Postdigital Intimacies for Online Safety

Dr Lindsay Balfour
Dr Adrienne Evans
Dr Marcus Maloney
Dr Sarah Kate Merry
We would like to thank the contributions made to this report by all the participants and their organisations: Liz Ashall-Payne, CEO of the Organisation for the Review of Care and Health Apps (ORCHA); Heather Cook, Special Advisor at BigHealth and Health and Social Care Council Member at TechUK; and Carmel Glassbrook, Professionals Online Safety Helpline Project Lead at Southwest Grid for Learning (SWGfL); Morgane Taylor, European Lead for Public Policy at Bumble; Tallulah Belassie-Page, Policy and Campaigns Officer at the Suzy Lamplugh Trust; Zara Ward, Senior Practitioner at the Revenge Porn Helpline; Jim Pollard, Editorial and Creative Consultant, Men’s Health Forum; Ruth Pott, Head of Workplace Wellbeing, BAM Construction; Marcus Hurcombe, Belonging, Resilience and Vocabulary Project, Chilypep; Corey Sills, Belonging, Resilience and Vocabulary Project, Chilypep, Tim Allard, Development Manager, MensCraft; Mubeen Bhutta, the Head of Policy, Public Affairs, and Campaigns for Samaritans; Chris Thomas, Programme Lead for Online Excellence at Samaritans; and Maeve Walsh, a Policy and Government Relations Consultant and Associate at Carnegie UK Trust.

We are grateful to Research England’s Research Excellence Development Fund available at Coventry University, with which we have been able to undertake this project.

We would also like to thank: Kauser Husain, Research Delivery Support Partner; Holly Higgins, Senior Policy Advisor; and Rosamund Chester Buxton, Research Impact Officer. This report has been skillfully designed by Scott Davis at Twenty3Creative. It was launched at Coventry University, and we would like to extend our appreciation to all those who spoke at and contributed to the launch event, as well as for the care and thought that Rt Hon. Baroness Nicky Morgan has imparted in her Foreword.
It is a great pleasure to write the foreword to this excellent report. I would like to thank everyone who has been involved in thinking through the difficult and challenging issues raised here.

As someone who has played a role both in shepherding the Online Safety Bill on its path (originally called the Online Harms Bill when I was Culture Secretary) and is now involved in scrutinising the Bill as it makes its way through Parliament it can be very easy to get drawn straight into the detail. This report is a helpful reminder of the bigger picture about the regulation of our digital spaces.

It is quite true that the internet can be a force for good and the desire for a flourishing digital society is a noble aim. We cannot undo the invention of the internet, social media or the telephones and other devices we all carry around which enable us to access these platforms in an instant. But that does not mean that online and digital harms should be accepted without question in the name of progress and technological innovation.

The Online Safety Bill is a world-leading piece of legislation, and the role of Ofcom is critical. But legislators and regulators are undoubtedly playing catch up to the tech and social media platforms. The recommendations in this report are useful not just at this moment as the legislation is, hopefully, approved but also as the lengthy implementation process unfolds.

The report is right to remind us that VAWG has been deemed by the Government to be a national threat and yet the words ‘women and girls’ are not used in the current draft of the Bill at all. The legislation needs to protect not just children but all those who are vulnerable such as those with enduring mental health needs, which don’t just stop at the age of 18. And the research is also right to point out the continuing gaps, even after a lengthy and complex Bill has become law, such as the lack of regulation around digital health apps and data.

The findings set out in this report are useful for policymakers, legislators and anyone who cares about how our society is changing. The reminder to calculate the collective societal harms arising from the growth and constant evolution in technology-enabled abuse is very timely. And this research is particularly insightful as it was designed to hear directly from those affected as well as those who work in the areas covered.

The workshop participants often suggested ways to tackle not just the specific problem they were grappling with but the need for broader cultural change online. I am very grateful for the support for a VAWG Code of Practice to tackle the overall culture of misogyny and gender-based abuse online. Recognising that culture change must be achieved through collaboration as much as legislation reminds us of the work ahead. In the 21st century what happens online shapes our individual and collective wellbeing. For a healthier society overall we need healthier digital spaces too.

Nicky Morgan
The Rt Hon the Baroness Morgan of Cotes
House of Lords, May 2023
Table of Contents

ACKNOWLEDGMENTS 2

FORWARD 3

ABSTRACT 6

SECTION 1: POSTDIGITAL INTIMACIES FOR ONLINE SAFETY 7

SECTION 2: RESEARCH METHOD AND DESIGN 10

SECTION 3: FEMININE TECHNOLOGIES, DATA SURVEILLANCE, AND HARM REDUCTION IN HEALTH TRACKING APPS 12

SECTION 4: IMAGE-BASED AND TECHNOLOGICALLY-ENABLED ABUSE 17

SECTION 5: BOYS, MEN, AND ‘TOXIC’ COMMUNITIES 23

SECTION 6: MENTAL HEALTH AND VULNERABILITY IN ONLINE SPACES 28

SECTION 7: CONCLUSIONS AND RECOMMENDATIONS 34

REFERENCES 37
Abstract

This report offers a multi-sector response to the Online Safety Bill (OSB). The shape and content of the OSB has generated discussion amongst policy specialists, stakeholders and lobbyists in key services and sectors, political advisors and appointed representatives, and academics and researchers – as well as a general public interested in what the OSB will mean for people made vulnerable or at risk of harms online. We report on the discussions that took place in four co-production workshops with representatives from the areas of: intimate digital health tools and services marketed to those who identify as women; image-based and technologically-enabled abuse; “toxic” internet communities; and protections for people with mental health conditions and neurodiversity. As the OSB reaches the final stages of approval through the UK government, this report provides a response from people working in these areas, highlighting the voices and perspectives of those invested in ensuring a vibrant, equal, inclusive, and safe digital society can flourish. Our recommendations include the need for: robust, transparent risk assessment and frameworks for preventing harm that work across life-stages; going above and beyond the current OSB legislation to raise awareness and educate to reduce harms; recognition in the OSB and elsewhere of the national threat of Violence Against Women and Girls (VAWG); and, an increase in information sharing and working across sectors of the technology industry, service providers, and charity, law, and government to generate new approaches for a better future.
Section 1: Postdigital Intimacies for Online Safety

Introduction to the Online Safety Bill

The Online Safety Bill (OSB) is a piece of UK legislation, implemented by the communications regulator Ofcom, aiming to protect children and adults online by imposing a duty of care on social media services and search services, with fines of £18 million or 10% of a technology providers’ global annual turnover for breaching such obligations. The aims of the OSB date back to the publication of the 2017 Internet Safety Strategy green paper, followed by the 2019 Online Harms white paper, which identified that “appalling and horrifying illegal content and activity remains prevalent on an unacceptable scale.” After a period of consultation, in 2020 the Government gave a full response and commitment to regulation. The OSB was originally the responsibility of the Department for Digital, Culture, Media and Sport (DCMS), together with the Home Office. Since 2019, the Secretary of State for DCMS has changed several times, impacted by wider political changes and uncertainty, and in 2023 responsibility for the OSB was transferred to the newly-created Department for Science, Innovation and Technology (DSIT). However, as we write this, the OSB is currently progressing through the House of Lords, after which it will reach the final stages and be given Royal Assent. Ofcom will shortly thereafter take responsibility for drafting risk assessment, transparency reporting, enforcement guidelines, and other elements that allow the OSB to come into force, with these frameworks for reporting and enforcing the OSB to take shape between 2023 and the end of 2024. While we recognise that the OSB is likely to pass before this Report can have direct impact, we aim to have the gaps and opportunities we identify here formally recognised, and our recommendations taken up as a part of the implementation process, and subsequent legislation.

Wider implications and gaps

Over the last few years, regular news segments, television programmes, and newspaper articles have outlined the importance of the OSB for protecting vulnerable and at-risk online users, especially children, and thus have also raised awareness of several harms that people may experience through their engagements with online and digital technologies. Vital campaigns have lobbied for the legal recognition of specific harms. For example, teenager Molly Russell’s suicide in 2017 has been directly linked to self-harm content on the social media platforms Instagram and Pinterest, with the coroner in 2022 calling for better regulation, while her father criticised the pausing of the OSB in that same year as the Government sought to ensure ‘freedom of speech’. Others have noted trolling and hate speech as creating hostile environments online that require people have adequate legal protection, with the OSB shaping discussions from online racism in football, to the suicide of Love Island television presenter Caroline Flack following vicious online attacks, to the challenge of regulating hate speech propagated by figures like Andrew Tate and others like him. There is no doubt that the process of legislating the OSB has raised public consciousness around issues related to online harm, risk, and vulnerability.

---

1 The full current bill can be accessed here https://bills.parliament.uk/bills/3137
Other important campaigns have taken place around ‘epilepsy trolling’, where flashing images are sent to people with epilepsy to induce a seizure. Led by 11-year-old Zach Eagling, the practice will now be covered by ‘Zach’s Law’, as part of the OSB. Meanwhile, another new offence currently written into the OSB is the sending of photographs or film of genitals to “cause alarm, distress or humiliation”\(^1\), colloquially known as cyber-flashing, recognition of which is the result of substantial lobbying campaigns by a number of women’s organisations, service providers, academics, and members of the public (see Section 4 of this report for a discussion and links to relevant groups/projects).

However, a number of issues still remain. The OSB’s overwhelming remit is towards children and, while this is undoubtedly an important constituency deserving of protection, recent changes to the OSB fail to recognise how online harms occur across life-stages. For example, the removal of the category of ‘harms to adults’ (or ‘legal but harmful’) from the OSB has been widely criticised as an ideological move that will allow harmful content to persist. Yet, in research by Compassion in Politics, Clean Up the Internet, Fair Vote, and Glitch in 2021, 60% of the public believed freedom from abuse was more important than freedom of speech, and 69% wanted the OSB to contain protections for adults as well as children.

One significant issue has been the way the OSB elides a wide spectrum of online harms that are gender-related and target vulnerable adult populations including women and girls, at-risk men, adults with neurodiversity and/or mental health conditions, and those with other combined characteristics such as non-conforming gender and sexuality, as well as racial, ableist, and classist marginalisations. Violence against women and girls (VAWG) is not addressed and, although amendments have been tabled, the terms ‘woman’ or ‘women’ do not appear anywhere in the OSB. As a campaign currently being led by EE and Glitch reads: “262 pages. Zero mention of women and girls. The online safety bill must change,” while Baroness Nicky Morgan, member of the House of Lords, has stated that the OSB is “sorely lacking” in its provisions for women and girls. In her words, “with the recent wholesale removal of ‘legal but harmful’ content regarding adults in its latest iteration, women and girls have in fact lost protections committed to address misogynistic content” (emphasis added).

There are further concerns about the ability of the OSB to protect vulnerable groups, especially in our present context in which online hate is on the rise. For example, police data gained by Leonard Cheshire and United Response has identified a 52% increase in disability online hate crime in the year 2020-2021. Many groups have also noted an increase in the incidents of such crime and abuse during the UK Covid-19 lockdowns.

“With the recent wholesale removal of ‘legal but harmful’ content regarding adults in its latest iteration, women and girls have in fact lost protections committed to address misogynistic content”.

---

\(^1\) Online Safety Bill, https://bills.parliament.uk/bills/3137, Section 167, p. 143.
Another significant issue with the OSB is in its focus on ‘the online’, as opposed to the digital and the technological, and the way it is primarily concerned with content rather than on the systems, structures and affordances of how technology is designed. The OSB will have minimal impact on the development of new technology. For example, there are only limited mentions of ‘health’ in the OSB, and none of these relate to the dramatic growth of industries like Feminine Technologies (FemTech), explored in Section 3 of this report, or the increasing use of digital tools and technologies to deliver healthcare, which remain largely unregulated despite the potential vulnerabilities to mental and physical health, as well as risks to data privacy and protection. Similarly, the focus on large technology companies such as Meta (i.e. Facebook, Instagram), TikTok, and Twitter means that communities of hate will still be able to exist in smaller, dedicated online spaces, and will continue to appeal to precarious groups and at-risk individuals. This was raised by Baroness Anna Healy in the House of Lords during the OSB’s second reading, where she recorded that ‘involuntarily celibate’ or incel communities, which are discussed in Section 5 of this report, are “a threat to women but also to young men” and noted that the largest of these communities online also contains large amounts of content related to suicide and self-harm.

**This project and report**

For us – as researchers of ‘postdigital intimacy’ – the landscapes we have outlined above are intricately connected to one another, and to the OSB as it reaches its final stages. Our research is collectively interested in the way digital culture, including the online, has become increasingly embedded in the way we build relationships, interact, engage, and connect with each other. We work together on developing research that shows how what happens in digital, technological, and online cultures also shapes our health, wellbeing, and material worlds. Thus, the gaps we outline above cannot be understood separately, and require a cross-cutting analysis of online safety that recognises the multiple lenses and contexts through which someone could be at harm or made vulnerable by digital culture.

The aim of this project, therefore, has been to formulate a collective response to the OSB, working collaboratively across multiple sectors with a number of stakeholders. The project, funded by Research England through Coventry University’s Research Excellence Development Fund, develops discussion around four areas that we ourselves are currently researching, namely: intimate digital health tools and services marketed to those who identify as women; image-based and technologically-enabled abuse; boys, men, and “toxic” internet communities; and the benefits or otherwise of using online communities for mental health support. We recognise that further important areas need to be discussed, especially to foreground the gaps in the OSB around the harms of racism and transphobia, and how these interact with other combined characteristics. Where intersections within and between thematic areas emerged in discussion, we have highlighted them in the pages that follow. We have also proceeded in the hope that our response will see such gaps taken up within a wider remit of definitions of what online safety and online harms mean – including legislation that is separate to the OSB.

In the following section, we introduce our methods, which included stakeholder workshops with several groups and organisations. We then provide a discussion of each workshop, and the strengths, opportunities, concerns, and consequences of the OSB for the communities and groups that our stakeholders represent. We finish this report by outlining shared recommendations.
Section 2: Research method and design

This section details our research design, including objectives and methodology, workshop structure, and ethics approval.

The purpose of the project was to:

- Contribute to a wider understanding around issues connected to the Online Safety Bill (OSB) and online harms more generally;
- Co-build a response to the OSB with partners from health and technology industries, government, charity organisations, service providers, and advocacy groups;
- Influence the development of future and subsequent legislation around online safety particularly as it relates to marginalised groups, including women and girls and at-risk men, and in consideration of mental health and neurodiversity.

To this end, we engaged in a series of workshops to collaborate with industry, policy, service providers and charity stakeholders to develop a response and recommendations regarding the OSB. The project employed a co-production methodology to bolster interdisciplinarity, strengthening the link between research and practice and offering a unique co-design approach. This approach was chosen because it empowers stakeholders as collaborators rather than subjects. Co-production thus involves using creative methods that foster the building of relationships between stakeholder groups that have different perspectives and needs. It treats all stakeholders as collaborators in shaping the project, offering multiple pathways to contribution and impact, and helping balance power in multi-stakeholder groups. Co-production also increases credibility for the research as fair, ethical, and transparent, due to the involvement of stakeholders and attention to their concerns.

The value of a co-production approach in this project is that it allowed contributors a way to share stakeholder experiences and expertise that enable us to better understand how the current OSB has taken shape and what steps can be taken to ensure future policy reflects a broader and more inclusive set of terms. Rather than conduct academic research in a vacuum, these workshops were designed to ensure that those actively affected by (or who represent those affected by) the OSB have their voices heard. Through these workshops, stakeholders had the opportunity to speak directly of their experiences of the OSB and wider issues, as well as make recommendations. All sections of this report have been shared with our participants ahead of publication, providing a vital member checking device and ensuring that their views are accurately represented.
Our intention was that the project would be multi-vocal and bring together a cross-section of different perspectives, allowing us to provide a holistic response to the OSB and highlight areas for future collaboration. A total of four stakeholder groups came together for this project over the period of 9th March to 30th April 2023. The groups were:

- The digital health ecosystem, drawing on the expertise of Southwest Grid for Learning (SWGfL), Organisation for the Review of Care and Health Applications (ORCHA), and BigHealth;
- Image-based and technologically-enabled abuse, with contributions from Bumble, Revenge Porn Helpline, and the Suzy Lamplugh Trust;
- Boys’ and men’s groups and health organisations, including Men’s Health Forum, MensCraft, Chilypep, and BAM Construction;
- Sectors addressing disabled people and those with mental health disorders particularly vulnerable to harm in online spaces, with Samaritans and Carnegie UK Trust.

At each workshop, stakeholders were guided through a series of discussion points that addressed the purposes of this project. Thus, although these were tailored to the issues that concern each of our stakeholder groups and we allowed discussions to be guided by the participants, each workshop also spoke to: the strengths, gaps and opportunities of current policy and regulation, and what concerns participants had about each of these areas; what the consequences of the OSB and other frameworks might be for the areas and people that they represent; and what future changes they would like to see happen to generate a more vibrant, equal, inclusive, and safe digital and technological society.

We made a conscious decision to not record the workshops, but instead chose to note-take the discussions as they happened, with key quotes and insights member checked through the process of stakeholder peer-review as we drafted this report.

This project and its methods have been reviewed and approved through Coventry University’s formal research ethics procedure (ref: P147047). Participants received information sheets, signed consent forms, and were given the option to be anonymous. Stakeholders from all sectors worked collaboratively with the research team to produce this report, including the option to add, remove or correct content, enhancing value through continual partner engagement and strengthening existing networks across multiple sectors.
Section 3: Feminine Technologies, Data Surveillance, and Harm Reduction in Health Tracking Apps

The following documents information and feedback gained during a workshop on safeguards in (and lacking in) women’s digital health. This workshop was held on 9th March 2023 at the London offices of FemTech Lab, at The Exchange. Follow up virtual meetings and emails also occurred. Our project partners in digital health included Liz Ashall-Payne, CEO of the Organisation for the Review of Care and Health Apps (ORCHA); Heather Cook, Special Advisor at BigHealth and Health and Social Care Council Member at TechUK; and Carmel Glassbrook, Professionals Online Safety Helpline Project Lead at Southwest Grid for Learning (SWGfL).

The focus of this workshop was the relationship between gender and digital health technologies, and the extent to which provision should be made for such technologies within the remit of online safety. In its current form, the Online Safety Bill (OSB) has no mention of digital health at all, let alone any acknowledgement of the diverse ways in which gender intersects with intimate health, and intimate health data. While the participants of this workshop agreed that the provision for children’s safety online is important, they also felt that the current Online Safety Bill fails to address not only women’s digital health and FemTech, but digital health more broadly. Indeed, as Glassbrook of SWGfL pointed out, attempts to bring this Bill to fruition have resulted in a “watered down” approach to online safety.

Attempts to bring this Bill to fruition have resulted in a “watered down” approach to online safety.

In 2016, Ida Tin, the founder the digital Danish menstruation application Clue, coined the term “FemTech,” (Dodgson, 2020), a portmanteau of “feminine” and “technologies” that refers to the wide range of digital products designed with women’s health in mind.
What are the main concerns?

Regulatory practice around digital health consistency falls well below the pace of innovation, particularly due to the lack of requirement or quality assurance that is required to promote a health app on online stores offered through Apple or Google. As Ashall-Payne, CEO of ORCHA noted, currently only 9% of health apps available meet the quality thresholds determined by the NHS (this criterion is also known as the Digital Technology Assessment Criteria, or DTAC). This number has, in fact, fallen from last year, where the number of accredited apps was 20%. The consequences of so many digital health applications slipping through the cracks of quality thresholds should be immediately clear. Digital health providers are able to market a product that is potentially medically inaccurate, due in large part to (1) their advertising of “wellness” rather than medical services, and (2) the reality that the DTAC is strongly encouraged but not mandated. Moreover, under-qualified apps risk subjecting users to data breaches and third-party information sharing. Ultimately the figures posed by Ashall-Payne along with the narrative experiences of workshop participants confirm that many users are accessing FemTech applications that are uncertified and unsafe.

The gaps in regulation are particularly amplified in apps that are targeted to women, and the vast range of intimate health needs of those who identify as such. FemTech includes tools offered for a range of women’s health needs, including menstruation and ovulation tracking, diet and fitness, sexual health, pleasure, and wellness, contraception and maternal health and, less frequently but still importantly, tools for conditions such as endometriosis, polycystic ovary syndrome (PCOS), menopause, mental health, and more. Sadly, as the figures cited by Ashall-Payne confirm, FemTech products rarely meet the target for medical safety, nor do they offer an accessible data management strategy or commitment to protect women’s data from being sold to consumer-driven marketing schemes. In December 2018, for instance, London-based charity Privacy International reported that many well-known menstruation apps were regularly sharing user data with social media platforms. Of the 36 applications they tested, more than 61% immediately transferred data to Facebook when a user opened the app. More recently, with the overturn of Roe v. Wade and new prohibitions on abortion in the United States, menstruation and ovulation tracking applications have come under fire for not protecting their users’ data in the face of increased scrutiny over women’s reproductive health practices. In the weeks following the decision of the Supreme Court, the internet was flooded with calls for women to “delete your apps” in fear that intimate data could be sold, or subpoenaed. At the same time, it could be argued that FemTech is needed in situations where women have nowhere else to go for their reproductive health needs. The stakes are clear, especially with regard to safety and surveillance, and the potential for health apps to do more harm than good. In short, the failure to include women’s digital health within the remit of the OSB, particularly when more women than ever are turning to technology to meet their health needs, is a significant and potentially fatal oversight.

---

5 See also Asher-Hamilton and Reuter, 2022; Page, 2022; Wetsman and Song, 2022.
What are the roadblocks to online safety within the digital health ecosystem?

Stakeholders identified several significant barriers to safe digital health. These include:

- Lack of digital access, particularly among underserved and/or marginalised communities. This challenge is exacerbated without effective pathways to commercialisation that would see DTAC certified apps reimbursed for providing safe and inclusive access rather than passing along the cost of safety to the consumer (Cook).

- Lack of gender-specific research and investment (often referred to as the “gender data gap”). This is well supported in the sparse but impactful research around FemTech. Indeed, while a cumulative two billion dollars was invested in women’s digital health worldwide between 2013 and 2020, that represents less than 3% of total digital health investments, despite the fact that women make up 80% of the healthcare workforce, are responsible for 80% of healthcare decisions in their household, and spend 29% per capita more than men on general health.

- Fragmentation. While there are many players in the digital health market, the structure is one of fragmentation rather than collaboration or centralisation. This seems to mimic the challenges of digital culture more broadly. For instance, Glassbrook suggested that collaboration across social media has dissipated; instead, the OSB leaves the impossible and unsustainable task of regulating human behaviour up to individual platforms.

- Lack of strategy. Overall, policy and regulation surrounding digital health tends to be more reactionary than proactive. Often, it tends to forget about the “person” or “patient” who is being served and instead emphasises the process of innovation, fundraising, or commercial success (Cook and Ashall-Payne).
As of 2023, only 9% of digital health apps meet the NHS DTAC (Digital Technology Assessment Criteria) for quality assurance. In 2018, UK charity Privacy International found that 61% of the women's health apps they tested immediately transferred data to Facebook.

Roadblocks to online safety in FemTech
- Lag in regulatory practice means safety is outpaced by quick innovation.
- Lack of digital access, particularly among underserved and/or marginalised communities.
- Industry structure is one of fragmentation rather than collaboration or centralisation.
- Misguided focus on product and innovation rather than the person or patient.

FemTech and online violence
- 200+ mobile phone applications designed to prevent sexual violence available via the App Store and Google Play.
- Most are ineffective, heavily stigmatised, do not have adequate data privacy measures, and too-often assume that the perpetrator will be a stranger (Bivens and Hasinoff, 2018).
- 7 million unwanted pregnancies + 31 million occasions of gender-based violence.
- The potential result of 6 months of interruption to traditional healthcare services.
- "There is need for far more investigation into the intersectionality of gendered violence and its potential uptake as an aspect of digital health, how are webbased technologies positioned to overcome existing barriers to their use, particularly compared with nonweb-based options?" (Jewkes and Dartnall, 2019).

For our full report visit: https://tinyurl.com/4xws4eac
What are the next steps for FemTech and online safety?

A consensus emerging from the workshop was that regulation of digital health is not the only solution to the above challenges. While the OSB remains a significant opportunity to bring more awareness around the importance of safe digital health technologies, it is not the only pathway to impact and “single point solutions are not the answer” (Ashall-Payne). As such, the OSB and other legislation should work to make online safety in health technologies a priority, but what is really needed is a cultural shift and transformation in how we view digital health within the wider spectrum of online harm and safety. Moreover, the safety of women online, particularly when faced with harassment, gender-based violence (GBV) (including intimate partner violence) and invasions of privacy, is a critical health issue. FemTech products thus offer a complex site for thinking about gender-based violence as a critical health issue that is both exacerbated and potentially ameliorated by digital intervention. For instance, while there are over 200 mobile phone applications designed to prevent sexual violence available via the App Store and Google Play, most are ineffective, heavily stigmatised, do not have adequate data privacy measures, and too-often assume that the perpetrator will be a stranger. Moreover, there are concerns that such digital tools will be used by perpetrators of violence themselves. To leverage technology against GBV will require significant upgrades to current digital health regulation and far more investment in digital health as a critical aspect of online safety.

The Online Safety Bill thus represents a unique opportunity, but ultimately a missed one, to implement mandatory accreditation and bring safe digital health tools to those who need them most. As Ashall-Payne suggested, we need do not need to add more apps; instead, we need to make the safe and certified apps more readily accessible to a larger pool of users. Other workshop participants agreed – the current iteration of the OSB is truly a failed chance to see through the “noise” of a digital health market flooded with apps that do not live up to the standards anyone would demand in conventional health care. Feminine technologies offer the potential to combat gendered injustice and health inequalities, but recognition and regulation is needed to ensure such tools remain safe, effective, medically accurate, and data secure – all of which the current OSB fails to catalyse.

See also UNFPA, 2022.
This section discusses the results from the workshop on image-based and technology-enabled abuse. This workshop involved Morgane Taylor, European Lead for Public Policy at Bumble; Tallulah Belassie-Page, Policy and Campaigns Officer at the Suzy Lamplugh Trust; and Zara Ward, Senior Practitioner at the Revenge Porn Helpline. The workshop took place on 13th March 2023, at Coventry University Campus, London.

The focus of this workshop was based around the context of a growing awareness of the incidence and normalisation of image-based and technologically-enabled abuse. Examples of image-based abuse include manufactured ‘deepfake’ images, cyber-flashing, revenge porn and downblousing, where (often sexualised) images are taken, shared, edited and/or received without consent. Research in schools has shown that 76% of 12-18-year-olds had received unwanted sexual images, and in research commissioned by the feminist dating app Bumble, 48% of adult women aged 18-24 reported having received cyber-flashing images in the previous year. Both pieces of research identified the Covid-19 pandemic as having heightened the likelihood of cyberflashing occurring, since it created a context where people’s social and intimate lives became increasingly mediated through technology. EVAW and Glitch’s research has demonstrated that online abuse during the pandemic was particularly exacerbated for Black and minoritized women and non-binary people, demonstrating the need to thinking about combined characteristics and marginalisations. Moreover, in their testimony to the Online Safety Bill Committee, the Suzy Lamplugh Trust noted a 7% increase in stalking cases that included social media reported to the National Stalking Helpline. The Suzy Lamplugh Trust’s recent research shows that, of the people who had experienced repeated unwanted behaviour, 84% reported this taking place online, compared to 70% who experienced in-person behaviours.

Another issue raised both by campaigners and in research is the way technology is implicated in the practices of such abuse. Cyber-flashing, for example, often makes use of the technological functions of short-range wireless connections like Apple Airdrop and Bluetooth. Moreover, geolocation tracking technology that uses WiFi, Bluetooth and GPS, such as the Apple Air Tag – designed to help users keep track of items – has been used in intimate partner abuse, including behaviours that amount to coercive control and stalking. Yet, it is unclear how the Online Safety Bill will address broader issues of technologically-enabled abuse, which does not always employ the internet itself, but leverages the digital nonetheless.
What are the main concerns?
The participants noted some of the strengths of the OSB, including that it was ambitious and was the first step to challenging some forms of online abuse. Collectively, the workshop participants thought it was important that the OSB made technology companies responsible for attending to online harms and safety, formalising risk management and legal duties. Notably, this was seen as a positive since it reverses a trend whereby those who are made vulnerable by digital harms are also those made responsible for the issue.

However, there was also a risk that, as the process of engaging groups such as Bumble, Revenge Porn Helpline, Suzy Lamplugh Trust, and others through consultation and committee came to an end, the government would treat the OSB’s Royal Assent as “a tick and a pat on the back”. In other words, it was felt the Royal Assent of the OSB might signal the end of the discussion of online safety and issues would remain unresolved. There was also concern that abuses and harms would become folded into one another as though all could be equally addressed through the OSB. Participants felt that the significance of Violence Against Girls and Women (VAWG) as a national threat may not be adequately challenged by the OSB. As one participant noted, “tech companies are likely to choose the minimum option”, doing enough so that they are not financially penalised by the regulations, but not enough to fully protect people against online gender-based violence.

A significant concern was that priority has been given to freedom of speech, freedom of expression and anonymity, which could be misused, and that forms of gender-based violence would slip through the net via discursive arguments. A similar issue was raised over what Taylor from Bumble referred to as the “LOL clause”, whereby the intent to provide humour may be counterbalanced against the harm caused to the victim. For all the participants, the notion that humour is the main motivator of image-based and technologically-enabled abuse elides the sexism and misogyny that underpins these behaviours. Equally, it was noted that motive-based harms are connected to broader patterns of behaviour, and that what is happening digitally and online will have translatable real-life behaviours. Motive-based harms are connected to broader patterns of behaviour, and that what is happening digitally and online will have translatable real-life behaviours. It was considered that the OSB and other regulatory and legal frameworks do not account for such behaviours and beliefs, and consequently do not provide the necessary support to victims.
Several high-profile cases have emphasised the ‘life-ruining’ effects of being accused of sexual and other forms of violence, whether falsely or not, where victimhood is reversed, and accounts prioritise the perpetrator (especially when that person is in a position of power and privilege) and delegitimise the victim. In the workshop, the participants highlighted the way the victim will also be “hurting for the rest of their life”, especially when reporting such violence in itself can have re-traumatising and long-lasting effects. As Belassie-Page from the Suzy Lamplugh Trust noted, in cases of online stalking, the onus remains on the victim to collect the data, with often more than 100 instances of digital stalking by one perpetrator needed as evidence, even before a case is reported to police. Moreover, Ward from the Revenge Porn Helpline identified the way that, even with a prosecution against the perpetrator of revenge porn, the still and moving images often remain in digital spaces, and so have the potential to re-emerge over a victim’s lifetime.

A further concern was that the OSB would quickly become out-of-date and was ill-equipped to deal with present and developing abuses. Thus, the OSB will recognise cyber-flashing as an offence – although not without problems, including that intent to cause distress will be difficult to prove. Further, the workshop participants suggested that forms of abuse are constantly changing, enabled through, for example, manipulated images, AI-enabled harms, doxxing, forms of online fixated/obsessive behaviour, technologically-enabled public sexual harassment, or the growth of immersive technology (e.g. the ‘metaverse’) and how these are used for gendered, racialised and sexual abuse. There is also the technological capacity of screengrabs and websleuth-behaviour to be misused, without clear guidance about how this gets reported to, and by, platforms. Belassie-Page raised a concern that there was no way of knowing if someone online has a molestation or restriction order. Ward identified how the way revenge porn is experienced and reported can be based on religious, ethnic, and cultural differences. There was uncertainty about how the regulations in the OSB would practically be enforced. It was suggested that if the OSB overlooks important protected characteristics, it will not safeguard the most vulnerable people.

The workshop participants suggested that because of these concerns, the OSB is unlikely to protect women and girls from image-based and/or technologically-enabled abuse at a time when, as Taylor noted, both are “skyrocketing” – which puts added pressure on victims and victim/survivor services. It was also noted that much image-based and technologically-enabled abuse is now normalised and, without proper regulation, would feed into a lack of recognition and thus a lack of reporting. The wider societal effects include declining mental health, leading to withdrawal and silencing that has a broader impact on relationships, communities, and women’s equality, public visibility, and voice.

“Reporting such violence in itself can have re-traumatising and long-lasting effects. It also takes an industry to move the needle.”
What are the opportunities?

There was a collective agreement that what is needed is broader societal change; a general awareness raising and public pedagogy that “abuse is never ok”, and a wider public discussion about the impact of systemic sexism, misogyny and gender-based violence. However, as Taylor noted, “it also takes an industry to move the needle”. For example, Bumble have implemented practices and technological affordances that develop a safety-by-design approach. This includes software that allows users to participate in consent-based sharing of sexual images through blurring photographs and allowing users to toggle consent, meaning that consent can both be given and withdrawn. A further practice shared in the workshop was Bumble’s approach to reporting, where they begin from the perspective of believing the victim. An important part of this is building in signposting to services, and Bumble work alongside intersectional and survivor-led organisations like Chayn and their Bloom project, which offers courses, advice and one-to-one support for healing from trauma.

However, it was also noted that safety-by-design was not shared across the sector. What was needed was take-up of such practices and technological affordances, especially by larger companies like Google and Twitter. There was a sense that the tech industry knew there was a problem, but that they needed to implement innovative safety-by-design examples by other platforms to see the benefits. It was also recommended that there should be a mandating of clear process for online content to be removed, and of information sharing between platforms, including distributing examples of best practice or ‘gold standard’ affordances – and reflecting on the relative strengths and weaknesses of different tools and software.

Content moderation is a significant future direction, as well as whether this content should be moderated by people working for tech companies or by AI systems. Overall, it was proposed that human moderation supported by “block-first approaches using open-source technologies” were preferable. It was noted that, in some instances, AI was beneficial where harmful content online was vast but services were limited in their capacity to offer human moderation – the example given by Ward, for instance, was the case of exploitative or illegal pornography. However, it was also recognised that often AI was simply not qualified to recognise the complexity of abuse and gender-based violence. Participants suggested that AI moderation only had human-based input to go on, and a culture of sexism and misogyny may end up reproducing the same challenges evident in wider culture.

Another shared sentiment was that mainstream approaches to gender-based violence will not transform if change happens in silos. There was a need for more dialogue between victim support services and providers, the tech industry, and the police. Belassie-Page said that it was a “coin toss” as to whether or not a report would be taken seriously by the police, and a “boys will be boys” attitude that was reflected in wider culture, and which needs to change. It was identified that gender-based violence needs more recognition and real time intervention. One potential direction was the implementation of a VAWG Code of Practice.
Such a code of practice, building on the work of EVAW, Carnegie, Refuge, 5 Rights, Glitch and the NSPCC, with Professors Glynn and Woods, was one that the workshop participants saw as something that could enable dialogue and collaboration, connecting groups and services committed to make such a culture change, and allowing them to work together towards a shared goal and future.

**What are the future directions?**

While overall it was evident that the participants in this workshop had several concerns about the OSB and other current regulation, there was a sense that there are future approaches that could make a positive intervention into instances of image-based abuse and technologically-enabled harm. As highlighted throughout the discussion, these interventions need to be designed and implemented with a perspective that acknowledges the relationship between digital and real worlds, and that these abuses have lived, material consequences. As one of the participants said, “don’t talk to strangers” no longer works in a culture so imbricated in, and connected through, technology. It was also clear that future directions need a collaborative, information sharing approach. If we are to “move the needle”, the wider culture of sexism and misogyny that has shaped gender-based violence needs to be recognised and challenged through wider public discussion and awareness raising, alongside a multi-perspective approach that productively brings together different sectors.
Technologically-enabled violence and online safety

48% of women aged 18–24 report having received cyberflashing images in one year (Bumble, 2021)

84% of unwanted repeated behaviour happens online (Suzy Lamplugh Trust, 2023)

Roadblocks to online safety

- Violence Against Girls and Women (VAWG) is a national threat
  Current regulation is unlikely to protect women and girls from image-based and/or technologically-enabled abuse at a time when both are "skyrocketing"

- Ideas that humour or freedom of speech/expression are the main motivators of image-based and technologically-enabled abuse elides the sexism and misogyny that underpins these behaviours

- Legislation like the OSB will quickly become out-of-date and is ill-equipped to deal with technological change and present and developing abuses.

Laws and Legislation at a glance

262 pages in the OSB

100 incidences of stalking needed before stalking is reported to the police, leaving owness on survivors to collect data, remember details, and relive trauma

"Coin toss" how a determination is made whether of not reports of abuse are taken seriously by police

Next steps

- Broader societal change; a general awareness raising and public pedagogy that "abuse is never ok", and a wider public discussion about the impact of systemic sexism, misogyny and gender-based violence;
- Advocacy and implementation of a safety-by-design approach by the tech industry;
- Adoption of the VAWG Code of Practice into the Online Safety Bill.

For our full report visit: https://tinyurl.com/4xws4eac
Section 5: Boys, men, and ‘toxic’ communities

This 30th March 2023 workshop centred on boys, men, and online harm, with a principal focus on how to combat the online propagation, especially among cisgender-heterosexual cohorts, of ‘toxic’ masculine ideologies. These are defined as ideologies espousing anti-feminist and misogynistic, and more broadly anti-social, views that are harmful to both girls and women, and boys and men.

Contributing project partners included: Jim Pollard, Editorial and Creative Consultant, Men’s Health Forum; Ruth Pott, Head of Workplace Wellbeing, BAM Construction; Marcus Hurcombe and Corey Sills, Belonging, Resilience and Vocabulary Project, Chilypep; and, in a one-on-one follow up session, Tim Allard, Development Manager, MensCraft. The focus on boys and men as potential perpetrators of online harm uniquely positioned this workshop in relation to the others’ focus on protecting victims, lending it relevance to the issues highlighted elsewhere in this report. Beyond the focus on toxic online spaces, practitioners were encouraged to raise any other issues they deemed important.

What are the core issues?

When asked what the core issues are vis-à-vis the workshop’s stated aims and focus, discussion immediately turned – and to an extent remained throughout the workshop – to the broader contemporary context in which boys and young men are developing their social attitudes and practices, and their sense of identity more fundamentally. Sills, whose work with Hurcombe at Chilypep aims to foster higher levels of emotional literacy among boys and young men, was first to contribute, establishing the broad sociological focus by noting that any issues we might discuss were, first and foremost (and for better or worse), deeply tied to the intergenerational socialisation of boys by their fathers (including, importantly, in absentia) and other key male role models in their lives.
Attention then collectively shifted to notions of masculinity, and how boys and young men struggle to navigate ‘what it means to be a man’ in a contemporary context in which, on the one hand, traditional ideals and expectations are increasingly discouraged (e.g. aggression and stoicism) or more difficult to achieve (e.g. secure employment and meaningful intimate relationships); and, on the other hand, new and constructive ways forward remain unclear and contested. This has led to what Pott referred to as widespread “confusion” among boys and young men and what Hurcombe referred to as a generation of “lost boys”, diagnoses which resonated with others in the workshop. All agreed that toxic online influences such as Andrew Tate were merely stepping into this breach, deceitfully offering simple answers to the complex questions society-at-large was failing to answer. Acknowledging the indispensably positive role feminist thought has played in fostering much-needed debates around masculinity, Pollard expressed some unease over the tendency in these debates to unduly blame boys and young men themselves – especially when considering class and socioeconomic factors – for a set of culturally and historically entrenched issues of which they are also victims of a sort.

When prompted to consider issues of importance beyond the focus on toxic online spaces, various examples were highlighted, including: exploitative forms of pornography, and how this fosters problematic attitudes and expectations around sexual practices (among both boys and men); the popularity of content featured on video sharing platforms such as TikTok in which people are demeaned, ridiculed and bullied for comedic purposes; and the predatory financial practices built into the design of both video games and dating apps (of which boys and men represent the main paying consumers). Pollard was especially concerned with how the design of both hardware (i.e. mobile phones) and software aims to elicit ceaseless engagement among users that is fundamentally antithetical to physical and mental wellbeing – and that inevitably exacerbates the more gender-specific issues we explored elsewhere in the workshop.

Boys and young men struggle to navigate ‘what it means to be a man’ in a contemporary context in which, on the one hand, traditional ideals and expectations are increasingly discouraged; and, on the other hand, new and constructive ways forward remain unclear.
Issues relating to boys and men are either “not talked about” or, when they are, discussion veers unhelpfully towards a stigmatisation which only further isolates and disenfranchises.

**Masculinity, online safety and toxic cultures**

45% of men have a positive view of misogynistic online influencer Andrew Tate, saying ‘he gives good advice’ and ‘wants men to be real men’.

Daily references to dehumanising misogyny recorded online (Townsend, 2022)

**Roadblocks to online safety**

- The current OSB fails to adequately address ‘legal but harmful’ online content, especially in respect to adults
- Focus on content moderation is itself insufficient, and focused on symptoms rather than causes
- Emphasis on perpetrators of violence is punitive rather than rehabilitative or preventative

**Masculinity and mental health**

37% of boys and young men are experiencing mental health difficulties

**Barriers to asking for help**

- 30% feel weak or ashamed
- 21% worry people will laugh or think less of them
- 14% would feel less ‘masculine’

'Toxic masculinity' is stopping boys from seeking mental health support (Stem4, 2021)

**What is needed**

- Preventative and rehabilitative approaches to online toxicity, with consultation from men’s health and youth organisations.
- Digital media literacy – the capacity to interpret and evaluate information online, and make informed choices around content consumption – should be a fundamental component of both child and adult education.

For our full report visit: https://tinyurl.com/4xws4eac

---

Daily references to dehumanising misogyny recorded online (Townsend, 2022)

37% of boys and young men are experiencing mental health difficulties
Throughout this portion of the workshop, discussion regularly circled back to broader social and cultural contexts. Participants spoke of how masculinity was in a state of flux, and how these contemporary circumstances were fostering a generation of isolated and confused boys and young men uniquely susceptible to toxic influences, and other online harms. In this sense, what was occurring online was agreed by all to be ultimately understood as a product what was occurring offline; though Pollard, drawing on substance abuse as an analogy, emphasised the importance of acknowledging both the conditions which lead boys and men to harmful online practices and the ways in which platforms, apps and devices actively encourage these outcomes. With this proviso in mind, consensus was reached to view issues relating to boys, men, and online harm as a collision between a set of broader social and cultural conditions; and a rapidly evolving, and under-interrogated, set of digital technologies thrown into the sociocultural mix.

How are these issues presently addressed?

Having established across the preceding discussion the importance of focusing on the social and cultural drivers of online harm, the core shared response to the above question was that the issues relating to boys and men are either, to quote Pott, “not talked about” or, when they are, discussion veers unhelpfully towards a stigmatisation which only further isolates and disenfranchises. Reinforcing this, Allard expressed concern over the lack of “positive and constructive frames” in policy-related agendas, suggesting that they would be more effective in shaping attitudes and practices than condemnation and/or criminalisation. Compounding this view of policy-related debates was a similarly shared sense of frustration that men’s health practitioners, as natural stakeholders in issues of online harm and safety, had much to contribute but were not being offered room at the table. Furthermore, Pollard expressed a sense of men’s health groups and practitioners as being politically homeless: stuck between sensationalist voices on the right purporting to defend men’s rights (e.g. MP Nick Fletcher and his claim during a Westminster debate marking International Women’s Day that the introduction of a female ‘Doctor Who’ would exacerbate male crime rates), and the tenor of debate on the left which, as mentioned, tended to stigmatise and/or only broach boys’ and men’s wellbeing in so far as it impacted others.

In respect to the additional areas of concern highlighted – exploitative pornography, generalised internet ‘addiction’ stemming from software and hardware design, and the predatory financial practices widespread across apps and video games – participants were all too aware of the lack of regulatory frameworks ensuring safety and wellbeing. In respect to all three of these issues, Pollard expressed scepticism over the government’s willingness to act against the financial interests of digital service providers in favour of public health and individual wellbeing, evidencing its current perfunctory approach to online gambling. Such doubts are also supported by evidence such as the government’s 2022 decision to exclude video games’ gambling-style paid mechanics from the 2005 Gambling Act. In sum, the view expressed here was that economic interests unduly take precedence over public interests in policy and regulation, and any meaningful shift in balance towards the latter would be a welcome development.
Next steps?

What follows is a summary of recommended governmental approaches that participants felt would be most effective in grappling with the range of difficult issues explored in the workshop. Importantly, this section of the workshop began with a discussion of the participants’ views on the sorts of content moderation approaches which the OSB (insufficiently, as it is argued in this report) aims to address. In respect to online toxicity especially, there was a shared pessimism to such approaches as essentially ‘whack-a-mole’ or ‘band-aid’ (the facilitator’s articulations) solutions focused on symptoms rather than causes. Collectively, the workshop identified several avenues for potential intervention in relation to online harm and safety:

- **Investment in digital media literacy.** Digital media literacy – the capacity to interpret and evaluate information online, and make informed choices around content consumption – should be a fundamental component of both child and adult education in 21st Century British society.

- **Preventative and rehabilitative approaches to online toxicity.** Complimenting the above recommendation, and speaking to the work currently being undertaken by practitioners, the issue of online toxicity should be approached by government in the same way as other radicalising ideologies, such as those relating to terrorism and the Government’s Prevent Strategy – even though this strategy is not without its problems – with an understanding that vulnerability lies at its heart. Men’s health and youth practitioners should be meaningfully consulted, and provided with opportunities to share knowledge with tech industry representatives.

- **National coordination between groups focused on boys’ and men’s wellbeing.** To share best practice, and, as Pott suggested, minimise “duplication of efforts”, government should develop coordination strategies to make fuller use of insights from men’s health and youth practitioners. It should be noted that Allard (based on prior experience) expressed apprehension over the potential of such inter-organisational efforts to result in echo chambers and groupthink.

- **Stronger regulation of software and hardware design.** Vendors of digital products should be required to adhere to a set of basic mental wellbeing principles, informed by psychological and social scientific research, in all aspects of their design. Within this, government should reconsider its position on predatory financial mechanics in video games, beyond the 2005 Gambling Act’s remit.

In sum, participants saw all the issues raised as requiring a two-pronged approach which addresses both the social and cultural drivers of online harm, and the ways in which digital technologies (including but also beyond the issue of how speech and content are moderated) enable these harms to flourish.
Section 6:
Mental health and vulnerability in online spaces

This section summarises the outcomes of a workshop on online safety for people with poor mental health, which was held at Coventry University London Campus on 29th March 2023. The workshop was attended by Mubeen Bhutta, the Head of Policy, Public Affairs, and Campaigns for Samaritans, and Maeve Walsh, a Policy and Government Relations Consultant and Associate at Carnegie UK Trust. A further virtual meeting and email discussions also took place with Chris Thomas, the Programme Lead for Online Excellence at Samaritans.

The workshop and subsequent discussions concentrated on the reduced levels of protection in online spaces for adults who are vulnerable due to mental health problems, neurodiversity, or disability. At the point at which it was sent to the House of Lords, the Online Safety Bill (OSB), mentioned ‘disability’ (classified as “any physical or mental impairment”) only within the definitions of abusive content targeting specific characteristics, or content which incites hatred7. There was no mention of neurodiversity at all.

What are the strengths and opportunities of the OSB?

The workshop participants felt that there were many positive aspects to the OSB, not least of which is that there is clear cross-party support, as is evident in its long journey from the 2017 green paper to its current Committee stage in the House of Lords (as of April 2023). They agreed that it has strong foundations, and that despite the removal of risk assessments for adult users it remains fundamentally risk-based, and has the potential to be a powerful Bill, with scope for future amendments and revisions.

Other strengths include the clear recognition of the need to tackle illegal content online and the inclusion of new criminal offences including promotion of self-harm, false communication (where harm is likely or intended), and ‘epilepsy trolling’ (the sending of flashing images to people with epilepsy with the intent to cause seizures). The OSB will force companies to be open about, and accountable for, what goes on in their platforms, and thus enable Ofcom to provide evidence-based regulation and actions.

What are the gaps in the legislation?

Despite the acknowledged strengths of the OSB, the workshop participants noted that there are a number of omitted, or removed, aspects that are or may become problematic. Violence against women and girls and toxic masculinity were referenced as two of these significant omissions and, as such, are addressed elsewhere in this report. Bhutta, from Samaritans, noted that there is no acknowledgement of the fact that people all ages are at risk of harm from suicide and self-harm content, and while within the OSB suicide is a priority concern for children, this is not the case for adults. As Julie Bentley, CEO of Samaritans, stated: “You don’t stop having suicidal feelings or self-harming as soon as you turn 18 and this new law must help protect everyone, on any site, whether they are 16 or 66”.

The OSB is fundamentally designed to protect children, and protections for adults have been gradually reduced since it was first introduced. Indeed, over the course of its progression through the House of Commons, adult safety duties (i.e. the ‘legal but harmful’ provisions) were replaced with a ‘triple shield’, requiring platforms to:

- remove illegal content;
- remove content prohibited by the site’s own terms and conditions; and
- provide adult users with empowerment tools which enable them to avoid potentially harmful content.

The triple shield has significant limitations, particularly in regard to the third duty, when it comes to protection of vulnerable adults. Although children are automatically protected from potentially harmful content, adults will be required to take responsibility for their own protection, as the user empowerment tools will be toggled off by default. For adults who may not recognise their own vulnerabilities, including as a result of mental health problems or neurodivergence, this is likely to result in increased exposure to harmful material and, depending on the site’s terms and conditions, they may have no recourse.

Similarly, as part of the removal of the adult safety duties from the OSB, the requirement for platforms to conduct risk assessments for users aged over 18 no longer exists. This is significant, as it places the onus for protection from harm upon the users themselves and makes no allowance for those adults who do not have the capacity to do so due to neurodivergence, mental illness, or other vulnerabilities.

For adults who may not recognise their own vulnerabilities, this is likely to result in increased exposure to harmful material.
Moreover, the OSB focuses on ‘Category 1’ platforms – the largest user-to-user sites. Smaller platforms (Category 2B) fall outside the scope of the OSB’s primary protections. As Bhutta noted, access to these sites is expected to be managed through search engines (Category 2A), which have a duty to prevent users from finding some of the more dangerous or harmful sites. Without addressing this gap, users may have no protection from accessing smaller sites which contain harmful content or promote harmful behaviours.

Relatedly, there is a potential risk that user protection activities within Category 1 services may be paused as those platforms await Ofcom’s new codes of practice which will come into force once the OSB becomes law.

Other gaps discussed during the workshop were the lack of provisions addressing misinformation and disinformation, particularly in relation to health, and the need for digital media literacy provision. Indeed, these themes were raised across the four workshops and are reflected in our recommendations which follow in Section 7 of this Report.

What are the main concerns?

There was consensus among participants regarding concerns about the OSB. Although they agreed that the progress of the OSB has been slow, and it is a large and complex document, they also believed that if specific issues are not addressed within the OSB – and therefore do not require action from platforms – more delays and more harm will result, at least until the OSB is amended again. Bhutta remarked that legislation needs to be narrow to be effective, particularly when it relates to topics such as suicide and self-harm.
Nuance is important when considering the online safety of people who are neurodivergent or who have mental health conditions, and is admittedly difficult to address within a complex piece of legislation. For example, individuals who are in mental health crisis might make posts which appear to be harmful to a wider public, when in fact they are more likely to hurt themselves than others. Bhutta stated that there are forums and other spaces online which provide valuable assistance to people who are in crisis or who need peer support when they are experiencing self-harm or suicidal thoughts, and these spaces should not be made illegal. The content of support groups could be considered to be illegal when in fact they mitigate harm, or have a more nuanced relationship to potential harms – which might not be recognised by moderation tools. As Walsh (Carnegie UK Trust) observed, human content moderation is much more useful for issues relating to mental health and neurodiversity than AI moderation – but it is also more expensive, and leads to additional concerns regarding potential harm to the moderation staff.

There was some discussion within the workshop regarding the duties of Ofcom as the online safety regulator. It was noted that “there is a long tail” (Walsh) on the codes of practice and guidance which Ofcom has to produce, and indeed on legislation more widely. She noted that the evidence requirement is very important and that the delays to the passage of the OSB should mean that some of the policies are ready to go as soon as it is passed. There were some concerns that, even when the OSB has become law, lobbying will not stop and there will be pressure on Ofcom to reduce the robustness of its regulation.

Both workshop participants expressed their belief that, while the OSB can ultimately seek to protect individuals online, there are broader societal and cultural shifts which need to occur in order to provide a safer, less toxic, and more inclusive online environment.

There are wider concerns which need to be addressed with regard to protecting adults online. Walsh commented that even if the triple shield works it does not prevent that harm from happening, nor does it put any onus on platforms to mitigate the impact of its effect being felt by online communities, or to individuals from similar backgrounds to the user initially targeted. Essentially, “it does not address the toxicity of the wider environment; it just says that you, as a user, can protect yourself”.

Bhutta agreed that there has not been enough focus on the harm that one user’s freedom can cause to the wider population: “[It is] focused on one user causing harm to another user, not about societal impact”. Walsh gave the example of online abuse targeting women MPs: she noted that it is not just about an individual’s dislike of a particular MP, “it is about trying to silence her [and] her contribution to democratic discourse”. Both participants agreed that there is a cumulative impact on society that needs to be recognised within the regulation of online harms.

There are broader societal and cultural shifts which need to occur in order to provide a safer, less toxic, and more inclusive online environment.
Mental Health and Online Safety

83% of survey respondents reported that they had seen self-harm and suicide content on social media even though they had not searched for it (Samaritans, 2022).

77% of people with mental health conditions have experienced at least one potential harm online (Ofcom, 2022)

Omissions in the OSB

- Protections for adults have **gradually reduced** since the OSB was first introduced.
- The ‘triple shield’ has **significant limitations**, particularly in the case of **vulnerable adults**.
- There is no acknowledgement of the fact that **people of all ages are at risk of mental illness**.
- Protection from harm within the Bill is **focused on the individual**, not the wider population.

Mental health and harmful content

1 in 4 people in the UK will experience a **mental health problem** each year (Mind, 2020)

38% of adults reported seeing harmful content **within the last month** (Ipsos, 2022)

Next steps

- Reinstate the risk assessment requirements to the Online Safety Bill.
- Ensure that adult empowerment tools are **on by default**.
- Work towards cultural and societal shifts – offline influences online, and vice versa.

For our full report visit: [https://tinyurl.com/4xws4eac](https://tinyurl.com/4xws4eac)
What are the next steps for protecting adults with vulnerabilities?

The participants agreed that the two most important steps towards protecting adults with neurodiversity or poor mental health are to reinstate the risk assessment requirements which were removed as part of the adult safety duties, and to ensure that the adult empowerment tools are on by default, thus ensuring that everyone is protected until or unless they choose not to be.

As Bhutta suggested in the workshop, “the bare minimum of what the Bill should be doing is preventing the amplification and targeting [of harmful material]”, as seen in the case of Molly Russell (which we discuss in the introduction to this report, see also The Coroner’s Service report for more detail). Even if an individual is not looking for specific (harmful) content, they may be pushed towards such content based on what the platform’s algorithms think that they are interested in. If a user searches for that content deliberately, the platform still has a duty of care – but that is very different to someone being pulled into a world they were not necessarily looking for.

When the Internet Safety Strategy green paper was first published, its goal was to ensure that “Britain is the safest place in the world to be online”. This continues to be the stated aim of the OSB, but it remains to be seen, once the Bill has passed into law, whether that will be the case not only for children, but also for vulnerable adults.
Section 7: Conclusions and recommendations

In this report, we have sought to co-produce a collaborative and cross-sector response to the OSB. We have done so by looking to the future of policy in relation to online safety, with the intention that this report will become part of a collective effort towards a vibrant, equal, inclusive, and safe digital society. What is unique about this approach and the issues raised therein is that our workshop participants 1) represent not only the users of internet platforms, but those services, groups, and industry stakeholders that act on behalf of members of the public, and 2) embody a multi-vocal response to the OSB and shared concerns across different sectors, increasing our combined contribution to future directions in policy and legislation.

Our objective has been to interpret findings that reach across the contributions made here. From the discussion that took place in workshops, we have identified several recommendations. These are not the only ones that emerged through our discussion, but do reflect a shared recognition across workshops and thematic constituencies of where change needs to happen.

1. Robust, responsive, and transparent assessment criteria for technologies, apps, and platforms.

There was a sense across the partner groups that safety needs to be built into apps and platforms at design stage, rather than treated as an issue of removing/not removing harmful content, and that design should be undertaken with the user in mind, not the product itself. This could be implemented through assessment criteria that promotes safety-by-design frameworks and makes both criteria and compliance transparent and visible to users. While this is a challenge with emergent technologies and platforms, whose innovation outpaces ethical concerns, it is nonetheless imperative that design – particularly that which focuses on intimate and gender-defined health – builds safety, privacy, and harm reduction into its foundation. It was also suggested that guidelines and regulations needed to be responsive, rather than reactive, to new and emerging harms/abuses emerging from technological development and innovation. Assessments need to be adaptable and consider the technological and digital aspects of harm, alongside the online ones – especially where there is considerable overlap between technology, the digital, and the online, for example in technologically-enabled abuse, where mobile phones make use of digital photography or GPS to share content online and over short-range connections between devices.
2. Risk assessments for adults should be reintroduced to the OSB, and the user empowerment features included in the ‘triple shield’ should be on by default in all platforms.

While there was a shared recognition from all workshops that the protections that the OSB offer to children are necessary, this does not need to come at the expense of adults – and protections for both children and adults can be achieved in current and future legislation. Risk assessments were seen as important in mitigating vulnerabilities of particular populations, for example neurodivergent individuals with reduced awareness of risk, or adults in mental health crisis. It was recognised that the ‘triple shield’ would not by itself prevent harmful material from existing, nor would it fully stop harmful material reaching those made vulnerable by it. Having user empowerment tools on by default in platforms would protect those individuals who are more vulnerable to harmful content. In addition, it can be seen as a step towards a version of consent, if implemented correctly, so that consent could be given and taken away, as well as toggled between consent and non-consent. Such consent-based innovation would require the forms of robust and responsive assessment criteria noted above before being taken to the public – since it is also recognised that abuse within the current or suggested features was still possible.

3. Raising levels of awareness and education to ensure harm reduction.

As the OSB comes into force, it is an opportune time to invest in and support groups and organisations seeking to make positive changes in society by funding awareness raising and educational campaigns addressing all people, regardless of age. Relevant groups and organisations should be given opportunities, and the financial means, to coordinate their efforts in the name of online safety and engage in knowledge-transfer with representatives from tech industries. As stated earlier in this report, digital media literacy should be considered a fundamental component of the British educational curriculum, providing young people with the necessary tools to evaluate information online, and make informed choices around content consumption. Finally, this report has clearly established the need to focus on the broader social and cultural context which continues to enable forms of online harm to proliferate, and education and awareness initiatives should tackle these issues accordingly.
4. Formal recognition of VAWG and challenges to the wider culture of sexism and misogyny that shape gender-based violence.

Across the workshops, it was recognised that VAWG and gender-based violence should be recognised in the OSB and that women and girls should be named as a group particularly at risk of online abuse and harms – as an intensified risk that the research cited in this report makes clear. Collectively, we also call for protected and combined characteristics to be recognised in the OSB and in all future legislation relating to digital health, wellbeing and safety. This must happen alongside raising awareness and education, but specifically in relation to the wider cultural and societal impact of sexism and misogyny that effects mental health, leading to withdrawal and silencing that has wider societal impact on relationships, communities and women’s public visibility and voice. Support services need more funding, and a nuanced discussion of human and/or AI moderation needed to happen as the OSB is implemented. Finally, the VAWG Code of Practice needs to be adopted as part of the execution of the OSB. This requires ongoing support, development, and implementation across sectors, especially to take account of VAWG happening across online, digital and technological platforms.

5. Change will not happen in silos.

The OSB is just the beginning. While it usefully places responsibility within the tech industry, rather than victims, survivors, and vulnerable adults, meaningful and measurable change is going to need a multi-sector approach, emerging from policy and legislation. This will need to incorporate technology design (e.g. a safety-by-design approach), support for services, education, funding for academic research on mitigating harm, training and engagement in dialogue with the police and Crown Prosecution Service, public awareness campaigning, and the capacity and scope for Ofcom to draw on expertise and regulation from other sectors. Online harms need to be recognised in the future as interconnected and multi-issue, and the approach to these kinds of harms needs to acknowledge the digital and technological, including the relationship between hardware and software, algorithms and platforms, online and offline. Future directions should be responsive to technological and societal change to really make a difference to people’s everyday lives.
References


Asher-Hamilton, I. and Reuter, D. (2022). You shouldn’t feel you have to delete your period-tracking app because Roe v. Wade was overturned – but you should know the risks, expert says. Business Insider. Available at: https://www.businessinsider.com/tech/news/you-shouldnt-feel-you-have-to-delete-your-period-tracking-app-because-roe-v-wade-was-overturned-but-you-should-know-the-risks-expert-says-articleshows/92444585.cms


Bloom https://bloom.chayn.co


Chyan https://www.chayn.co

Compassion in Politics, Clean up the Internet, Fair Vote, and Glitch (2021). Public opinion on the Online Safety Bill. Available at https://d3n8a8pro7vhmx.cloudfront.net/cip/pages/304/attachments/original/1631280474/Public_Opinion_on_the_Online_Safety_bill_%284%29_%281%29_%281%29.pdf?1631280474%20


McGlynn, C. (2023). Twitter thread from Prof Clare McGlynn KC (Hon) @McGlynnClare. Available at https://twitter.com/McGlynnClare/status/1647887005592739840


Online Safety Bill. Available at https://bills.parliament.uk/bills/3137


Page, C. (2022). Supreme Court Overturns Roe V. Wade: Should you delete your period-tracking app?. TechCrunch. Available at: https://tcn.ch/3OZBtJ0


Suzy Lamplugh Trust submission to Online Safety Bill Committee (n.d.). Available at https://bills.parliament.uk/publications/47089/documents/2053


