofcom. Each platform has different audiences with different needs and different formats as well

[52] Meta, Meta's Third-Party Fact-Checking Program, accessed 31 January 2022, https://www.facebook.com/journalismproject/programs/third-party-fact-checking
[53] First Draft, 28 September 2020, Data deficits: why we need to monitor the demand and supply of information in real time, https://firstdraftnews.org/long-form-article/data-deficits/
[54] Stefan Stieglitz, Milad Mirbabaie & Maximilian Milde, 2018, Social Positions and Collective Sense-Making in Crisis Communication, International Journal of Human–Computer Interaction, https://www.researchgate.net/profile/Milad-Mirbabaie-2/publication/322808864_Social_Positions_and_Collective_Sense-Making_in_Crisis_Communication/links/5a7abc100f7e9b41dbd69c02/Social-Positions-and-Collective-Sense-Making-in-Crisis-Communication.pdf; Kate Starbird, et al., 2016, Could This Be True? I Think So! Expressed Uncertainty in Online Rumoring, https://dl.acm.org/doi/pdf/10.1145/2858036.2858551

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

as insight on engagement. Over time they should find increasingly effective ways to allow their users to engage with high quality factual information.

Action for government Amend the Online Safety Bill to require Ofcom to monitor the online environment for situations where the dissemination of harmful misinformation and disinformation is being exacerbated by information vacuums or engagement deficits, and make public recommendations about how this can best be addressed. Service providers should be required to support Ofcom in that function by providing relevant information and intelligence (to be set out in a Code of Practice issued by the regulator).

Action for the regulator Ofcom will need to have capability to identify and address information vacuums, and to ensure the requirements on in-scope companies address the risk of harm emerging in this way.

Action for platforms Promote good information to users and support public authorities monitoring emerging and existing data and engagement deficits.

Case study: 5G misinformation was a known risk long before it led to attacks on infrastructure and harassment of telecoms engineers

In just a few weeks, Full Fact saw posts about 5G – the next generation wireless network technology – go from a niche corner of the internet to several fully fledged conspiracy theories piggybacking on the world's biggest news story, and endorsed by celebrities.

Full Fact began researching 5G conspiracy theories in the UK claiming that 5G was harmful in early 2019. Themes included 5G causing the death of flocks of birds or harm to trees, and claimants tended to draw selective attention to official statements or academic studies to back up their points which suggested that magnetic and electromagnetic fields might be carcinogenic[55][56]. 5G rumours have been remarkably successful at infiltrating a variety of online communities – from

[55] IARC Publications, 2002, IARC Monographs on the Evaluation of Carcinogenic Risks to Humans Volume 80, https://publications.iarc.fr/Book-And-Report-Series/Iarc-Monographs-On-The-Identification-Of-Carcinogenic-Hazards-To-Humans/Non-ionizing-Radiation-Part-1-Static-And-Extremely-Low-frequency-ELF-Electric-And-Magnetic-Fields-2002

[56] World Health Organisation, 31 May 2011, IARC classifies radiofrequency electromagnetic fields as possibly carcinogenic to humans, https://www.iarc.who.int/wp-content/uploads/2018/07/pr208_E.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

anti-vaccination groups to climate change sceptics – as well as offline spaces including UK parliamentary debates about the potential effects on health[57], or councils planning to block 5G as a result of misinformation[58].

Full Fact warned that the lack of official information about 5G was a problem in 2019. Then, the only public information available was documents from Public Health England on electromagnetic field safety[59] and the safety of 5G[60], which the government pointed to when questioned on 5G and health. However, those concerned by the claims – including Labour MP Tonia Antoniazzi – described the advice as "far from reassuring". As we noted in the Full Fact Report 2021, it was clear that a more proactive public information campaign was necessary from far earlier on, responding specifically to the most common arguments against 5G[61].

When conspiracy theories about 5G converged with the coronavirus pandemic in January 2020, it was not surprising that the severity and scale of misinformation worsened, with claims circulating about 5G causing the virus or being a hoax to enable the government to install 5G under the cover of lockdown.

Things escalated as public freedoms became tighter: telecoms engineers were filmed or berated at work, on new infrastructure which was seen as evidence that the government was hiding something[62]. A theory emerged that Covid-19 symptoms were "mass injury" from 5G, with surrounding claims including that Covid-19 broke out in Wuhan because of 5G there, or that cruise ship outbreaks were due to radiation-emitting technology used on them.

The UK government finally acknowledged this information gap in April 2020[63], and worked with health bodies and mobile infrastructure companies to create new

[57] Tonia Antonazzia MP, 25 June 2019, Westminster Hall Debate, Electromagnetic Fields: Health Effects https://hansard.parliament.uk/Commons/2019-06-25/debates/7D18471E-627A-41C4-B338-11F278CEA9B7/ElectromagneticFieldsHealthEffects
[58] The Times, 12 October 2019, Councils block 5G as scare stories spread, https://www.thetimes.co.uk/article/councils-block-5g-as-scare-stories-spread-gnfgshn58
[59] Public Health England, 3 October 2019, Electromagnetic fields, https://www.gov.uk/government/collections/electromagnetic-fields
[60] Public Health England, 3 October 2019, Guidance: 5G technologies: radio waves and health, https://www.gov.uk/government/publications/5g-technologies-radio-waves-and-health/5g-technologies-radio-waves-and-health
[61] Full Fact, 28 January 2021, Fix information failures or risk lives: the Full Fact Report 2021, https://fullfact.org/blog/2021/jan/fix-information-failures-or-risk-lives-full-fact-report-2021/
[62] Twitter user @aaqua_mel, 2 April 2020, https://twitter.com/aaqua_mel/status/1245671758222561280
[63] Twitter user @DCMS, 5 April 2020, https://twitter.com/DCMS/status/1246746235253542915

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

materials on the safety of 5G, while the internet companies worked to promote that information on their platforms. However, the response prior to this was insufficient to stem the tide of increasingly severe and harmful misinformation.

During a health crisis like the pandemic, when society has been turned on its head, it is hardly surprising that people's rational defences are down and they are stressed and confused: a context which must be taken into account in any response.

Case study: foresight work at the beginning of the Covid-19 pandemic

At the start of the pandemic in early 2020, UK citizens and decision-makers had no prior experience of living through or responding to a pandemic, and there were numerous information gaps where scientific evidence did not yet exist or was contradictory.

March and April 2020 saw a surge in news use as people in the UK turned to different media for more information about the crisis and the government response [64]. The absence of certainty and clear answers proved to be fertile ground for speculation and theories to gain traction, including about causes of the virus, symptoms and cures, and different actors' motivations during the pandemic.

The deficit of information about the safety of vaccines for pregnant women is covered above, and other vacuums included information about the scale of Test and Trace (where organisation charts and operational information was either delayed or never published), blood clots following Astrazeneca vaccines, details of testing targets and testing capacity, and the safety of ibuprofen for people with Covid-19[65]. Some of these vacuums were more long-lasting than others.

[64] Reuters Institute and the University of OXford The UK COVID-19 news and information project, accessed 31 January 2022, https://reutersinstitute.politics.ox.ac.uk/UK-COVID-19-news-and-information-project

[65] Full Fact, 16 March 2020, There's mixed evidence on whether people with Covid-19 should avoid ibuprofen, https://fullfact.org/health/covid-19-ibuprofen; Full Fact, 10 July 2020, Did the government meet its Covid-19 test targets?, https://fullfact.org/health/six-test-targets/; Full Fact, 10 March 2021, Misleading claims about Serco's role in Test and Trace resurface, https://fullfact.org/health/test-trace-march-2021/; Full Fact, 17 March 2021, 17 countries haven't 'banned' the Oxford-AstraZeneca vaccine, https://fullfact.org/online/blood-clot-az-ban/;

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Many organisations were quick off the mark in responding to these gaps, with different sectors of society taking different approaches. The Office for Statistics Regulation rapidly produced guidance for statistics producers, instructing producers to consider coherence, caveats and transparency about decisions made regarding new and existing releases, and giving constructive feedback throughout the pandemic[66].

The World Health Organization (WHO) convened an ad-hoc consultation on managing the Covid-19 infodemic[67], resulting in a competency framework that highlighted the importance of social listening to understand community concerns and questions, and to more quickly identify and fill information voids[68].

Full Fact joined WhatsApp's partnership programme which allowed us to gain a better understanding of which claims were popular on the closed platform and what questions citizens wanted answering.

Google's pre-existing Question Hub allowed the company to identify and fill information gaps by collecting unanswered questions and then sharing the insights with content creators to connect demand and supply. However, this information was not always shared with others.

Civil society organisation First Draft produced a research paper on data deficits[69] (building on Data and Society's work describing search engine queries that turn up little to no results[70]), recommending that platforms provide more transparency over search trends and noting, "If we can gather this data, then we need to start tracking multiple high-risk topics — not just the coronavirus, but conspiracy theories, vaccines, elections and climate change. Targeting specific topics, and breaking them down into subtopics, can develop targeted monitoring of search for high-risk issues". First Draft did make progress in developing qualitative indicators

[66] Office for Statistics Regulation, March 2020, Regulatory Guidance: Guidance on Statistical Practice for Statistics Producers during the Coronavirus Crisis, https://osr.statisticsauthority.gov.uk/wp-content/uploads/2020/07/Regulatory-guidance_changing-methods_Coronavirus.pdf
[67] World Health Organisation, 20 April 2020, WHO consultation on infodemic management framework - Provisional programme, https://www.who.int/publications/m/item/provisional-programme
[68] World Health Organisation, 15 September 2021, WHO competency framework: Building a response workforce to manage infodemics, https://www.who.int/publications/i/item/9789240035287
[69] First Draft, 28 September 2020, Data deficits: why we need to monitor the demand and supply of information in real time, https://firstdraftnews.org/long-form-article/data-deficits/
[70] Data and Society, 29 October 2019, Data Voids, Where Missing Data Can Easily Be Exploited, https://datasociety.net/library/data-voids/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

of demand for information, but this has not been widely adopted by relevant actors so far.

While these approaches were undoubtedly successful in different ways, increased systematic information sharing and collaboration early on would have helped these different actors to act more quickly and effectively, for example identifying groups particularly vulnerable to the harm of information gaps, or topics which had more urgent gaps to fill than others.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 5: Identify and coordinate responses to information incidents openly

Emergency procedures should be open and transparent

Recommendation Ofcom should have responsibility for transparently identifying information incidents and overseeing arrangements with regulated services for responding to incidents and mitigating harm. This should include the power to set out a policy covering information incident identification and mitigation; the creation of a public reporting system about what incidents it and other actors have responded to; and the ability to require information from service providers so that Ofcom can provide informed advice and regulatory action such that responses to information incidents are proportionate and fair (and more likely to be effective).

The Online Safety Bill must cover information incidents and crises

After a white supremacist gunman murdered 51 people in the New Zealand city of Christchurch in March 2019, technology companies and governments came together to review how to combat terrorist content online[71]. The gunman had live-streamed the attack on the mosque, and the video was viewed around 4,000 times before being removed. Governments and technology companies committed to measures such as mitigating the specific risks of terrorist and violent extremist content disseminated through livestreaming, regular transparent public reporting, and working together to ensure cross-industry efforts are coordinated and smaller platforms are supported to remove terrorist and violent content.

Incidents like this can cause real harm, such as targeted radicalisation of vulnerable users or inspiring further attacks. They can take those working to counter them by surprise even if risks have been assessed and preparation has taken place, often leading to rushed and uncoordinated responses. It is therefore welcome that the draft Online Safety Bill recognises that many actors have a role to play in creating a robust

[71] The Government of New Zealand, Christchurch Call, accessed 31 January 2022, https://www.christchurchcall.com/index.html

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

and stable information environment, including technology companies, government, parliamentarians, civil society, the media and regulators.

Certain events can corrupt the information environment by increasing the complexity of accurate information, creating confusion or revealing information gaps - all of which can result in an increase in the volume of harmful misinformation and the speed at which it spreads. We describe these moments of heightened vulnerability as 'information incidents'. They are often characterised by a proliferation of inaccurate or misleading claims or narratives, which relate to or affect perceptions of our behaviour towards a certain event or issue happening online or offline. This can occur suddenly.

Even when events and their effects on the information environment have been relatively predictable, organisations and institutions responsible for counteracting the harm done by misinformation in such incidents or crises have not been prepared. Considered, long-term initiatives like the Christchurch Call are rare, with measures more often being introduced spontaneously, and without enough consideration of unintended consequences or consultation with stakeholders and affected groups.

The urgency of some situations has allowed powerful actors to bypass normal stakeholder consultation procedures or let censorship-by-proxy creep in at times when we need to be most careful to protect freedom of expression and maintain public trust in authorities (this is covered further in Chapter 8).

Law, regulation and voluntary arrangements should enable transparent and effective responses to online and offline harms that are supercharged during information incidents

The government is aware of the harms that can result from information incidents. The Online Harms White Paper states that: "there may be instances when urgent action is required to address disinformation and misinformation during emergency situations," as was demonstrated by the pandemic. DCMS has also taken part in several roundtables convened by Full Fact to discuss the need for counter-disinformation actors to be better prepared for the next major information incident. The resulting Framework for Information Incidents[72] is a model to help decision-makers understand, respond to and mitigate information crises in proportionate and effective ways. The DCMS Counter-Disinformation Forum – a body bringing together industry, government, civil society and experts to limit the

[72] Full Fact, 2022, Incident framework, https://fullfact.org/about/policy/incidentframework/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

spread and harmful effects of misinformation and disinformation – has already integrated the Framework's severity levels into the agreed protocols for how the Forum should be convened during crises.

Despite this understanding, the Online Safety Bill is insufficiently explicit about periods of heightened risk. It does not encourage or provide a structure for ensuring the preparedness of providers of internet services to effectively respond to information incidents and crises with others. Whilst it could be argued that information incidents implicitly fall within the duties and provisions around risk assessments, greater reassurance is needed.

We need to know that the Online Safety Bill will help keep citizens safe during an information incident or crisis. If the government, Ofcom, parliamentarians, regulated companies and other stakeholders in the new regulatory regime develop the system without proper regard to information incidents of all levels of severity, it will not provide for effective responses to the unique threats these incidents pose.

Situations likely to trigger information incidents in the UK

The harms that can result from information incidents are varied, and include (often compound) threats to physical safety, civil order, health, life, personal and public finances, democratic processes and participation, access to services; and the risks of polarisation and abuse or attacks, for example on minorities, public figures or service workers. In some contexts there is a thin line between disinformation and abuse.

Terror incidents

Threats posed by terrorism-related information incidents: threats to physical safety and civil order, and risk of or actual abuse or attacks on minority groups.

The London Bridge attack, the Manchester Arena bombing and Westminster car attack all led to immediate demand for and production of news, with the press and social media saturated with updates, commentary and pulsing 'Live' red buttons within hours. As with most terror incidents there is often a gap before information is confirmed, which may lead to a surge in false information, often with a hateful edge.

Terrorist content is generally dealt with in Principle 1 of the Interim Code of Practice on Terrorist Content and Activity Online[73], which sets out sets out provisions related

[73] The Home Office, December 2020, Interim Code of Practice on Terrorist Content and Activity Online, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944036/1704b_ICOP__online_terrorist_content_v.2_11-12-20.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

to terrorist content and its dissemination and provides detailed guidance for companies to help them understand how to mitigate the range of risks arising from online terrorist content and activity.

The Christchurch Call[74], set up in the aftermath of the Christchurch mosque attack in New Zealand, also highlights the need for emergency protocols in the aftermath of terrorist events. It calls on governments to "Develop processes allowing governments and online service providers to respond rapidly, effectively and in a coordinated manner to the dissemination of terrorist or violent extremist content following a terrorist event. This may require the development of a shared crisis protocol and information-sharing processes, in a manner consistent with human rights protections."

However, it's not currently clear how the Online Safety Bill will work when harmful misinformation and disinformation is not from online terrorist content and activity itself, but is in response to events that may be or are terror-related in the UK, or such events in other countries which people in the UK are affected by.

Elections and major votes

Threats posed by election-related information incidents: threats to democratic processes and participation, and risk of polarisation and abuse.

Recent elections and referendums in the UK have spurred polarisation and there have been instances of high profile inaccurate claims from influential public figures, presenting risks of harm to social cohesion, democratic participation and trust in the political system.

There may come a time during an election when the public needs to be warned about a specific threat identified by the security services, but at the moment the decision would be up to the government of the day, which would be put in a difficult position and is likely to be seen as conflicted. We prefer the model in Canada, where there is a public protocol—the Critical Election Incident Public Protocol (CEIPP)—for handling such situations and cover this in Chapter 10.

Public health emergencies

Threats posed by public health-related information incidents: threats to health, life and access to services, plus risk of or actual abuse or attacks on minority groups.

[74] The Government of New Zealand, The Call, accessed 31 January 2022, https://www.christchurchcall.com/call.html

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

The Covid-19 pandemic is the most severe example of an information incident in recent years. The volume of information was unprecedented; the scientific content matter was challenging for the public, the media and politicians to grapple with; and there were information gaps about causes and treatment and multiple changes in official advice (most famously on mask-wearing). Baseline responses designed to deal with day-to-day misinformation were quickly recognised as insufficient.

It is clear that some groups carry the burden of information incidents long past the time when policymakers believe an incident to be over. Full Fact's partnership checking health misinformation with Pregnant Then Screwed has revealed continued widespread confusion, fear and inaction among pregnant women, caused by conflicting claims and disinformation about vaccine safety and effects, more than eighteen months after the start of the pandemic.

The government's response to the Online Harms White paper[75] promised that the Bill would give the regulator the power to act to ensure companies address disinformation and misinformation that poses a reasonably foreseeable risk of significant harm to individuals, specifically mentioning public health. However, the draft Bill relies on a Secretary of State power (Clause 112) to direct Ofcom in special circumstances, when they have 'reasonable grounds for believing that circumstances exist that present a threat to the health or safety of the public, or to national security'.

This power includes, as the explanatory notes put it, 'directing Ofcom to prioritise action to respond to such a specific threat when exercising its media literacy functions' and 'to require a service provider to publicly report on what steps it is taking to respond to that threat'. It seems odd to situate effective responses around media literacy. Carnegie UK has speculated that this may be because this is about addressing collective harms where online safety regulation is focussed on harm to the individual. The explanatory notes say that this 'provides the Secretary of State with the option to step in to ensure that Ofcom is taking steps to address threats of disinformation and misinformation'.

Whilst there may be a case for Secretary of State power to direct Ofcom in matters relating to national security and public safety, given, as Ofcom has stated: 'there will clearly be some issues where the Government has access to expertise of information

[75] The Department for Digital, Culture, Media and Sport, 15 December 2020, Online Harms White Paper: Full government response to the consultation https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

that the regulator does not, such as national security', as the Joint Committee says these 'powers should not be exercised without oversight or scrutiny'.

Full Fact believes that the Bill should allow the regulator the space to take decisions based on the available evidence. Ofcom should have enough powers to address threats to public safety, public security and national security.

We recommend that Ofcom is given direct power to ensure service providers consider reasonably foreseeable risks related to public health misinformation within their risk assessments.

Require service providers to implement systems and processes to identify reasonably foreseeable risks of harm, including special arrangements during periods of heightened risk

The draft Bill does not explicitly suggest that information incidents should be covered in risk assessments or other systems and processes. It does mention criteria that might be used in identifying an incident, for example risk assessments should cover "how easily, quickly and widely content may be disseminated by means of the service". The draft Bill also requires risk assessments to determine the nature and severity of harm that might be suffered in encountering harmful content on a service.

Severe incidents are often characterised by harmful content moving from one (usually smaller) platform to another (usually larger). The draft Bill does not recognise this: service providers only need to consider the risks of harmful content on their own platforms, not the (likely) risks of harmful content coming from another, and overwhelming their systems.

The intention of the Online Safety Bill is to impose duties on internet companies so that they manage harms which take place on their platforms. Currently, the Bill largely envisages these harms on a day-to-day basis: it accepts that some harm will take place in an open society, but requires platforms to show how they will mitigate these. Ofcom may choose to highlight periods of intense vulnerability in its future risk assessment guidance, but that is not expressly required by the draft Bill. Without that direction or guidance, providers of regulated services may focus their assessments on everyday risks rather than those arising out of periods of heightened vulnerability.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Strengthen Ofcom's role in identifying and mitigating information incidents and its capability to act and convene for effective response

After the first wave of the pandemic, the unprecedented scale and speed of false information was much-discussed. However, the draft Bill does not incorporate any learning from this experience. The government's Online Harms White Paper said, 'Where disinformation and misinformation presents a significant threat to public safety, public health or national security, the regulator will have the power to act. In such situations, Ofcom will be able to take steps to build users' awareness and resilience to disinformation and misinformation, or require companies to report on steps they are taking in light of such a situation.'[76]

This is not yet sufficiently explicit in the legislation. If another severe information crisis emerges soon after the Online Safety Act is in place, Ofcom will need the necessary powers to act and to ensure the readiness of service providers to mitigate the risks of future incidents. A generous interpretation could say that the powers granted to the Secretary of State in Clause 112 regarding national security or public safety could cover this ground. Yet this power appears limited to the prioritisation of Ofcom's media literacy functions, or making Ofcom require providers to issue a public statement about steps they are taking to address the circumstances in question.

Ofcom should be able to act to ensure effective response to information incidents without instruction from the Secretary of State. Service providers themselves are often well placed to consider and articulate the additional risks posed by periods of heightened vulnerability: it is therefore imperative that platforms are obliged to share information about emerging information incidents of varying severity as well as everyday online harms.

Ofcom addressed some of these issues in its follow up note to the Joint Committee[77], including introducing the concept of reasonably foreseeable risk, as well as a concept of 'adequacy' or 'suitability' to enable Ofcom to force improvements to insufficient risk assessments. Together, these changes could provide a mechanism for prompting

[76] The Department for Digital, Culture, Media and Sport, 15 December 2020, Online Harms White Paper: Full government response to the consultation https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

[77] Ofcom, 19 November 2021, Follow-up note for the Joint Committee on the draft Online Safety Bill, https://www.ofcom.org.uk/__data/assets/pdf_file/0025/228247/follow-up-note-draft-online-safety-bill.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

service providers to consider how to mitigate the reasonably foreseeable risks presented by common or likely information incidents as described above.

The Joint Committee recognised this in its December 2021 report on the Draft Online Safety Bill, arguing that the Bill should include a responsibility on service providers to have systems and processes to identify reasonably foreseeable risks of harm arising from the design of their platforms and take proportionate steps to mitigate those risks of harm, including "special arrangements during periods of heightened risk (such as elections, major sporting events or terrorist attacks)".

As a body that is independent from government and industry, Ofcom can play a credible convening role. To do this they should have good access to information from service providers in order to make informed judgements about when an incident is occuring or likely to occur. We recommend that Ofcom introduce a system whereby incidents can be publicly reported as either emerging or happening, and different actors such as fact checkers, news organisations, community representation groups and service providers can request that Ofcom convene a response group to discuss severity and response. For Ofcom, additional staff and a new proactive mindset may be needed to rise to this challenge, since its regulation style to date has been to respond after the fact. Where information incidents are concerned, responding after they have happened is too late.

Ideally, a cross-sector group would work together to decide on an incident's severity level, including representatives from civil society such as fact-checkers, local and national government (or former government representatives), press and media, regulators, relevant experts and academics, and service providers. The government-convened Counter-Disinformation Policy Forum had many of these core participants in its pilot stage, but could be expanded to include major broadcasters, newswires and open-source intelligence groups. Powerful entities such as the government and service providers should not declare a level for others, as this might undermine the action of others and their distinct roles (or perceptions around this).

It is worth noting, given the draft Online Safety Bill is geared heavily towards larger platforms (with fewer requirements on other in-scope companies), that periods of heightened vulnerability or actual information incidents will bring additional risks across platforms of varying sizes.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Ensure public oversight of incident identification and mitigation

Information incidents should be identified and mitigated in an open manner. This is currently lacking, and the draft Online Safety Bill fails to propose any mechanisms for changing the situation. There is no effective parliamentary oversight of the work of the Counter Disinformation Unit, and the approach of DCMS to influencing the actions of internet companies is largely behind closed doors in invite-only spaces. This may be justified to some extent by the fact that these parties are aware that the Online Safety Bill is imminent, and that a more open and transparent relationship was due to arrive, but this has not yet materialised. There are also risks of censorship by proxy (which are covered in Chapter 8 of the report).

Crucially for the question of how service providers manage the risks of information incidents, there is no requirement to publish risk assessments in the draft Bill. Ofcom may well choose to encourage or require service providers to publish risk assessments in the guidance it creates, but this is not currently required by the draft Bill. This means that parliamentarians, civil society and the public would have no access to the risk assessments and therefore no way of making an informed judgement about the risks identified and mitigation measures proposed by service providers, nor information by which to judge Ofcom's regulatory approach. Service providers may understandably be unwilling to include commercial information or be sufficiently robust or candid to make this information sharing effective, which could lead to possible disagreements between the regulator and those who wish to access information for accountability purposes. Further improvements in law, regulation and practice are therefore necessary even if pre-legislative recommendations from the Joint Committee are adopted.

Action for government and parliament Amend the Bill where necessary to ensure the law and regulation enables effective preparation, mitigation and response to information incidents and crises by Ofcom and regulated companies (working with other actors) in a way that provides accountability to stakeholders.

Action for the regulator Ofcom should demonstrate that it is sufficiently prepared and resourced to deal with information incidents both as a strategic actor (for example, in its remit such as issuing related guidance), and in developing preparation structures and being part of real-time effective response with others.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Appendix: Full Fact Framework for Information Incidents

The Framework for Information Incidents is a tool to help identify emerging information incidents and crises and to enable effective, proportionate responses from organisations and institutions that tackle harmful online content. It has been designed as a voluntary tool intended to enable open collaboration and consistency, and to do so as law, regulation and good practice evolve.

Not every information incident is equally severe, and judging severity is, at least to some degree, subjective. The Framework offers criteria for determining severity so that different actors can approach a conversation on the basis of shared understanding and bring evidence to the table to justify judgements. It has a five level system, ranging from business as normal at Level 1, where (in an open society) some misinformation will be circulating, to Level 5, which should rarely occur and requires maximum cooperation and response when it does.

Incidents might move between levels over time, either escalating or de-escalating and coming to a close. Responses can be adapted accordingly: measures put in place for an incident at Level 4 are likely to be unsuitable or disproportionate for the same incident when it is at Level 2. It may not be clear from the outset how long an incident will last, so building in review periods is important.

Whilst major internet companies often engage to some degree with external collaborative structures, it is unclear whether service providers have sufficient systems and processes to address fast-onset threats to online safety during moments of heightened vulnerability: the Online Safety Bill should address this problem head on by requiring significantly increased transparency from service providers about their systems and processes for identifying and responding to information incidents, and the Framework for Information Incidents could support this by providing a common reference with its severity levels.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 6: Prioritise tackling specific harmful behaviour over restricting content

Focus on harmful behaviours to be more effective and proportionate

Recommendation The Online Safety Bill should be amended to cover both regulated content and activity. The remit of the Advisory Committee on Misinformation and Disinformation should be widened to include reporting on misinformation and disinformation behaviour. Parliament should be prepared to legislate in the future to tackle emerging forms of activity that lead to specific online harms.

Amend the draft Online Safety Bill to cover "regulated content and activity"

We support the Joint Committee's recommendation: "that references to harmful "content" in the Bill should be amended to "regulated content and activity", the government's original language (Recommendation 6, Paragraph 68).

The Committee explains: "This would better reflect the range of online risks people face and cover new forms of interaction that may emerge as technology advances. It also better reflects the fact that online safety is not just about moderating content. It is also about the design of platforms and the ways people interact with content and features on services and with one another online."

Specialists in misinformation and disinformation sometimes use the Actor Behaviour Content model[78] to describe the causal chain that leads to harm from bad information. In their recommendations, the Committee rightly points out that both the activity of users and the activity of the internet companies themselves matter, and that these two interact.

[78] Camille François, 20 September 2019, Actors, Behaviors, Content: A Disinformation ABC, https://science.house.gov/imo/media/doc/Francois%20Addendum%20to%20Testimony%20-%20ABC_Framework_2019_Sept_2019.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

One striking example of how simply a behavioural intervention can address harmful false content is Twitter's experiment in asking users to read an article before they click to share it. They reported very significant results:.

"More reading – people open articles 40% more often after seeing the prompt

"More informed Tweeting – people opening articles before RTing increased by 33%

"Some people didn't end up RTing after opening the article – which is fine!"[79]

The beauty of this example is that it is not coercive and it does not limit anybody's freedom of expression, yet it has a meaningful effect on how well informed the conversation is. Anybody who wishes to reduce the harm from misinformation while protecting freedom of expression should want to ensure that choice-based interventions like these are fully explored.

In general we believe that targeting specific carefully defined actors and behaviour is more likely to produce proportionate responses to harmful false information than seeking to control what content anyone can see and share. The fact that it is crudely possible to monitor and filter public conversations at large scale doesn't mean that it is a good idea.

Prioritising in this way will need to include keeping pace with the patterns of behaviour that lead to particular types of harm, and deciding how best to address them.

Parliament should be prepared in future to develop the law to tackle specific kinds of deceptive behaviour

There are many examples of criminal offences to tackle deceptive behaviour already on the statute book.

- The existing offence of making false health claims in advertising is a targeted and proportionate response to certain kinds of health misinformation.
- The existing offences of falsely reporting a fire, or impersonating a police officer, both tackle behaviours that would damage public safety by weakening the emergency services.
- The existing offence of fraud by false representation tackles people who make a false representation, dishonestly, knowing that the representation was or

[79] Twitter, 24 September 2020, https://twitter.com/twittercomms/status/1309178716988354561?lang=en-GB

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

might be untrue or misleading, and with intent to make a gain for themselves, to cause a risk of loss to another.

Provided that such offences are well defined and tackle clear problems, they raise few objections on the grounds of freedom of expression. Typically such targeted restrictions tackle not just broad kinds of content but motive (e.g. profit), who does it (e.g. people with certain responsibilities), culpability (e.g. knowing or reckless of harm) and sometimes the topic, context, and/or the audience.

The internet changes the opportunities for people who are willing to deceive others in ways that cause harm, for example by making it easier than ever to misrepresent your own credentials. It will not be appropriate to tackle the actions of a minority by censoring the majority.

Parliament needs to recognise that the Online Safety Bill is not as a one-stop solution to online harms, but the first part of a new body of law that will need to be added to and updated over time.

The advisory committee on misinformation and disinformation should be given a remit to report on patterns of misinformation and disinformation behaviour

Government and Parliament can only act to address problems they are provided with evidence of.

The Advisory Committee on Misinformation and Disinformation is being set up by the Online Safety Bill to advise Ofcom on what regulated services should do and on the discharge of its functions of requiring information from regulated services and promoting media literacy.

It would be simple to give the committee a slightly wider remit to report on misinformation and disinformation more generally, their causes, and potential proportionate responses. This would also allow the Committee to advise Ofcom about emerging patterns of behaviour. Given the reliance on this provision of the draft Online Safety Bill to tackle harmful misinformation and disinformation, it will be a mistake to limit the committee's remit in a way that makes it harder for future governments and parliaments to keep up with such a rapidly changing set of problems.

Action for government Accept the Joint Committee recommendation to return to the language of "content and activity", and amend the draft Online Safety Bill to extend

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

the remit of the Advisory Committee on Misinformation and Disinformation to include reporting on emerging patterns of misinformation and disinformation behaviour and potential responses.

Action for the regulator Ofcom should work with the Advisory Committee on Misinformation and Disinformation to identify patterns of risky behaviour and possible proportionate responses.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 7: Make government interventions in content moderation transparent

Limit 'censorship-by-proxy' where government pressures internet companies to restrict content that parliament would not choose to

Recommendation The Online Safety Bill should be amended to introduce a reporting requirement for the government to publish details of all efforts it makes to influence internet company decisions on items of content, accounts and their terms of service. Parliamentary scrutiny of this activity must be strengthened.

The government's role in content take downs must be made public and accountable

The government can and does seek to limit speech online by lobbying internet companies. It has secured changes to their terms of service and then reported content for violating those terms. It has daily interactions with nearly all of the internet platforms, including on content removal. The government has come to think that its role on online content includes identifying particular bits of legal content on the internet that should not remain online, and pressuring internet companies to remove them.

This government enthusiasm for censorship-by-proxy has been a marked feature of its response to the Covid-19 pandemic. A government press release stated that "Up to 70 incidents a week, often false narratives containing multiple misleading claims, are being identified and resolved."[80] It did not define 'resolved'.

A DCMS minister subsequently sought to reassure the House of Lords Select Committee on Democracy and Digital Technologies that "the government does not mandate the removal of any content, only indicating to platforms where we have

[80] The Cabinet Office and The Department for Digital, Culture, Media and Sport, 30 March 2020, Government cracks down on spread of false coronavirus information online, https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

identified potentially dangerous and incorrect claims [...] for platforms to make a decision on." Only weeks earlier, the Home Secretary had given the impression government was involved in requesting removals of misleading content[81].

Around the same time another story briefed by the government to the BBC said: "The culture secretary is to order social media companies to be more aggressive in their response to conspiracy theories linking 5G networks to the coronavirus pandemic."[82]

The government "summoned" internet companies to tell them to remove certain content about 5G mobile networks after harassment of telecoms workers and attacks on facilities. Whether that was a proportionate response deserves debate. Full Fact had warned about the danger of 5G misinformation the year before and called for the free speech response of better public health information. This warning was not heeded and after the situation escalated, perhaps avoidably, the government turned to censorship-by-proxy through the internet companies (Chapter 3 sets out what the effective and proportionate response to the 5G information vacuum should have been).

Of course, it can be accepted that measures taken with good intentions during an emergency are never likely to be perfect. But instead of establishing open, democratic, transparent methods for responding to harmful false information in future, the draft Online Safety Bill is too quiet on misinformation and disinformation risks. Continued silence on this will lock in censorship-by-proxy as the new normal unless the government and parliament amend the legislation and rectify this situation.

To date, citizens can only rely on the good faith and judgement of staff currently in the relevant posts in government departments and agencies – a situation that leans heavily on brittle public trust. Ignoring this situation creates suspicion and leaves the government open to the accusation of what has also been termed extrajudicial state censorship. A perception of covert pressure on internet companies to remove unwanted lawful speech can easily be created. If this is not the reality then some transparency and oversight enshrined in law should not present a problem. If it is,

[81] The Secretary of State for the Home Department, Priti Patel MP, House of Commons, 8 February 2021, Home Office Questions, https://hansard.parliament.uk/commons/2021-02-08/debates/5F2F0112-3889-4D9A-85E5-019CA14CBD38/Anti-VaccinationExtremism#contribution-ACE7F753-40C9-4995-81AB-946F30F15DFF

[82] BBC News, 5 Apr 2020, Coronavirus: Tech firms summoned over 'crackpot' 5G conspiracies, https://www.bbc.co.uk/news/technology-52172570

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

then there is an even greater imperative to do it. Either way, a mechanism is required to limit potential overreach by less scrupulous future decision-makers.

End unnecessary secrecy in government work to counter false information

Ministers have been reluctant to be more open on the work of the Rapid Response Unit set up to work with social media companies to take action on online content[83]. As one parliamentarian said: "We have heard very little about its work and received no detail on what its achievements or actions are".

In answer to a parliamentary question in December 2021 as to how many posts have been reported to Facebook, Twitter, Instagram and YouTube for anti-vaccine disinformation by the government's Rapid Response Unit, the Minister for Tech and the Digital Economy replied: 'As an operational matter it is not appropriate for the government to give a running commentary on the amount of disinformation identified.'[84]

No figures have been given. We do not believe there is a proper justification to withhold the number of requests the government makes of any internet company and that the volume of such requests should be made public. The public should be given more information on volume and types of disinformation and harmful misinformation the government is reporting to internet companies.

The Cross-Whitehall Counter Disinformation Unit[85], which stood up for recent elections and was again standing from March 2020 due to the pandemic, also undertakes this activity. Its 'primary function' is 'to provide a comprehensive picture of the extent, scope and impact of disinformation and misinformation regarding Covid-19 and to work with partners to ensure appropriate action is taken'. It does this 'where dangerous and incorrect claims about the virus are identified these are

[83] Based in the Cabinet Office and No10, the Rapid Response Unit (RRU), 'uses robust data-driven insights to improve government communications through high-quality online analysis'. It combines a function informing communications across government with a counter-mis and disinformation role both in the short-term, such as breaking news and crises communications, and a longer-term focus to improve government communications on issues relating to social media, the media environment and mis and disinformation

[84] Minister for Tech and the Digital Economy, Chris Philp, 16 December 2021, Vaccination: Disinformation, https://questions-statements.parliament.uk/written-questions/detail/2021-12-10/90926

[85] For full disclosure, Full Fact has worked in partnership with DCMS, which leads the Counter Disinformation Unit, as part of the Counter Disinformation Policy Forum#, but we are not involved in how the government flags or makes requests about content to the internet companies.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

flagged to the relevant platforms, whose responsibility it is to take action in accordance with their terms and conditions'[86].

The Counter Disinformation Unit undertakes very valuable work on disinformation and misinformation. However, more transparency on what it does addressing specific content would help protect its overall reputation, recognising that revealing some tactics may not be advisable as it may advantage bad faith actors (for which reason appropriate mechanisms of oversight should be identified). Unnecessary secrecy around government attempts to counter false information should be ended through the Online Safety Bill.

Parliament must ensure transparent oversight

We need to move beyond the present situation where a minister can summon internet companies and call on them to remove certain content from the internet with no democratic oversight. Activity the government undertakes around the content of UK internet users needs legal and other safeguards, including targeted transparency measures.

The Online Safety Bill should include some form of reporting requirement for the government to publish details of all efforts it makes to influence internet company decisions about specific items of content, specified accounts or their terms of service.

Such a requirement could recognise the need for a limited time delay in the case of content considered sensitive to national security. This could be subject to review by the Joint Committee on Human Rights (JCHR)[87] and/or the Intelligence and Security Committee of Parliament (ISC)[88].

Strengthen freedom of expression with democratic transparent oversight of political decisions as well as commercial ones on online speech

Just as internet companies should not be left to make decisions on issues as fundamental as freedom of expression without proper scrutiny and oversight – a fundamental tenet of the Online Safety Bill – then neither should the government of

[86] Minister for Tech and the Digital Economy, Chris Philp, 16 December 2021, Vaccination: Disinformation, https://questions-statements.parliament.uk/written-questions/detail/2021-12-10/90926/
[87] House of Commons, Joint Committee on Human Rights, accessed 31 January 2022, https://committees.parliament.uk/committee/93/human-rights-joint-committee/
[88] The Intelligence and Security Committee of Parliament, accessed 31 January 2022, https://isc.independent.gov.uk/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

the day. A good Online Safety Bill would actually strengthen freedom of expression by providing open democratic transparent oversight of both commercial and political decisions which seek to limit ordinary internet users' freedom of expression.

Censorship-by-proxy with little-to-no political or legal scrutiny is a threat to freedom of expression. We need protections against what the internet companies are doing and what the government is currently doing of its own accord. Lack of oversight of the action of government and internet companies is part of a wider problem of which the vague duties on freedom of expression in the draft Online Safety Bill are also symptomatic.

It is worth noting that many internet companies publish transparency reports that include requests from governments around the world on content. They do so in part as an open way to try to reduce over-reach removals and ensure relevant laws do apply. If the Online Safety Bill is to be world leading, then including additional transparency in law would set a better standard internationally than the status quo.

Action for government Amend the draft Online Safety Bill to include a requirement for the government to publish details of all activities it makes to influence the decisions about specific items of content, specified accounts or their terms of service.

Action for parliamentarians Ensure the Online Safety Bill is amended to include a requirement for the government to be open about when it communicates to regulated internet companies on content, accounts or the terms of service of in scope companies.

Committees that provide scrutiny to departments involved in making requests to internet companies should press for proper scrutiny and accountability mechanisms to be in place.

Action for the regulator Ofcom should recognise the problematic nature of government influence on areas of its remit, for example around platform terms and conditions, and press for transparency so that the new regulatory system is not undermined. In addition, it should be transparent on any requests that flow to it from government to the same ends and include requests from government in its own transparency reports as well as in those of in-scope companies.

Action for platforms Improve transparency on government requests at a UK level with meaningful data and information that citizens and NGOs can easily access.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Continue to, or begin, publishing transparency information about government interventions on content, including the UK Government.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 8: Require independent testing of algorithms which restrict or promote what people can see and share

The Online Safety Bill should grant Ofcom full audit powers and ensure independent researcher access to algorithms

Recommendation The Online Safety Bill should be amended to give Ofcom clear powers to audit and test the algorithms used by regulated service providers to moderate and curate content on an ongoing basis. The Bill should also be amended to ensure third party researchers have access to the data necessary to conduct their own research.

Ofcom needs powers to test and audit algorithms

In our submission to the Joint Committee inquiry on the draft Online Safety Bill, Full Fact called for independent testing of 'safety-critical' content moderation algorithms, which can prevent some content from being shown and which can do real good as well as real harm:

> *'unlike many safety-critical technologies, the safety consequences of deploying a certain content moderation algorithm are not always obvious. How safe an aeroplane is will ultimately be visible for all to see, despite all the expertise that goes into its engineering. A qualified person can and must test whether an electrical system is safe. The effects of content moderation algorithms are far harder to understand, but their design is subject to no external scrutiny at all.'*[89]

[89] Full Fact, 20 September 2021, Written evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/writtenevidence/39171/html/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Other organisations (including Demos)[90] have also highlighted the crucial role of content curation algorithms, which suggest content to users.

The draft Online Safety Bill proposes several powers for Ofcom that can be used to obtain information from platforms, including issuing an information notice (clause 70), 'skilled person' investigations (74), summoning witnesses for interviews (76), and powers of investigation and entry (77), as well as requiring platforms to produce transparency reports (49, 50) and to publish assessments of the impact of their processes and procedures on users' freedom of expression and privacy (12). Both Ofcom, in written and oral evidence to the Joint Committee, and the Department for Digital, Culture, Media and Sport (DCMS) consider the draft Bill gives Ofcom sufficient powers 'to lift the lid on the algorithms'.[91]

Civil society organisations did not share this view in their evidence to the Joint Committee. For example, Carnegie UK thought the transparency reporting requirements were tightly drawn, and some of the information gathering powers 'more burdensome and also problematic in longitudinal tracking'.[92] A recent report by the Ada Lovelace Institute identifies six different ways of auditing algorithmic systems – code audits, user surveys, scraping audits, API audits, sockpuppet audits, and crowdsourced audits ('mystery shopper') – some of which require ongoing monitoring and are therefore not obviously within Ofcom's powers as set out in the draft Online Safety Bill.[93]

The report by the Joint Committee (Powers of audit, 337) states: 'Algorithms can both increase and reduce the spread of content that creates a risk of harm. As Full Fact put it: "content moderation algorithms can do real good if they work well, and if they malfunction, they can cause real harm", yet "the safety consequences of deploying a certain content moderation algorithm are not always obvious"'.

---

[90] Demos, 28 September 2021, Written evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/writtenevidence/39336/html/

[91] Ofcom, 13 September 2021, Written evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/writtenevidence/39067/pdf/; Ofcom, 1 November 2021, Oral evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/oralevidence/2934/pdf/; The Department for Digital, Culture, Media and Sport, 4 November 2021, Oral evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/event/5673/formal-meeting-oral-evidence-session/

[92] Carnegie UK, 17 September 2021,Written evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/writtenevidence/39242/html/

[93] Ada Lovelace Institute, 9 December 2021, Technical methods for regulatory inspection of algorithmic systems, https://www.adalovelaceinstitute.org/report/technical-methods-regulatory-inspection/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

The Joint Committee makes several recommendations to government on algorithms, including onits central proposition to require service providers to have systems and processes 'to identify reasonably foreseeable risks of harm arising from the design of their platforms and take proportionate steps to mitigate those risks of harm', including risks created by algorithms, and strengthening Ofcom's role in developing risk profiles.

Most relevant to auditing algorithms are the Joint Committee recommendations that:

- Government should publish an assessment of Ofcom's audit powers compared to other regulators, including the Financial Conduct Authority and Information Commissioner's Office, to reassure parliament that Ofcom has sufficient powers. Ofcom would be required to report to parliament on its use of these powers after six months (Recommendation 78, Paragraph 339).
- There should be a statutory responsibility on the largest and highest-risk service providers to commission annual, independent, third-party audits of the effects of their algorithms, their risk assessments and transparency reports (Recommendation 79, Paragraph 340), and the outcome of these annual audits should be required to be included in the transparency report (Recommendation 102, Paragraph 410).
- Ofcom should have explicit powers to review these audits and undertake its own audits. Ofcom should also develop a 'framework for the effective regulation of algorithms based on the requirement for, and auditing of, risk assessments' (also Recommendation 79 as above).[94]

These are sensible recommendations. The government should amend the draft Bill to clarify that Ofcom would have the powers, or even be required, to test and audit algorithms used by regulated service providers, often before something goes wrong, and on a continuing basis. That includes Ofcom having the power to request the necessary data and information on a longitudinal basis. Ofcom should also be required to report transparently on its work on algorithmic audits. The government should also ensure Ofcom is adequately resourced to hire and develop the staff, tools and other infrastructure necessary to conduct algorithmic audits on an ongoing basis.

[94] Joint Committee on the Draft Online Safety Bill, 10 December 2021, Draft Online Safety Bill, https://committees.parliament.uk/publications/8206/documents/84092/default/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Regulated service providers should be required to make data available to third party researchers

Granting Ofcom stronger powers and a clearer remit is necessary, but not sufficient, in testing and auditing algorithms. The wider 'ecosystem of inspection' – including academic and civil society institutions with the capability and capacity to research content-related algorithms and their effects – also need access to data from social media companies[95]. This has been a controversial subject in recent months, with Facebook restricting access to researchers studying its platform.[96]

At present, clause 101 of the draft Online Safety Bill requires Ofcom to produce a report about researchers' access to platform data. Several civil society organisations have called for trusted experts and academics to have greater access, including the Ada Lovelace Institute;[97] Demos, in their own submission and in a report with Digital Action, Doteveryone and others;[98] and Reset, who also note that transparency powers should be extended to include sharing data with accredited researchers, which would align the Online Safety Bill with the EU's Digital Services Act.[99] Melanie Dawes, chief executive of Ofcom, also raised this point in evidence to the Joint Committee and worried that UK researchers would be disadvantaged. She called for the independent research access provisions to be toughened.[100]

The Joint Committee recommends that Ofcom should start work 'as soon as possible' on a report about access to data for independent researchers, and have the powers to put recommendations from that report into practice. The Joint Committee also sets out other recommendations about service providers having to conduct risk assessments about opening up their data to third parties, and for Ofcom to annually

---

[95] Ada Lovelace Institute, September 2021,Written evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/writtenevidence/39256/pdf/

[96] Reuters, 4 August 2021, 'U.S. lawmaker says Facebook move to cut off researcher access is "deeply concerning"', https://www.reuters.com/technology/us-lawmaker-says-facebook-move-cut-off-researcher-access-is-deeply-concerning-2021-08-04/

[97] Ada Lovelace Institute, September 2021, Written evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/writtenevidence/39256/pdf/

[98] Demos, 28 September 2021, Written evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/writtenevidence/39336/html/; Demos, Doteveryone, Digital Action, Open Rights Group, Global Partners Digital, Institute for Strategic Dialogue, April 2020, Algorithm inspection and regulatory access, https://demos.co.uk/wp-content/uploads/2020/04/Algo-inspection-briefing.pdf

[99] Reset, 27 September 2021, Written evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/writtenevidence/39303/pdf/

[100] Ofcom, 1 November 2021, Oral evidence to the Draft Online Safety Bill Joint Committee, https://committees.parliament.uk/oralevidence/2934/pdf/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

assess what data should be made available to third parties. While these are welcome, they do not go far enough.

The draft Online Safety Bill should be amended to require social media platforms to give accredited researchers access to data necessary to understand the operation of their algorithms. Ofcom should be empowered to design and oversee an accreditation regime in concert with the other organisations currently listed in clause 101 – namely the Centre for Data Ethics and Innovation, UK Research and Innovation, the Information Commissioner's Office, and other experts.

Action for government Amend the Online Safety Bill to clarify and strengthen Ofcom's powers on algorithmic testing, audit and inspection, and to provide for a regime of accredited researcher access to platform data; ensure Ofcom is adequately resourced to exercise these powers.

Action for parliamentarians Ensure the Online Safety Bill is amended so that Ofcom has the power to test, audit and conduct research on algorithms.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 9: Secure public confidence in how elections are protected through transparency

Introduce a public protocol for elections and ensure the Online Safety Bill strengthens protections for democracy

Recommendation The Online Safety Bill should improve democracy and address harms to democracy including protecting against harmful misinformation and disinformation in elections. The Government should also establish a UK Critical Election Incident Public Protocol to secure public confidence in how elections are protected, given they are vulnerable to interference.

Resolve confusing concepts around democratic content and political debate

The draft Online Safety Bill places a duty on providers to protect democratic content. Yet the definition of "content of democratic importance"[101] is not sufficiently clear about what "is or appears to be specifically intended to contribute to democratic political debate". This lack of clarity has the potential for serious and unintended consequences, including harmful misinformation and disinformation.

The explanatory notes to the draft Online Safety Bill [102] offer just two kinds of examples: 'content promoting or opposing government policy' and 'content promoting or opposing a political party'. This raises serious questions about what else may or may not fall within the definition. The press release for the draft Online Safety Bill added that such content could be 'ahead of a vote in Parliament, election or referendum, or campaigning on a live political issue'. This raises the prospect of protection being afforded to politicians and political campaigners but not the public,

[101] The Department for Digital, Culture, Media and Sport, May 2021, Draft Online Safety Bill, Part 2, Section.13(6)(b), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

[102] The Department for Digital, Culture, Media and Sport, May 2021, Online Safety Bill, Explanatory Notes, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985031/Explanatory_Notes_Accessible.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

including it seems in an election. No further satisfactory explanation of these concepts has emerged during the pre-legislative scrutiny period.

The Joint Committee agreed with Full Fact, and many others, about the lack of clarity around this type of content. The pre-legislative scrutiny body felt 'that "democratic importance" may be both too broad – creating a loophole to be exploited by bad actors – and too narrow – excluding large parts of civil society'. It has recommended that the existing protections around content of democratic importance (Clause 13) should be replaced by a single statutory requirement to have proportionate systems and process to protect 'content where there are reasonable grounds to believe it will be in the public interest', and that Ofcom should produce a binding Code of Practice on steps to be taken to protect such content and guidance on what is likely to be in the public interest.

This may be a step forward, but without further exploration of what this may look like in practice, it is difficult to judge how workable the proposed solution might be - even with fast appeals processes and Ofcom guidance about systemic, unjustified removal of 'public interest' content (something the Joint Committee point out would be 'failure to safeguard freedom of expression as required by the objectives of the legislation').

Address democratic harms and election integrity

On democratic integrity, the Government appears resistant to tackling societal or collective harms without a clear link to individual harm. Though the Government is aware such threats and risks are real (indeed, they have teams that work on this issue), they have indicated that foreign state disinformation campaigns during UK elections will be out of the scope of the Online Safety Bill.

We do not believe it is right that the national security and other implications of disinformation campaigns during UK elections are out of the scope of the Online Safety Bill. Full Fact has been calling for the Online Safety Bill to be strengthened and amended to improve democracy and address harms to the democratic process, including protecting against harmful misinformation in elections. The Joint Committee agrees. It says: 'Disinformation and misinformation surrounding elections are a risk to democracy. Disinformation which aims to disrupt elections must be addressed by legislation. If the Government decides that the Online Safety Bill is not the appropriate place to do so, then it should use the Elections Bill which is currently making its way through Parliament.'

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

The Prime Minister assured Parliament in March 2021 that the Online Safety Bill would contain sufficient powers to tackle collective online harms, including threats to our democracy[103]. The Government must revisit this area and provide greater clarity on which legislative vehicle it intends to use to tackle disinformation during elections in particular.

In addition, in recommending that the Bill includes a specific responsibility on service providers to have in place systems and processes to identify reasonably foreseeable risks of harm and to mitigate them, the Joint Committee have said that Ofcom should be required to produce a mandatory Safety by Design Code of Practice on this, including that service providers have in place 'special arrangements during periods of heightened risk such as elections.'

The Joint Committee also set out their views on how disinformation about election administration might be considered in the Online Safety Bill as well as election material funded by a foreign organisation targeting voters in the UK or failure to comply with the requirement to include information about the promoter of that material in the Elections Bill (see also below on the latter).

Establish a UK Critical Election Incident Public Protocol

There may come a time during an election when the public needs to be warned about a specific threat identified by the security services. However, at present, the decision would be up to the government of the day, which would be put into a difficult position and would likely be seen as conflicted.

In Canada, this problem has been solved by setting out a public protocol - the Critical Election Incident Public Protocol (CEIPP)[104] - for handling such situations. The idea being to depoliticise a key area where a general election may be vulnerable to interference and require a solution to protect and defend electoral systems and processes.

The purpose of the protocol is to determine whether to inform the public that an incident that threatens the integrity of an election has arisen. A panel of senior public servants determines whether a threshold has been met and, if so, informs the Prime

[103] The Prime Minister, Boris Johnson MP, House of Commons, 16 March 2021, Integrated Review debate, https://hansard.parliament.uk/commons/2021-03-16/debates/52D67D49-A516-4598-AC69-68E8938731D9/IntegratedReview#contribution-76EFB229-E887-4B38-BBBD-09B5E13FA760

[104] The Government of Canada, 11 November 2020, The Critical Election Incident Public Protocol, https://www.canada.ca/en/democratic-institutions/news/2020/10/the-critical-election-incident-public-protocol.html

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Minister, political party officials, and the elections body.
Barring any national security considerations, the public are then informed of what is known about the incident and any steps they should take to protect themselves. Canada's successful model can be adapted for the UK to secure public confidence in how elections are protected.

The UK Government should develop and publish a similar protocol for alerting the public to incidents or campaigns that threaten the UK's ability to have free and fair elections. The Minister for the Cabinet Office has responsibility for both defending democracy and for electoral law and could initiate a process to bring about a UK Critical Election Incident Public Protocol.

The Elections Bill should provide an enabling environment for such a protocol to be agreed. It is important that the Elections Bill does, as the government has stated, work alongside measures in the Online Safety Bill and Counter-State Threats Bill 'to protect our globally respected UK democracy from evolving threats'. Coherence is required across different regulations and associated practices, including on known and foreseeable risks.

The draft Online Safety Bill contains a provision (under Clause 112 Secretary of State directions in special circumstances) enabling the Secretary of State to give Ofcom directions when they consider there is a threat to the health or safety of the public, or to national security. This clause, which requires significant scrutiny in Parliament if it is retained in the next version of the Bill, does not explicitly mention elections.

In the present draft Bill, Clause 112 is largely focused on directing Ofcom to respond to such a specific threat through the prioritisation of its media literacy functions, and requiring certain internet companies to publicly report on what they are doing to respond to such a threat.

We believe that democratic harms should be included in the scope of the Online Safety Bill given the regulation is to prevent harm emerging from internet companies' platforms. This could then interlock with other regulators and actors to address harmful misinformation and disinformation or other incidents threatening free and fair elections. In any case, there is a need to bring clarity to how the various pieces of related legislation will work together.

Alongside the development of legislation and regulation, a sensible precautionary provision is required to ensure that the public can be informed of any threats through a predictable and trusted process which shows how threats can be effectively mitigated. The public notification process was unused at the 2019 Canadian election

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

and this is, of course, the desired outcome. Independent evaluation demonstrated the benefits of providing a non-political mechanism for warning the public[105]. Election disinformation can succeed simply by sowing doubt, so such a protocol is confidence-building for the public.

As it stands a decision about whether to warn the UK public of a threat to our elections is as likely to be taken in California as Westminster – and either way, too late to protect confidence in the outcome of the vote. An election is possible at any moment. If conducted under current rules or indeed, as the present Elections Bill and draft Online Safety Bill envisages, it will be vulnerable to a serious incident with no protocol in place.

Increase online advertising transparency and ensure digital imprints work as they should

Full Fact, along with the Electoral Commission, the Committee on Standards in Public Life and many others, has been pressing for the introduction of digital imprints for a long time. We therefore welcome that The Elections Bill (Part 6) introduces a new long-needed requirement for digital campaigning material to display a digital imprint, with the name and address of the promoter of the material or any person on behalf of whom the material is being published, and who is not the promoter.

As the Electoral Commission has underlined, the definitions that set the scope of the requirements are highly sensitive and there is a risk of unintended consequences and loopholes[106]. The government and parliament need to ensure the Bill is amended so that compliance is required in all possible instances.

Post-legislative scrutiny of this part of the resulting Elections Act legislation is required after the next general election. We urge the government and relevant bodies including those in parliament such as the Public Administration and Constitutional Affairs Committee to make arrangements for this to happen. Stakeholders should seek to build an evidence base so that the next government, relevant committees and other actors can make an informed assessment about what further changes may be required for a robust system.

---

[105] The Government of Canada, 11 November 2020, Report on the assessment of the Critical Election Incident Public Protocol, https://www.canada.ca/en/democratic-institutions/services/reports/report-assessment-critical-election-incident-public-protocol.html

[106] The Electoral Commission, 5 July 2021, Introducing digital imprints, https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-views-and-research/elections-bill/introducing-digital-imprints

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Ensure the policies of online platforms are positive for UK elections and set by a transparent democratic process.

Social media platforms play a very significant role in elections, and whilst government and regulators focus on official campaigns and associated rules, internet companies have their own policies which they enact around elections far beyond this.

- YouTube's election policies[107] include that it will 'reduce the spread of election-related misinformation'.
- Facebook briefed the press ahead of the last UK election on its policies which included new measures[108]. These included ad transparency, intended action to prevent election interference such as taking down fake accounts as well as the work of their election team and the company's policy in a number of areas related to political speech and political advertising.
- Twitter, another soon-to-be UK regulated company, has UK election policies[109] that include election-related misinformation mostly around misleading people about voting.
- TikTok has its global policies applied to the UK[110].

Whilst it is welcome that internet companies have taken measures to increase transparency on their own, the violent attempt to overturn a democratic election at the US Capitol on 6 January 2021 highlights how individual, inadequate policies and action on election-related misinformation and disinformation can have very serious consequences for democracy. US fact checking organisation PolitiFact named inaccuracies relating to the Capitol attack 'Lie of the Year'.[111]

---

[107] YouTube, How does YouTube support civic engagement and stay secure, impartial and fair during elections?, accessed 31 January 2022, https://www.youtube.com/intl/ALL_uk/howyoutubeworks/our-commitments/supporting-political-integrity
[108] Meta, 7 November 2019, How Facebook Has Prepared for the 2019 UK General Election https://about.fb.com/news/2019/11/how-facebook-is-prepared-for-the-2019-uk-general-election/
[109] Twitter, 11 November 2019, Serving the public conversation for #GE2019, https://blog.twitter.com/en_gb/topics/events/2019/serving-the-public-conversation-for-ge2019
[110] TikTok, Election Integrity, accessed 31 January 2022, https://www.tiktok.com/safety/en-us/election-integrity/
[111] Poynter, 15 December 2021, PolitiFact's 2021 Lie of the Year: Lies about the Jan. 6 Capitol attack and its significance, https://www.poynter.org/fact-checking/2021/politifacts-2021-lie-of-the-year-lies-about-the-jan-6-capitol-attack-and-its-significance/

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

This underlines why the UK's election rules should be consistent across platforms and set through an open transparent democratic process, not just decided in the terms and conditions of individual platforms as they see fit.

In Canada, alongside supporting its protocol, platforms made a public commitment to work together to ensure principles of integrity, transparency and authenticity were in place to support healthy and safe democratic debate and expression online. This public declaration[112] was made with the government and set out accountabilities to citizens and civil society. This offers one model of at least some greater alignment to address the fact that harmful misinformation and disinformation can spread on platforms in ways that can undermine elections and democratic institutions, and forment societal tension.

The draft Online Safety Bill in the UK differs from the EU Digital Services Act (DSA), which does expressly address potential risks to electoral processes (in its Article 26). Large platforms are required to include 'actual or foreseeable effects related to electoral processes' in their risk assessments. The inclusion of harms to electoral processes in the DSA but not, at least presently, in the UK draft Bill, underlines the extent to which there are active choices to be made in law and regulation on ways to secure public confidence in how elections are protected through transparency.

The draft Online Safety Bill and associated measures currently give little assurance that election integrity will be strengthened for future elections. We set out above why a protocol is needed when an election becomes a serious information incident, but this alone is not enough for the public to be confident that any election is protected even when public safety is not at risk or foreign actors are not involved to any great degree in interference.

The Online Safety Bill should match the proposal outlined in the EU's Digital Services Act to include provision for Category 1 service providers to be required to risk assess the functioning and use of their services that leads to widespread dissemination of information which has a negative effect on electoral processes.

[112] The Government of Canada, 18 August 2021, Canada Declaration on Electoral Integrity Online, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/declaration-electoral-integrity.html

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Work towards elections where more people choose to vote and every vote is an informed vote

As we set out in our publication *Tackling Misinformation in an Open Society* (2018)[113], when we think of harm that may arise from misinformation in relation to democracy there are various areas of concern. There is election interference, which the protocol proposed here is part of addressing in relation to disinformation. And there is also disengagement from democracy, which can include abuse of power and factors of distrust leading to reduced participation, trust and consent around the democratic process of elections.

Attempts to disrupt the process or outcome of elections and democratic choices now take place in a landscape transformed by social media. Harmful misinformation and disinformation often have wide reach during elections (although what happens between elections may be just as important as what happens during official campaign periods).

Politicians misleading the public is a harmful and often ignored form of misinformation with social media offering new techniques to a range of political actors. Open democratic societies must be built on a strong foundation of trust. Trust is easier to erode than it is to build, especially at a time when information sources are expanding and held less in common, making it harder than ever for people to know where to place their trust. A risk is that people simply switch off.

Addressing election-related misinformation or state-sponsored disinformation should be seen as part of a wider effort to work towards elections in a digital era in which people have access to good information and do want to exercise their vote, and when they do, be informed in making their choice.

Action for government

- Revisit the definition of 'content of democratic importance' in the Online Safety Bill and ensure that it does not create unintended consequences, including legitimising disinformation in elections.
- Establish a UK Critical Election Incident Public Protocol, preferably amending draft legislation to establish transparent protocols for responding to

[113] Full Fact, 'Tackling Misinformation in an Open Society', 2018, fullfact.org/media/uploads/full_fact_tackling_ misinformation_in_an_open_society.pdf

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

disinformation and misinformation incidents in the Online Safety Bill (or in the Elections Bill)

- Clarify how the Online Safety Bill will work alongside the Elections Bill
- Include democratic harms in the Online Safety Bill
- Ensure that UK election policies are consistent across platforms and set through an open transparent democratic process.

Action for parliamentarians Ensure the Online Safety Bill is amended in ways that improve democracy and public debate, protect the integrity of elections, and interlock clearly with other legislation, including that on elections.

Action for the regulator Ofcom should seek to clarify its role as a regulator in relation to democracy and what it is being asked to regulate.

Action for platforms Develop transparent policies to help secure public confidence in UK elections, including arrangements for a UK protocol.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Chapter 10: Continue to ensure the supply of high quality news

The law should require a minimum supply of high quality news on Category 1 internet services

Recommendation The law requires a minimum supply of high quality news on public service television. This should be extended to Category 1 internet services.

Parliament has previously recognised the need for news as part of a healthy society. For example, the Communications Act 2003 requires it as part of public service television output. There are similar requirements on the BBC through the Charter and Agreement.

As the relative share of attention in legacy media declines, and as audiences fragment, we recognise the erosion of the shared reality that comes from shared access to news. That has consequences for our democracy and society more generally.

We believe that Parliament could consider whether a similar requirement to include news content should now be applied to the largest internet companies ('Category 1' in the draft Online Safety Bill) so that internet users are exposed to news in a similar way that broadcast audiences are. It is far better to pre-empt problems of misinformation by making good information readily available than to respond later with measures that restrict freedom of expression, and extending news provision in this may be one pathway to shift the balance towards proportionate measures.

There are two reasons for this.

The first reason is to nurture democracy by supporting an informed public, which is a long-established goal of the law. Section 279 of the Communications Act 2003 ("News and current affairs programmes")[114] provides for regulatory conditions to ensure that certain television services include high quality news and current affairs content.

[114] UK Government, 2003, Communications Act 2003, https://www.legislation.gov.uk/ukpga/2003/21/section/279

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

This is an uncontroversial principle: Parliament should never seek to control what news people are exposed to, but in seeking to ensure that high quality news is available it is simply acting to nurture and protect democracy.

The second reason is to protect democracy from misuse of the power that Category 1 internet services have. That is a new but real and clear threat. Whoever has the power to define our information environment has the power to shape our democracy.

Facebook dramatically demonstrated that power when in 2017 they decided to alter their algorithms to reduce the reach of political news. It has not previously been possible for a single decision maker to make such a powerful decision about news distribution without oversight and it is a serious concern with serious consequences for democratic debate.

In 2021, Facebook acted again deliberately to reduce the amount of political content in people's feeds. They said that "These changes are in response to common feedback from our community... One of the themes we've heard is that some people feel that there's too much political content in their News Feeds." News has always competed with entertainment for attention, even on television and radio. What the law recognises in those contexts is that the average person having ready access to high quality news is a public good and not just a private matter.

Changes to the design of the products of internet companies can affect the news environment even when that is not the purpose of the change. In 2018, Facebook made changes designed to promote more interactions between individual users of their services.[115] A predictable side effect was to significantly affect the reach of news.

And deliberate changes can have unintended effects on the news environment too. As the Wall Street Journal reported in 2020: "In late 2017, when Facebook tweaked its newsfeed algorithm to minimize the presence of political news, policy executives were concerned about the outsize impact of the changes on the right... Engineers redesigned their intended changes so that left-leaning sites... were affected more than previously planned, the people said. Mr. Zuckerberg approved the plans."[116]

In the light of all this, the question is: why would Parliament leave it up to internet companies to exercise so much power with no accountability?

---

[115] Facebook, 11 January 2018, News Feed FYI: Bringing people closer together, https://www.facebook.com/business/news/news-feed-fyi-bringing-people-closer-together
[116] The Wall Street Journal, 16 October 2020, How Mark Zuckerberg Learned Politics https://www.wsj.com/articles/how-mark-zuckerberg-learned-politics-11602853200

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

If most people's 'news' consumption becomes partisan, inaccurate, and/or perhaps driven by overseas interests, it will have profound effects on our democracy. This is currently no safeguard to prevent private overseas decision makers driving exactly that kind of change.

Action for government Amend the Online Safety Bill so that Ofcom has similar powers to ensure a minimum provision of high quality news on Category 1 internet services as it does on public service television.

Action for the regulator Ofcom should use the powers it has to risk assess the impact of regulated services decisions about the supply of news to their users.

Action for platforms Platforms should recognise the distinction between news which would meet the requirements of due accuracy and due impartiality under the Communications Act, and other partisan or low quality news and current affairs output. They should seek to preserve a minimum level of high quality news.

A registered charity (no. 1158683) and a non-profit company (no. 6975984)
limited by guarantee and registered in England and Wales

Full Fact
2 Carlton Gardens
London
SW1Y 5AA

fullfact.org/contact

@FullFact

fullfact.org

Published by Full Fact, February 2022.
Published under the Creative Commons Attribution-ShareAlike 4.0 International License.
Cover photo: Zach Guinta on Unsplash