Written evidence submitted by Gina Miller (OSB0112)

I am writing this submission from several perspectives - personal, as an investment professional, and as a social justice and transparency campaigner.

On the personal front, having been one of the most targeted and abused women across social media platforms[1], which resulted in the CPs bringing two landmark cases to court where the individuals were found guilty, I have experienced the emotional, social, and inter-personal damage of online abuse.

Closed Groups

The first case was for malicious communications on a closed Facebook group inciting physical harm against me which resulted in the conviction and imprisonment of Viscount St Davies but no action against Facebook. This was a closed group and the only reason I was made aware of the threat was because a member of the group become extremely worried and sent me a screenshot.

On another occasion, I met a member of another prolific Facebook closed hate group that were targeting me - https://www.bbc.co.uk/news/av/stories-52488074 - I was shocked by much of what he told me. I had presumed that such closed groups had a few hundred members at most. But I soon learnt they can have thousands, all discussing ways to do me harm and inciting others to do so. Such closed groups must come under the new legislation as they are breeding grounds for grooming and encouraging individuals to act dangerously and often criminally, in the real world. I was also told there is a huge amount of goading and upmanship that can lead to pressure on group members to carry out actions against targets of abuse.

There is also new data on the dramatic rise of online-linked sexual crimes against children with the number of reported cases of predators abusing children after contacting them online having risen 78% in just four years according to new data from the NSPCC, much of which occurs in private chat rooms, closed groups, and encrypted messaging[2]. These toxic, secret areas must be within scope of the legislation, not left up to providers to police.

Crowdfunding Platforms

The other experience I wish to share with the Committee concerns the setting up a GoFundMe page to raise *'£10,000 to Hire a Hitman to Kill Gina Miller'* which resulted in

---

[1] Anti-Social Media? by John Mair - https://www.worldofbooks.com/en-gb/books/john-mair/anti-social-media/9781845497293?gclid=EAIaIQobChMIsL-W7teD8wIVRYfVCh3AVQ8KEAQYAyABEgIIS_D_BwE

[2] https://news.sky.com/story/dramatic-rise-in-online-linked-sexual-crimes-against-children-leads-to-calls-for-tougher-regulations-12408264

prosecution and a derisory £200 payment to me for distress caused, but absolutely no action against the GoFundMe platform.

In terms of funding platforms, these should also be covered by the legislation as these platforms have enabled crimes including modern day slavery/trafficking, drug dealing, money laundering and scam charitable fundraising that were previously happening off-line but have now moved online. During the pandemic, we have seen great examples of humanity and people selflessly helping each other, but also increasingly on crowdsourcing websites like GoFundMe.com, where people can quickly host fundraising pleas to cover unexpected medical bills or personal tragedies. However, it is concerning that the platform does not verify individual requests, so there is no way to know if a person's story is real or a scam, yet it continues to make millions.

On both these occasions, as well as the other six 'cease and desist' letters issued by the Police to perpetrators of online abuse targeting me, not only did the Police teams I worked with say there was no legislation under which they could charge the social media platforms and but that funding for policing online crime was almost a major issue. The proposed legislation does not adequately address this funding issue and these platforms effectively escape any/all liability.

I would also suggest more work needs to be undertaken on the scope of the proposed regime. The fact that paid-for advertisements, "one-to-one live aural communications" (communications made in real time between users), though the exclusion applies if the communications consist solely of voice or other sounds and do not include any written message, video, or other visual images, appears to be a gap which could lead to unintended consequences.

The same is true with the significant power the Bill gives to the Secretary of State for Digital, Culture, Media and Sport to amend Schedule 1 to either add or remove services to the list of exemptions, based on an assessment of the risk of harm to individuals. This power would give the Minister a huge amount of discretion, which, if misused, could lead to policing private messaging and communications channels such as Messenger or Zoom. Questions about the effect of the Bill on encryption, security and privacy remain unanswered.

The scoping components of the Bill have other problems, too. The draft does not refer to "platforms", even though the government uses the term to refer to Category 1 service providers. This conflation of terms creates confusion. I accept that once the Bill is passed, the Secretary of State will prepare delegated secondary legislation and OFCOM will introduce codes of practice to specify different levels of duty of care and liability, but the extent and reach of duty of care in the Bill is unclear.

Protecting Children

I believe another flaw in the Bill is that it is attempting to treat children and adults the same online when we do not offline, or in other legislation. Rather than trying to work out what an appropriate way of helping to ensure that children's safety is developed to stop, for example, the shocking growth of self-harming, bullying, grooming, pornography and encouraging suicide, the Bill is simply saying we will treat adults and children all the same

and ask platforms to mitigate risks across all people in the same way. This is far too simplistic in my view and experience.

I also believe there is inadequate provision or clarity in the Bill for special needs or vulnerable adults. My eldest daughter, now 33 years old, has an academic/learning capacity of a six/seven-year-old and has been a victim of online grooming and abuse, yet platforms treat her as an adult due to her biological age. As a vulnerable individual, her characteristics make her and others like her, more vulnerable to online abuse. She has been asked to send explicit sexual images without understanding what she was being asked to do. We know that self-generated images account for a growing proportion of child/vulnerable abuse images, whether these are shared consensually or are the result of peer-to-peer grooming. This led to her being bullied, blackmailed, and lured to a meeting where she would have been taken, if we had not discovered what was happening. This was all happened on Facebook who refused to take down her page as she had lost the password, but being over 18 years old, they refused to let me take it down. They eventually did so only because I threatened to go to the press.

During the past year my [age redacted] daughter and several of her friends have experienced and educated me on the toxicity online around self-harming which I can only describe as a deeply disturbing epidemic of child mental health crisis, self-harming, eating disorders and now attempted suicide. I personally know of families where two or more children in the same family are being referred to child and adolescent mental health services but where services are so overwhelmed that children are having to wait for months or being cared for in centres miles away from their families. In some cases, children as young as five are being put on antidepressants while they wait to see mental health services. According to the NHS statistics, children are being prescribed antidepressants in record numbers. In 2020, there were 231,791 prescriptions for the drugs issued to children aged between 5 and 16. And a study in October 2020 by NHS Digital found that one in six children aged between 5 and 16 in England is "likely to have a mental disorder", an increase of almost half since 2017[3]. Of the families I have spoken to, they all say social media platforms contributed to their children's mental health issues – this simply cannot be allowed to continue.

I know from my daily contacts with parents and children, mental health services and specialist charities that we are living through a terrifying crisis, yet we know some of the main protagonists and do nothing whilst we allow them to decide the rules. There can be no more important duty placed on society than to protect our children from harm. To this end, the Online Safety Bill legislation must deliver a more comprehensive package of measures to keep children safe today and in the future. The legislation must impose a duty on technology firms to tackle cross-platform abuse where abusers exploit the design features of social networks to contact children, before coercing them to migrate to encrypted messaging or live streaming sites. I would also urge the Committee to hold evidence panels with parents of children in crisis institutions and the staff at such places – public and private.

[3] https://www.thetimes.co.uk/article/record-numbers-of-children-are-being-prescribed-antidepressants-88268m0rt

As the legislation currently stands, small but high-risk sites such as Telegram and OnlyFans could be excluded from having a duty to protect children from harmful content as the duty only applies to companies with a "significant" number of children on their apps. This could result in bigger platforms/technology companies diverting harmful content onto new, smaller sites.

I would also suggest a senior manager regime with sanctions for senior managers at technology firms who breach their child safety duties of care face fines, censure, with criminal sanctions for the most significant failings that put children at risk of significant harm. Recently, a report in the Wall Street Journal exposed that Facebook-owned Instagram had conducted internal research into the effect social media had on teenager users, which showed teenagers blamed Instagram for increased levels of anxiety and depression. Yet Facebook kept it secret and have sought to defend the indefensible[4]. In response, the US campaign group Fairplay said the news showed '*Instagram was no place for children'.* Fairplay also called on the US government to demand Facebook released its research and blocked its plans to launch Instagram Youth aimed at under 13s.

When you also consider the statistics, that most mental health problems are established at a young age, with 75% of mental illness (excluding dementia) starts before age 18[5]. According to The Children's Society, "In the last three years, the likelihood of young people having a mental health problem has increased by 50%. Now, five children in a classroom of 30 are likely to have a mental health problem"[6]. Other research in 2020 found, one in six (16.0%) children aged 5 to 16 years were identified as having a probable mental disorder, increasing from one in nine (10.8%) in 2017. The increase was evident in both boys and girls.[7] The Bill must carry legal sanctions with enough heft on technology providers to ensure the protection of children.

Anonymity

This is a huge area of concern within the draft Bill. Much of the abuse my family and I still experience is facilitated by those hiding behind anonymity or suspected 'bots'. Like a growing number of concerned commentators and campaigners, it is believed that placing thoughtful restrictions on anonymity of online users will reduce bullying and hate speech by promoting accountability and transparency.

Recent analysis in the US of online anonymity concluded that it *'influenced behaviour by reducing societal boundaries in human attitudes'* and determined that anonymity made user behaviour increasingly aggressive and violent by producing environments less constrained by social norms. The data evidence that anonymity is a key driver of antisocial, harmful, and criminal behaviour across social media platforms. A recent poll of UK social media users, conducted by Opinium for Compassion in Politics, found that three-quarters of those experiencing online abuse say it comes from anonymous accounts. Very interestingly,

[4] https://about.instagram.com/blog/announcements/using-research-to-improve-your-experience
[5] https://mhfaengland.org/mhfa-centre/research-and-evaluation/mental-health-statistics/
[6] https://www.childrenssociety.org.uk/what-we-do/our-work/well-being/mental-health-statistics
[7]https://digital.nhs.uk/data-and-information/publications/statistical/mental-health-of-children-and-young-people-in-england/2020-wave-1-follow-up

previous polling by Compassion in Politics found that four in five people would be willing to upload some form of ID to gain a "verified" account. Their latest research also demonstrated strong support for government intervention to reduce the number of anonymous accounts: three in four (73%) said they would support such action including 82% of Conservative supporters.

Psychologists say when social media users are anonymous, they feel much more powerful and willing to behave badly, a phenomenon known as the "Online Disinhibition Effect". At present, if an anonymous troll does get banned, they can easily create a fresh anonymous account with a new pseudonym and continue their vile trolling and abuse.

Anonymity can undoubtedly have positive effects, however, there is a growing body of evidence establishing the positive correlation between online anonymity and the expression of extremist, racially biased and prejudiced hate-speech. One study found there was a much higher chance of group polarisation within anonymised computer-mediated communications than within face-to-face setting.[8] Another study in 2019 found that high levels of anonymity among Twitter users was a significant predictor of online expressions of extreme radical attitudes and behaviours, extreme anti-social behaviour, and extreme prejudicial bias.[9]

But it is not just about individual activity, anonymity can lead to like-minded members of a collective to become more extreme in their views following group discussions.[10]

The Bill does mention anonymity in Section 135 (2) (a), "creating a user profile, including an anonymous or pseudonymous profile" as one of 13 "functionalities" which companies should consider when fulfilling their various safety duties, and which Ofcom should consider when conducting risk assessments. But this is a very weak provision, and it is unclear how the proposed regulator, Ofcom, would be able to challenge platforms' individual risk assessments. The outcome is therefore unlikely to drive change in this area.

Proposal - Add a new section specifically addressing anonymity

I support a solution being proposed by the campaign group Clean up the Internet as a straightforward approach whereby a new section is added to the Online Safety Bill introducing a duty on social media platforms to mitigate harms associated with anonymous accounts. This could include Clean up the Internet's three measures, listed below:

1 All social media users to verify their identity

---

[8] Sia et. al. (2002) in Christopherson, p.3043.

[9] Sutch, H. and Carter, P. 'Anonymity, Membership-Length and Frequency as Predictors of Extremist Language and Behaviour among Twitter Users.' International Journal of Cyber Criminology , 13:2, July-August 2019, pp., 439-459. https://www.cybercrimejournal.com/SutchCarterVol13Issue2IJCC2019.pdf , p.451,453.

[10] Christopherson, K. 'The positive and negative implications of anonymity in Internet social interactions: ''On the Internet, Nobody Knows You're a Dog.' Computers in Human Behaviour, 23 (2007), pp.3038-3056. https://www.researchgate.net/profile/Kimberly_Christopherson/publication/222428988_The_positive_and_negative_implications_of_anonymity_in_Internet_social_interactions_On_the_Internet_Nobody_Knows_You%27re_a_Dog/links/5dadf66d299bf111d4bf8bcc/The-positive-and-negative-implications-of-anonymity-in-Internet-social-interactions-On-the-Internet-Nobody-Knows-Youre-a-Dog.pdf , p.3043

Every social media user should be given the option of a robust, secure means of verifying that the identity they are using on a social media platform is authentic. Users who wish to remain unverified, should still be verified but not published and be free to continue to be anonymous, subject to the Terms & Conditions of the specific platform.

2 **Visibility**
The verification status of an individual user should be clearly visible to all other users, (rather like Twitter's "blue tick"). Users would then be able to bring their own judgement as to what a given verification status, or the lack of such, says about the credibility and reliability of another user's content.

3 **Users option to block interaction with unverified users**
Some users will be happy to hear from, and interact with, unverified users. Others will not. This should be a matter of individual user choice. Every social media user should be offered options to manage their level of interaction with unverified users, including an option to screen out communication, posts, and other interaction from unverified users as a category, rather than having to do so individually in response to abuse, spam etc.

The need for these measures is most acute on the largest platforms, because a) these platforms are where the largest numbers of users are exposed to abuse and disinformation and b) these platforms can most readily be considered an important part of the "public domain".

Other consequential amendments should be made to other parts of the Bill. For example, reducing harm from anonymous accounts should be mentioned as an "online safety objective" for the regulator, Ofcom, and included within the definitions of Ofcom's role in promoting media literacy.

The advantages of this approach are that it would express clearly and transparently what the Bill is trying to achieve, be on the face of the Bill, ensure proper democratic scrutiny, and crucially identify expectations on platforms to change their approach.

Social media companies should apply the 'Know Your Client/ Customer' principle, used in the financial sector. Using some of the legal framework required by companies offline, such as Customer Due Diligence in The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017[11], online companies should be legally required to verify users' identities before allowing use of their platform. Electronic identification techniques are already widely used by governments, financial institutions, and other businesses. For example, the Pan Canadian Trust Framework (PCTF) developed by the Digital ID & Authentication Council of Canada (DIACC) and the Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada[12]. The PCTF's principles include asking users to provide only the minimum amount of personal information, and privacy enhancing tools such as the 'right to be forgotten', inclusion and transparency[13]. This also allows the

[11] https://www.legislation.gov.uk/uksi/2017/692/part/3/made
[12] Pan Canadian Trust Framework Model, Final Recommendation V1.0. DIACC, 15 September 2020. https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf
[13] Ibid., p.7.

registration of legal entities such as businesses for a Digital Identity. It is crucial that while maintaining freedom of expression, people are not allowed to exploit anonymity which results in denying others their own freedom of expression.

It is hugely disappointing that in the face of growing evidence, the Government is failing to take this golden opportunity to include anonymity, and thus protect the public, in the draft Online Safety Bill. Put at its simplest, the same behaviour expected from offline hosts should also be expected from online equivalents.

Financial Harm

From a professional perspective, the shift to online financial crime and scams, which falls outside the FCA's regulatory perimeter but has increased some 300% - especially during the lockdowns and pandemic - are of grave concern to me as a consumer campaigner in the Financial services sector. Online fraud is up by a third in the UK during the pandemic, with £2.3bn lost by consumers in cases reported to the police[14].

The FCA has urged investors to check its register before conducting business after new figures revealed that nearly £80m was lost to 'clone firm' scams in 2020. The regulator has also stressed that online financial adverts should be regulated, alongside a warning against the need to regulate the promotion of crypto tokens[15].

Action Fraud and City of London Police said victims of these scams lose £45,000 on average, and during the last year more than £78m was lost to financial scams via clone firms of those on the FCA register. UK Finance claims that thousands of social media accounts are being operated by criminals to advertise for 'money mules', sell stolen identity and credit-card data, carry out phishing, and push bogus investment scams and impersonation fraud.

Industry pressure to include fraud in the scope of the reform seems to have worked, as the Bill now includes measures to tackle user-generated fraud. But fraud that is not user-generated and is conducted via advertising, emails or cloned websites, for example, will still fall outside the Bill's scope. Financial scammers would not be allowed to advertise or communicate with the public on traditional media with such impunity, so why are they being allowed to on modern technology platforms?

The increase in online financial scams, specifically highlighted through the pandemic and lockdowns, warrants including legislation to hold search engines and social media companies accountable for financial harm. Not including it within the scope of the Online Safety Bill underestimates the severity of the threat financial online harm does to people's lives. Recent research from the Money and Mental Health Policy Institute warned a lack of consumer protections against online scams had left vulnerable people as "easy prey" for fraudsters, with 4.5m people with mental health problems having fallen victim to fraudsters online[16]. Ignoring these issues risk the Bill falling short on the Government's ambition to 'bring the regulation the internet into the 21st century'. It is not too late to correct this omission.

---

[14] https://www.ft.com/content/e820cc8a-090c-4632-95f3-cb295d3d31ad

[15] https://www.ftadviser.com/regulation/2021/09/06/fca-in-renewed-push-for-regulation-of-online-ads/?page=1

[16] https://www.moneyandmentalhealth.org/press-release/vulnerable-people-online-scams/

The Tiered System / Approach and Duties upon In-Scope Companies

There needs to be more reassurance that the proposal to categorise content and activities into "Category 1 Services" and "Category 2 Services", with most companies likely to be deemed to be providers of the latter, will still capture smaller platforms that represent significant risk and percolate harm, abuse, hatred, and fake news across social media.

A small group of largest online companies, including Facebook, TikTok, Instagram and Twitter, will be in Category 1, while Category 2 services include platforms that host dating services, pornography, and private messaging apps. With less than 3% of UK businesses likely to fall within the scope of the legislation and the vast majority of companies falling under Category 2 services, as the government has claimed, significant clarity is needed on key elements of how the proposed regime will work in practice, including the criteria used for the categorised approach and 'high-risk services.

It is therefore vital that all companies, in both categories, have systems/processes in place to improve user safety. I would suggest this means more work needs to be done in the Online Safety Bill to set out detailed guiding principles and codes of practice which companies must have regard to when implementing these, in addition to the already published interim codes of practice on terrorist content and activity online, as well as child abuse and exploitation.

Legal Loopholes

The Bill contains a distinction between "illegal" and "legal, but harmful" content, but defines harm far too vaguely.

"The provider … has reasonable grounds to believe that the nature of the content is such that there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact on a child (adult)." What does indirect harm include?

The Bill states a provider will need to determine if the content is harmful (directly or indirectly) to children or adults, when a "*service has reasonable grounds to believe that the nature of the content is such that there is a material risk of harm[.]".* The legal standard used for this assessment is a risk of harm to an adult or child of "ordinary sensibilities" which is below that of the well-established standard of a "reasonable person". This will create uncertainties for those who are easily offended.

Section 12 of the Bill states it will protect individuals only against "unwarranted" privacy invasion, which begs the question of what are "warranted" invasions?

A worrying consequence of the Bill, as it stands, is that technology providers will be required to make judgment calls, including what counts as democratic, political, and journalistic speech and which content is harmful to users, directly or indirectly and to what extent. One must question the bureaucratic, administrative, and legal burden which could see smaller providers become unsustainable and the government create a powerful oligopoly. The government should therefore consider tightening up the loopholes and vagueness in the current Bill as well as providing templates and a simple rule book once the legislation is passed.

Conclusion

Regulation will not be a panacea, as it cannot address every aspect of online harm, but as a responsible society, we do need to start somewhere and send very strong messages to platforms causing endemic harm across our modern society, whilst making billions with impunity.

It is an important aspect in an array of required measures, including education, the need to address social inequalities, responsibility and transparency by companies, and lays foundations we can build on over time. Legislation should remain relevant, in the context of technological advances and emerging practices, as well as seeing how the regulation works in practice, in a fast-moving sector. For example, this legislation may well need amending to cover the 'metaverse' and any disturbing behaviours resulting from such products.

21 September 2021