

GLITCH



THE RIPPLE EFFECT

COVID-19 AND THE
EPIDEMIC OF ONLINE
ABUSE

September 2020

Table of Contents

EXECUTIVE SUMMARY

Executive summary	5
Glossary	13

INTRODUCTION

Introduction	
--------------	--

FINDINGS

About the respondents	19
Respondents' experiences of online abuse during COVID-19	20
Intersectionality	22
Platforms, perpetrators and patterns of online abuse	23
Impacts of online abuse on respondents	27
Behavioural change and self-censorship online	28
Reporting	31
Abuse in the virtual workplace	34

TESTIMONIALS

Testimonials	36
--------------	----

CONCLUSIONS & RECOMMENDATIONS

Conclusions	36
Recommendations for employers	40
Recommendations for the government	40
Recommendations for tech companies	42
Recommendations for civil society	43
Appendix	44

Suggested Citation:

The Ripple Effect: COVID-19 and the Epidemic of Online Abuse by Glitch UK and End Violence Against Women Coalition under a creative commons lisenice.

You are free to:

Share – copy and redistribute the material in any medium licensor cannot revoke these freedoms as long as you follow the license terms. Under the following terms:

Attribution – You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

ShareAlike – If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions – You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

This report was design in Adobe InDesign and Illustrator by Visualst.

Please note that this report includes statistics, and personal accounts, of online abuse and discrimination which some readers may find triggering.

ACKNOWLEDGEMENTS

Special thanks is given to Sarah Green and Rebecca Hitchen as well as the staff at End Violence Against Women (EVAW) for being great partners and providing valuable guidance and feedback. We would also like to thank Lily Kennett and the team at Schillings for their advice on this survey, particularly in relation to data protection and cyber security. We would also like to thank Sam Smethers and the Fawcett Society for their financial support. Finally, we would like to thank our Board of Trustees for their oversight and encouragement during a difficult time for the entire world and the entire Glitch team, old and new. Without them there would be no research or report.

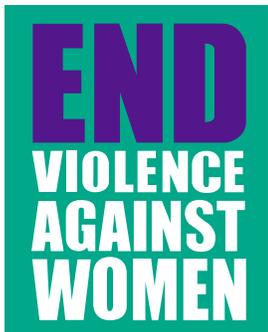
As two small organisations, if you'd like to support our work further, please do consider making a donation to our organisations, via our websites (www.fixtheglitch.org and www.endviolenceagainstwomen.org.uk)

ABOUT GLITCH

The logo for Glitch, featuring the word "GLITCH" in a bold, black, sans-serif font. The letter "I" is replaced by a yellow exclamation mark.

Glitch is a small and dynamic charity with a mission to end online abuse and champion digital citizenship across all online users, advocating for recognition that our online community is as real as our offline one and that we should all be working together to make it a better place. Glitch particularly focuses on the disproportionate impact that online abuse has on women and non-binary people of colour, and is the only UK charity with this area as its primary focus. Glitch is a registered charity (no. 1187714).

ABOUT EVAW

The logo for End Violence Against Women, featuring the words "END VIOLENCE AGAINST WOMEN" in a bold, white, sans-serif font, stacked vertically on a teal background.

The End Violence Against Women Coalition (EVAW) is a leading coalition of specialist women's support services, researchers, activists, survivors and NGOs working to end violence against women and girls in all its forms. Established in 2005, we campaign for every level of government to adopt better, more joined up approaches to ending and preventing violence against women and girls, and we challenge the wider cultural attitudes that tolerate and condone this abuse. The EVAW Coalition is a company limited by guarantee (no. 7317881) and a registered charity (no. 1161132).

Executive Summary

The impact of online abuse has been the subject of growing discussion in the UK and beyond in the last few years. Tech companies have come under increasing scrutiny for their failure to address the proliferation of online abuse and hate on their platforms. Governments across Europe are trying to address the problem by adopting legislation to regulate harmful content and behaviours online. At the same time, the COVID-19 pandemic and associated lockdowns have created a breeding ground for online abuse and pose new challenges for governments, employers, private companies and broader society.

The COVID-19 pandemic took the world by surprise. As cases of the virus started increasing sharply in Europe in early March 2020, governments began imposing lockdowns on their countries. The UK went into lockdown on 23 March; in April 2020, over one third of people globally lived under some form of lockdown restriction due to the pandemic.¹ Across the world, this resulted in increased internet usage and time spent online. During the initial days of lockdown, daytime internet usage more than doubled in the UK.² In other countries, early figures showed an average increase in internet usage ranging from 12% to 15% percent, and up to 30% in Italy, which became the first European state to impose a strict lockdown.³ **The vast majority of respondents to Glitch’s survey - 92% - reported using the internet more during the pandemic.**

Since its formation in 2017, Glitch has been campaigning to make online spaces safe for all, particularly women, girls and people with intersecting identities who are disproportionately affected by online abuse. Concerned with media reports and warnings by civil society organisations, including women’s advocacy organisations, of growing online and offline abuse in the early days of COVID-19 amid increased reliance on the internet and social media, Glitch launched a nationwide online survey to document the impact the lockdown had on online abuse against women and non-binary individuals. The survey was launched on 12 June 2020 in partnership with End Violence Against Women (EVAW) - a coalition of organisations working to address all forms of violence against women and girls - and remained open for one month.

This report presents the main findings of the survey and provides data-backed insights into the online experiences of women and non-binary individuals in the UK during the pandemic. It aims to provide decision-makers in the public sector, tech companies, private sector companies and civil society organisations with data on the scale, nature and manifestation of online abuse targeting women and non-binary people. It also provides recommendations on how to mitigate the increased risk of online abuse during COVID-19 and address the threat of the pandemic exacerbating existing inequalities.

¹Jon Henley, “EU urges caution in lifting coronavirus lockdowns,” The Guardian, 12 April 2020

<https://www.theguardian.com/world/2020/apr/15/eu-urges-caution-in-lifting-coronavirus-lockdowns#maincontent>

²Shabana Arif, “Daytime Internet Usage Has More Than Doubled Now That We’re on Lockdown,” Gizmodo, 26 March 2020

<https://www.gizmodo.co.uk/2020/03/coronavirus-lockdown-more-internet-usage-surge/>

³Matt Burgess, “No, coronavirus isn’t going to break the internet,” Wired, 21 March 2020

<https://www.wired.co.uk/article/coronavirus-internet-speed-shut-down>

Key Findings

This report presents the findings of the survey conducted by Glitch between 12 June and 12 July across the UK. The survey was limited to women and non-binary individuals and received 484 responses, the largest investigation into gender-based and intersectional online abuse during the pandemic in the UK. Some 83% of respondents were women, 2% were non-binary and 15% preferred not to disclose their gender.⁴ A total of 75% of respondents reported being from a white background, 11% from a Black and minoritised background, while the rest did not disclose their ethnicity. Respondents spanned a diverse range of age groups, with 22% belonging to the 18-24 category, 28% to the 25-34 age bracket, 22% aged between 35 and 44 and 19% between 45 and 54. A further 5% were aged between 55 and 64, while less than 2% were over 65.

⁴The introduction to the survey specified that the survey was designed for women and non-binary individuals. This includes trans women. While there is a chance that the 15% of respondents who preferred not to disclose their gender included some men who chose to take the survey despite not being targeted by this research, we consider this risk to be small and limited to few cases.

Who: Women and non-binary individuals

What: Insights from a survey that captured online experiences of women and non-binary individuals in the UK during the pandemic

When: 2020

12 June ————— 12 July

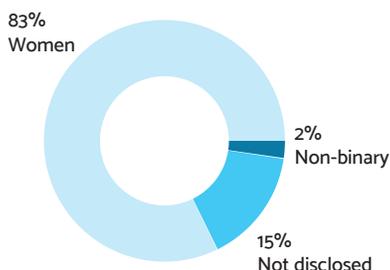
484

responses

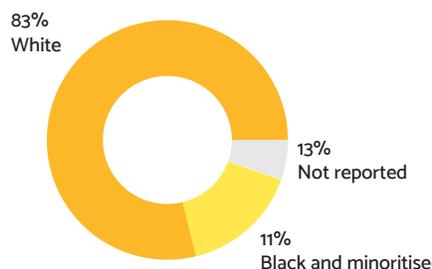
‘the largest investigation into gender-based and intersectional online abuse during the pandemic in the UK’

Respondent Demographics

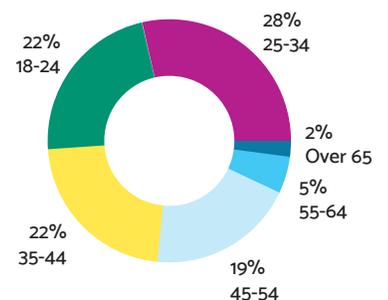
Gender:



Ethnicity:



Age:



While the survey covered a wide range of topics, there are some key takeaways. We found that:

> **Respondents reported experiencing online abuse since the beginning of COVID-19.**

46% of respondents reported experiencing online abuse since the beginning of COVID-19. This figure increased to 50% for Black and minoritised women and non-binary people.⁵

> **Of the respondents who experienced online abuse, it became worse during COVID-19.**

Of the respondents who had experienced online abuse in the 12 months preceding the survey, 29% reported it being worse during COVID-19. Black and minoritised women and non-binary people were more likely to report suffering increased online abuse during COVID-19, with 38% saying that the pandemic had led to increased online abuse.

> **Most of the abuse took place on mainstream social media platforms.**

Most of the abuse took place on mainstream social media platforms (Twitter, Facebook, Instagram) despite tech companies' commitments to making their platforms safe and addressing gender-based and intersectional abuse. Overall, 65% of respondents experienced abuse on Twitter, 27% on Facebook and 18% on Instagram.

> **A majority of respondents experienced online abuse from strangers.**

84% of respondents experienced online abuse from strangers - accounts that they did not know prior to the incident(s). Meanwhile, 16% of respondents faced abuse from an acquaintance and 10% from a partner or ex-partner. Some 9% of people faced abuse from a colleague or superior at work.

⁵The beginning of COVID-19 refers to the period starting with the implementation of the UK's lockdown on 23 March.

> **Gender was the most often cited reason for online abuse.**

Gender was the most often cited reason for online abuse. 48% of respondents reported suffering from gender-based abuse; 21% of respondents reported suffering from abuse related to their gender identity and sexual orientation, followed by 18% for their ethnic background and 10% for their religion and 7% for a disability.

> **The online abuse had a strong impact on respondents' behaviour and feelings.**

The experience of online abuse had a strong impact on respondents' behaviour and feelings towards using online technology and social media. 77% of respondents reported modifying their behaviour online as a result of the abuse, and 72% reported feeling differently about using technology and social media. This increased to 87.5% and 78% respectively for women and non-binary individuals of colour.

> **Respondents who reported online abuse during COVID-19 felt their complaint(s) had not been properly addressed.**

83% of respondents who reported one or several incidents of online abuse during COVID-19 felt their complaint(s) had not been properly addressed. This proportion increased to 94% for Black and minoritised women and non-binary people.

> **Only a few respondents received training from their employer on how to stay safe online.**

Only 9% of respondents received updated training from their employer on how to stay safe online while working from home, and 64% of those who did not receive any training felt that appropriate training would have been useful.

Recommendations

COVID-19 has created unprecedented challenges for the online safety of women and non-binary people, particularly from Black and minoritised backgrounds. As the prospect of further lockdowns continues to loom and with remote working likely to become a long term reality for many, urgent action is needed across the whole of society to address the growing undercurrent of online abuse against women and Black and minoritised communities.



UK Government



Employers



Tech Companies



Civil Society

1

The government needs to implement a comprehensive public health approach to tackling online abuse, including providing clear recommendations to employers on how to keep their employees safe online, publishing national guidance on digital safety, particularly when working from home.

2

There is an urgent need for greater financial investment from government, tech companies and employers in digital education programmes and research. While this research is the most ambitious attempt to document online abuse against women and non-binary people in the UK during COVID-19, more research is needed into gender-based and intersectional abuse, as well as the impact of online abuse on Black and minoritised communities.

3

Content moderation on social media platforms needs to be more effective and transparent and give more control to users over their online experiences. Content moderation efforts need to take into account the ever-evolving context.

Employers

Employers should put in place specific training to ensure their employees feel as safe online as possible. Employers have a statutory duty of care for people's health and safety at work and should provide appropriate guidance to staff working from home, including on digital safety. In the absence of national guidance on digital safety and wellbeing best practices, employers should make any reasonable effort to provide updated training to employees and share guidance with their staff.

'specific training to for employees'

Employers need to make all reasonable practical provisions to prevent online abuse in the workplace and adopt a workplace policy on gender-based violence and harassment, in consultation with employees and their representatives where possible. Employers should conduct a robust risk assessment in relation to online abuse and harassment at work, and take measures to prevent these threats.

'provisions to prevent online abuse'

Employers should cooperate with civil society organisations working to end abuse against women and marginalised communities to inform their response to the increased risk of online abuse while working from home, particularly for women and Black and minoritised employees.

'cooperate with civil society organisations'

Government

The government should provide clear recommendations to employers on how to keep their employees safe online and publish national guidance on digital safety, particularly when working from home. COVID-19 and the sudden widespread shift to remote working means that many employers do not always have sufficient training, skills and resources to ensure employees' safety in online working environments. Governmental guidance and a roadmap for Digital Health and Safety at work is therefore needed.

'clear recommendations to employers and national guidelines'

The government needs to implement a comprehensive public health approach to tackling online abuse. The government should adopt international standards to address harassment in the workplace, including the International Labour Organisation (ILO) Convention 190 on Eliminating Violence and Harassment in the World of Work. The government should also ensure that law enforcement officials and frontline workers receive updated training and appropriate resourcing to handle cases of online violence. Testimonials provided by respondents to the survey show that complaints are too often not taken seriously by law enforcement. One respondent said: "I reported the online harassment to local law enforcement, as there were physical threats via Facebook and Instagram from a stranger. There was no follow-through from the police." (see Testimonials for additional examples).

'comprehensive public health approach to online abuse'

The government must show greater leadership in tackling online harms and make the fight against online abuse a political priority. This includes ensuring that civil society and experts' responses to the Online Harms White Paper (OHWP) are reflected into legislation and including "hatred by sex" in the government's definition of online harms.

'leadership in tackling online harms'

The government should put pressure on tech companies to do more to tackle online abuse. The government's Digital Services Tax, which came into effect on 1 April 2020, imposes a 2% tax on tech giants including Facebook, Google and Twitter. Ringfencing at least 1% of this new tax annually is needed to fund efforts to effectively address online abuse.

'pressure on tech companies'

The government should fund further research into the impact of online abuse on women and Black and minoritised communities and intersectional online abuse. The government should invest more resources into digital citizenship education in the UK, including how to stay safe online, how to respond to online abuse and how to be an active online bystander.

'fund further research'

The government should work closely with and consult women's organisations about the risk of gender-based and intersectional online abuse and work with them to inform decision-making. Gender-based abuse should be also included in the government's digital policy strategy and inform its COVID-19 response and recovery decision-making, particularly around how to make online spaces safe for women.

'work with women's organisations about the risk of gender-based online abuse'

Tech Companies

Tech companies need to provide greater transparency about their content moderation efforts, including by allowing trusted research institutions and civil society organisations to access anonymised and disaggregated data about content removals and complaints submitted to the platforms, including the type of action taken, the time it takes to review reported content and increased transparency around appeals processes. Tech companies need to be transparent about their investment in and resourcing of content moderation, and need to invest more resources in human content moderation.

'provide greater transparency on content moderation'

Tech companies should provide more transparency about their policies related to dehumanising language based on gender, ethnicity and other protected categories. Policies should be regularly reviewed and updated to address new trends, patterns and manifestations of online abuse, including violence against women and people with intersecting identities.

'transparent policies related to dehumanising language'

Tech companies need to provide more financial support to civil society organisations working to tackle gendered and other types of abuse and harassment online and fund digital citizenship education initiatives. Funding is particularly vital to civil society organisations working with marginalised communities.

‘provide financial support to civil society’

Tech companies need to do more to address gender-based intersectional abuse on their platforms, in particular abuse targeting Black and minoritised women. Reporting processes should be improved and made easier for users of the platforms.

‘better reporting processes for gender-based abuse’

Tech companies need to do more to identify repeat offenders and make it more difficult for accounts that have been banned from platforms to resurface. IP addresses linked to permanently deleted accounts should not be able to recreate accounts for a significant period of time. Companies should also provide users with greater control and filters over their online experiences.

Civil Society

Research and civil society organisations working to end online abuse and harassment need to do more to understand the specific risks faced by minoritised communities. This survey and research highlighted the difficulties in obtaining significant datasets about particular minoritised communities. More targeted research is needed to document the online experiences of these communities.

‘more data on specific risks by minoritised communities’

Civil society organisations, charities and NGOs, particularly those with a strong brand presence online, should be at the forefront of digital health and safety in the workplace and should implement an online code of conduct that places online safety at its centre.

‘online code of conduct’

Civil society organisations working to end online abuse, gender-based violence and structural racism need cooperate and create partnerships to implement responses and action programmes. Civil society organisations need to build synergies and combine their respective expertise in research, training and interventions to ensure a more comprehensive response to the problem.

‘partnerships amongst organisations working to end online abuse’

Glossary

Digital citizenship

According to the Council of Europe, digital citizenship refers to the ability to engage positively, critically and competently in the digital environment, drawing on the skills of effective communication and creation, to practice forms of social participation that are respectful of human rights and dignity through the responsible use of technology.⁶ Glitch defines digital citizenship as “the concept of individuals engaging positively, critically and competently in all digital spaces.” Digital citizenship “requires everyone who engages with digital technologies to do so in a safe, responsible and respectful way that does not inflict or incite harm onto others.”⁷

Intersectionality and multiple identities

American scholar Kimberlé Crenshaw coined the term intersectionality to refer to the way different aspects of a person’s identity intersect. According to Lisa Bowleg, “intersectionality is a theoretical framework for understanding how multiple social identities such as race, gender, sexual orientation, SES, and disability intersect at the micro level of individual experience to reflect interlocking systems of privilege and oppression (i.e., racism, sexism, heterosexism, classism) at the macro social-structural level.”⁸

In addition to speaking about intersectionality, Glitch also refers to the concept of “multiple identities,” acknowledging that “women who face multiple and intersecting forms of discrimination offline because of their different identities (i.e. race, ethnicity, religion, sexual orientation, gender identity, disability, etc.) are also likely to be targeted with discrimination that targets their multiple and intersecting identities online.”

Online abuse

Glitch uses the phrase online abuse as an umbrella term to capture a plethora of tactics and harmful acts experienced by individuals online. Online abuse can include - but is not limited to - offensive or discriminatory comments and insults, threats of physical or sexual violence, stalking, harassment, bullying, impersonation, defamation, denial of service attacks, online impersonation, dead-naming, or violations of privacy such as “doxing” (posting private details online such as a person’s address or phone number with the aim to cause alarm or distress) or sharing intimate and private images of a person online without their consent.

⁶ See Council of Europe’s website: <https://www.coe.int/en/web/digital-citizenship-education/digital-citizenship-and-digital-citizenship-education#:~:text=Digital%20Citizenship%20refers%20to%20the,the%20responsible%20use%20of%20technology>.

⁷ See Glitch’s website:

<https://fixtheglitch.org/digital-citizenship/digital-citizenship-our-definition/>

⁸ Lisa Bowleg, “The problem with the phrase women and minorities: Intersectionality—an important theoretical framework for public health,” *American Journal of Public Health*, 102(7), 1267-1273, 2012
doi:10.2105/ajph.2012.300750 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3477987/>

Introduction

The COVID-19 pandemic has upended the world and changed the way we use social media and online technologies.⁹ As one third of the globe experienced lockdown restriction due to the pandemic in April 2020, internet usage and time spent online increased sharply. In the UK, internet usage more than doubled in the early days of lockdown.¹⁰ Some 92% of respondents to Glitch’s survey reported using the internet more during the pandemic.

Within a matter of days in late March 2020, the UK government imposed a nationwide lockdown, forcing hundreds of thousands of businesses to switch to remote working and making citizens more reliant than ever on online technologies to carry out everyday activities.

Social activities that previously took place physically migrated online; the internet provided a way to connect with loved ones and friends amid enforced social distancing and the government’s instruction to “Stay Home.”

Between 9 April and 20 April 2020, the Opinions and Lifestyle Survey found that 45% of adults in employment had worked from home at some point in the preceding week.¹¹ Another survey by the Office of National Statistics conducted between 23 March and 5 April showed the average proportion of the

workforce working remotely was 48%.¹²

In the early days of the pandemic, media reports showed new manifestations of online abuse, including in the workplace. Video conferencing applications such as Zoom and Google Meet became new hubs for online violence. On 29 March a meeting of Concordia Forum, a global network of Muslim leaders, about spirituality and wellness during COVID-19 was interrupted on Zoom when racial slurs appeared on the screen.¹³ This new form of abuse has since become known as “zoombombing.”

92%

of respondents to Glitch’s survey reported using the internet more during the pandemic

48%

average proportion of the workforce working remotely

⁹ Simon Kemp, “Digital 2020: July global statshot,” Date Reportal, 21 July 2020 <https://datareportal.com/reports/digital-2020-july-global-statshot>

¹⁰ Arif, *ibid.*

¹¹ “Coronavirus and the social impacts on Great Britain,” ONS, 30 April 2020 <https://www.ons.gov.uk/releases/coronavirusandthesocialimpactsongreatbritain30april2020>

¹² “Technology intensity and homeworking in the UK,” ONS, 2 July 2020 <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/technologyintensityandhomeworkingintheuk/2020-05-01>

¹³ Taylor Lorenz and Davey Alba, “‘Zoombombing’ Becomes a Dangerous Organized Effort,” New York Times, 7 April 2020 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3477987/>

The impact of the pandemic

Prior to COVID-19, multiple reports had highlighted the extent of abuse targeting women and Black and minoritised people online, in the UK and beyond:

- A 2018 report by Amnesty International examined tweets sent to 778 UK and US female politicians and journalists, finding that 7.1% of tweets received by these women were abusive or problematic, with Black women 84% more likely to receive such tweets than white women in the study.¹⁴
- Research published by Girlguiding in 2019 showed that 33% of girls and young women aged 11-21 had received mean or abusive comments on social media and 43% of girls admitted to holding back their opinions on social media for fear of being criticised - creating a situation where diversity is threatened.¹⁵
- In the workplace, a study by the Trade Union Congress (TUC) reported that women and LGBTQ+ people in the UK are disproportionately targeted by workplace harassment, with over 1 in 2 women and nearly 7 out of 10 LGBT workers reporting having been sexually harassed at work.¹⁶
- A BBC survey showed that half of a sample of 2,000 women were sexually harassed at work and of these, 63% did not report the abuse.¹⁷

Increased time online correlates with increased risks of online harms, ranging from hate speech and harassment to sexual violence and threats. As the pandemic developed, researchers and civil society organisations reported an uptick in extremist and “anti-minority mobilisation”¹⁸ and a proliferation of conspiracy theories and misinformation online scapegoating certain individuals and communities.¹⁹

¹⁴ Emily Dreyfuss, “Twitter Is Indeed Toxic for Women, Amnesty Report Says,” Wired, 12 October 2020
<https://www.wired.com/story/amnesty-report-twitter-abuse-women/>

¹⁵ Girls’ Attitude Survey 2019

<https://www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2019.pdf>

¹⁶ “Sexual harassment of LGBT people in the workplace,” TUC, 17 May 2019

<https://www.tuc.org.uk/research-analysis/reports/sexual-harassment-lgbt-people-workplace>

¹⁷ “Half of women’ sexually harassed at work, says BBC survey,” BBC News, 27 October 2017

<https://www.bbc.co.uk/news/uk-41741615>

¹⁸ Charlotte McDonald-Gibson, “‘Right Now, People Are Pretty Fragile.’ How Coronavirus Creates the Perfect Breeding Ground for Online Extremism,” Time, 26 March 2020

<https://time.com/5810774/extremist-groups-coronavirus/>

¹⁹ Emma Grey-Ellis, “Coronavirus Conspiracy Theories Are a Public Health Hazard,” Wired, 27 March 2020

A woman with COVID-19 who filmed herself in hospital and whose video went viral online received substantial abuse online from people claiming her video was a hoax.²⁰ Stalking support services reported a rise in cyber-stalking in the first four weeks of the lockdown via social media, messaging applications and emails, mainly over WhatsApp, Facebook and Instagram.²¹ Other examples documented by the media included unsolicited pornographic videos during online social events and zoombombing using racially charged and sexually explicit material.²²

While media reports and anecdotal evidence have shown that women and Black and minoritised communities suffer from online abuse as a result of COVID-19, there remains a notable lack of reliable data about the online experiences of women and non-binary people, especially from black and minoritised communities since the beginning of the pandemic. The survey launched by Glitch is a first attempt to fill this gap and provide data-backed insights into the impact of gender-based and intersectional online abuse.

The COVID-19 pandemic is a critical time for the fight against gender-based and intersectional abuse and requires an appropriate multi-sectoral response. In the last three years, European governments have adopted legislation to tackle the proliferation of hate speech on social media platforms, including

the NetzDG law (Network Enforcement Act) in Germany, adopted in June 2017. In April 2019, the UK government published the Online Harms White Paper, which sets out its strategy for safeguarding citizens' safety online.

As COVID-19 had a deep impact on the scale and nature of online abuse, regulatory efforts must take into account the changing nature of online harms. Tech companies are also facing new challenges on their platforms in what has been described as the first pandemic of the social media age. The problem of online abuse - already rife before the pandemic - has become more acute as content moderation has become increasingly reliant on Artificial Intelligence (AI). In the early days of the pandemic, tech companies took new steps to limit COVID-19-related disinformation on their platforms by highlighting official sources and removing medical disinformation, but online abuse continues to proliferate on platforms.

Violence against women and girls (VAWG) is an issue of human rights and has a deep impact on victims. Online, gender-based abuse can lead victims to adopt avoidance behaviours and can prevent them from accessing online support services, while widening the digital gender gap. As the results of our survey and testimonials from respondents have shown, it can have a deep negative impact on physical and mental health, as well as professional, social and financial situations.

²⁰ Aamna Mohdin, "Woman who filmed coronavirus warning receives online abuse," Guardian, 20 March 2020 <https://www.theguardian.com/world/2020/mar/20/dont-take-any-chances-warning-of-woman-with-covid-19-shared-online>

²¹ Jamie Grierson, "Surge in stalking victims seeking help during UK lockdown," Guardian, 8 May 2020 <https://www.theguardian.com/uk-news/2020/may/08/coronavirus-surge-stalking-victims-seeking-help-during-uk-lockdown>

²² "Online safety in a changing world - COVID-19 and cyber violence," Sexual Violence Research Initiative, 16 April 2020 <https://svri.org/blog/online-safety-changing-world-%e2%80%93-covid-19-and-cyber-violence>

²³ "Why policymakers need to tackle the digital gender gap," Web Foundation, 3 January 2019 <https://webfoundation.org/2019/01/why-policymakers-need-to-tackle-the-digital-gender-gap/>

Methodology

On 12 June, Glitch launched a nationwide survey in partnership with the End Violence Against Women (EVAW) coalition aiming to document the online experiences of women and non-binary people living in the UK. The survey included 22 questions (see Appendix) which covered respondents' use of the internet, their experience of online abuse during COVID-19, and the training provided by employers. It also included 12 questions related to demographics and data privacy. The survey was available online for a period of one month (12 June to 12 July 2020).

For safeguarding reasons, the survey was limited to adults aged over 18,²⁴ and therefore does not document the abuse that minors may have suffered during the UK lockdown. Further research is needed to understand the scale of abuse targeting children and teenagers during COVID-19. The results of the survey do not aim to present a comprehensive picture of online abuse in the UK as a result of COVID-19, but rather to provide data-backed insights into the experiences of women and non-binary people online during the pandemic.

Rather than assessing the extent of the abuse targeting the general population during COVID-19, we wanted to understand the impact of the pandemic on women and non-binary individuals, including Black and minoritised communities and people with intersecting identities, who are disproportionately targeted by online abuse. As a result, we limited the survey to women and non-binary people.

The questions we were seeking to answer when the survey was launched were as follows:

1 – The impact of COVID-19 on gender-based and intersectional online abuse

- What proportion of women and non-binary people have suffered from online abuse during COVID-19?
- Has increased internet usage during COVID-19 led to an increase of online abuse against women and non-binary people, particularly from Black and minoritised backgrounds?
- To what extent does intersectionality play a role in online abuse?²⁵
- What are the patterns of online abuse during COVID-19?
- What is the impact of online abuse (psychological, financial, social and emotional) of online abuse on women and non-binary people?

2 – How different stakeholders – including tech companies, law enforcement, employers and voluntary and mutual aid groups – have responded to the increased risk of online abuse targeting women and vulnerable communities during COVID-19

- Does reporting adequately address victims' complaints?
- What could different stakeholders do differently?
- Have employers put in place specific training and guidance for employees on how to stay safe online?

²⁴ The decision to exclude minors from the survey resulted from legal considerations surrounding safeguarding. Lawyers from Schillings provided pro bono legal advice for this project.

²⁵ Intersectionality refers to the way several aspects of an individual's identity intersect.

Glitch collected and analysed 484 responses to the survey, the largest dataset of testimonials about online abuse targeting women and non-binary people during COVID-19 in the UK.²⁶ We also gathered detailed testimonials over email from four participants who agreed to answer further questions. These deeper qualitative interviews allowed us to capture experiences which were difficult to gather in the survey, including behavioural and psychological impacts. Testimonials are presented in this report.

It is important to note the limitations of this research. While 484 respondents took part in the survey, not all answered the survey in full. Specific questions related to online abuse were answered by respondents who had suffered online abuse during the COVID-19 period. Some questions did not apply to all participants and were not compulsory to answer. The size of the data sample therefore varies by answer.

Out of 484 respondents, only 11 (2%) identified as non-binary. The sample of non-binary respondents was too small to draw any meaningful conclusions, and the results presented in this report are therefore not disaggregated by gender identity. However, where possible we are presenting anecdotal evidence about the experiences of non-binary respondents. While we were able to gather a significant number of responses from women, including from a range of Black and minoritised backgrounds, sample sizes are too small to present data about specific minoritised communities. This shows the need for more funding in research into intersectional online abuse and abuse targeting specific minoritised communities (see Recommendations).

Only results where a significant number of respondents answered are included below.

484

respondents took part in the survey, not all answered the survey in full



‘the largest investigation into gender-based and intersectional online abuse during the pandemic in the UK’



11 (2%)

only 11 (2%) identified as non-binary. The sample of non-binary respondents was too small to draw any meaningful conclusions, and the results presented in this report are therefore not disaggregated by gender identity

²⁶ The survey gathered 484 partial responses and 225 complete responses. Respondents had the option to skip certain responses if they were not relevant to them.

Findings

About the respondents

This section presents general observations about the demographics of respondents.

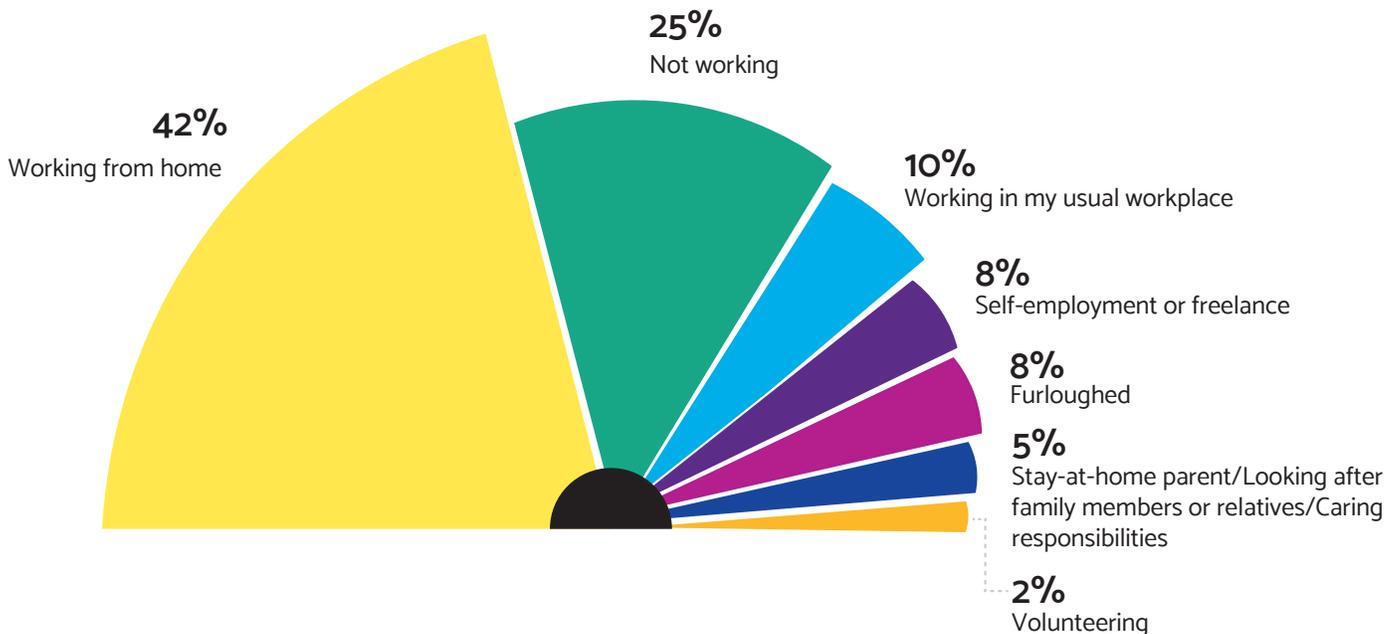
Of respondents who answered questions about their gender, 83% were women, 2% were non-binary and 15% preferred not to say. 75% respondents reported being white, while 11% reported being from an ethnic minority background. The rest of respondents preferred not to disclose their ethnicity. Results broken down by ethnicity exclude respondents who did not indicate their ethnic background.

While the majority of respondents identified as straight (60%), 11% of respondents identified as lesbian/gay, 13% as bisexual and 6% as queer.

The survey therefore captures the experiences of members of the LGBTQ community. Respondents came from different age groups, with 22% belonging to the 18-24 category, 28% aged from 25-34 age bracket, 22% aged from 35-44 and 19% aged from 45-54. However, only 5% of respondents were aged 55 to 64, and less than 2% were over 65.

The survey wanted to assess respondents' situation during COVID-19. 42% of respondents reported working from home, 25% reported not working at the time the survey was conducted, while 10% worked at their usual workplace.

Figure 1. Most women are working from home during COVID-19



Regardless of their professional situation, respondents overwhelmingly reported increased internet usage as a result of COVID-19. Some 92% of respondents reported increased internet usage since the beginning of the pandemic. The reasons for this increase were manifold: 61% reported increased internet usage for work, 80% for socialising, 72% for news and 21% for volunteering.

These findings are in line with official reports of increased internet usage during the pandemic. For instance, statistics released by Ofcom on 24 June showed that UK residents spent an average of 4 hours per day online during COVID-19, the highest time on record.

Respondents' experiences of online abuse during COVID-19

Increased time spent online during COVID-19 coincided with increased online abuse for the survey's respondents. In the months preceding COVID-19, 38% of respondents experienced online abuse. This proportion reached 50% for Black and minoritised respondents.

Some 52% of Black and minoritised women and non-binary people experienced online abuse during COVID-19, as opposed to 42% of white respondents. Of the respondents who experienced online abuse during COVID-19, 27% of reported increased online abuse during COVID-19.

Respondents experienced online abuse

Overall

38%

reported experiencing online abuse

Black & minoritised

50%

reported experiencing online abuse

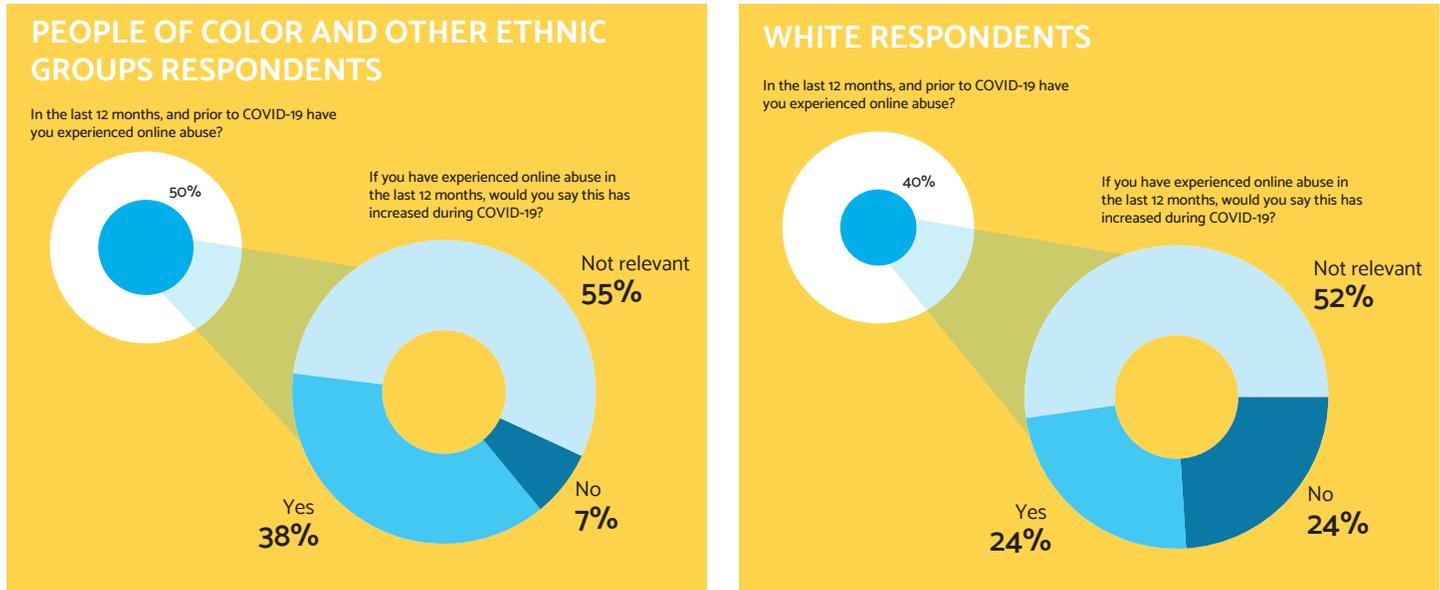
Respondents experiencing online abuse during COVID-19

▲ 27%

reported increased online abuse during COVID-19

²⁷ "UK's internet use surges to record levels," Ofcom, 24 June 2020 <https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/uk-internet-use-surges#:~:text=Ofcom's%20annual%20Online%20Nation%20report,hours%20in%20September%20last%20year.>

Figure 2. Experiences of online abuse worsened during COVID-19, especially for Black and minoritised women



Percentage of respondents who experienced increased online abuse during COVID-19

This figure increased to 40% for Black and minoritised respondents. “Social media has always tended to be contentious and abusive but since COVID and lockdown I believe the vitriol has increased exponentially,” one respondent said.

Participants in the survey highlighted the scale of online abuse targeting women during the pandemic and the feelings of alienation they felt on social media. “Nothing ever changes. I report lots of violent images and sexist abuse. It feels like the moderators are sexist too, as they allow it. People are cloning profiles and being abusive but write ‘parody’ in them so get away with it. There’s so much porn and violence against women and girls that it feels like a place where women aren’t treated as humans. We’re guests in a male space,” a respondent wrote.

While samples of respondents by specific Black and minoritised background were too small to draw statistically significant conclusions, the limited data we have shows that 50% of Black British respondents faced online abuse since the beginning of COVID-19 lockdown; the proportion was 58% for Asian British respondents.

These respondents reported that the online abuse had a significant impact on them. One wrote: “I now try not to reply to anyone online - as I feel my feed is being monitored and targeted by others.” How online abuse leads to self-censorship and avoidance tactics is further explored below (see “Behavioural change and self-censorship online”).

Intersectionality

When analysing online abuse, it is essential to keep in mind that individuals may be targeted on the basis of their different identities. This phenomenon is referred to as intersectionality. The findings from the survey show that Black and minorities women and non-binary people were more likely experience online abuse during COVID-19 and more likely to report the abuse being worse during the pandemic. This highlights the need to implement responses that include an intersectional lens.

Respondents were asked what aspect(s) of their identity the abuse they faced was related to. Gender was the most often cited reason for online abuse. Some 48% of respondents reported suffering from gender-based abuse, 21% of respondents reported suffering from abuse related to their gender identity and sexual orientation, followed by 18% for their

ethnic background and 10% for their religion and 7% for a disability.

Black and minoritised women and non-binary people were almost as likely to be abused based on ethnicity as they were to be abused based on gender, with 46% of Black and minoritised respondents of colour reporting abuse based on gender and 43% based on ethnicity. Black and minoritised respondents were also more likely to be abused for their religion than white respondents. While the sample of non-binary respondents was too small to draw statistical conclusions, anecdotal evidence shows they overwhelmingly experienced abuse related to gender identity and gender expression (7 out of 11).

Figure 3.1 Online abuse targeted different aspects of personal identity for white versus Black and minoritised women

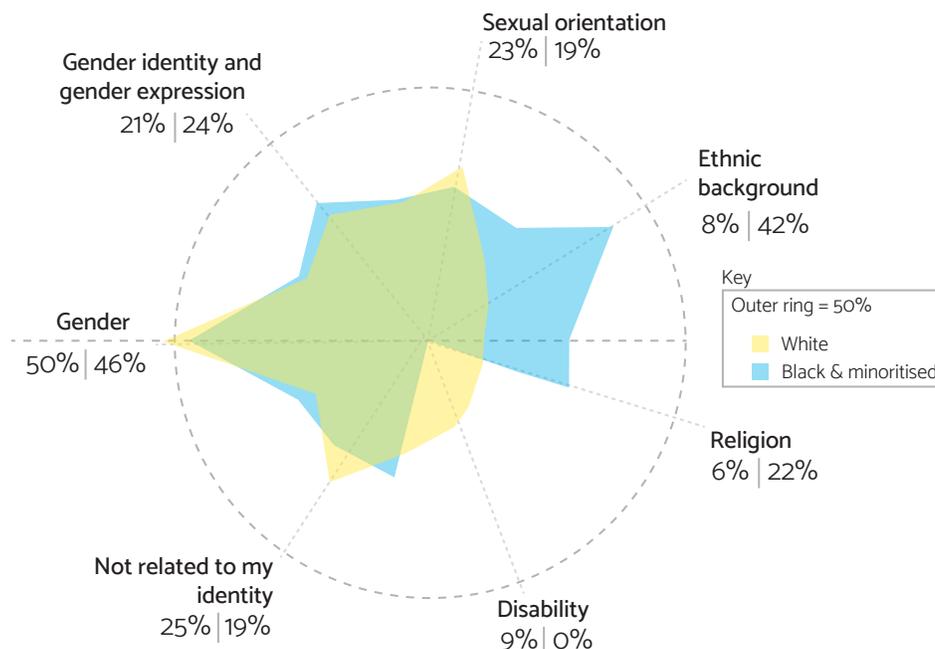
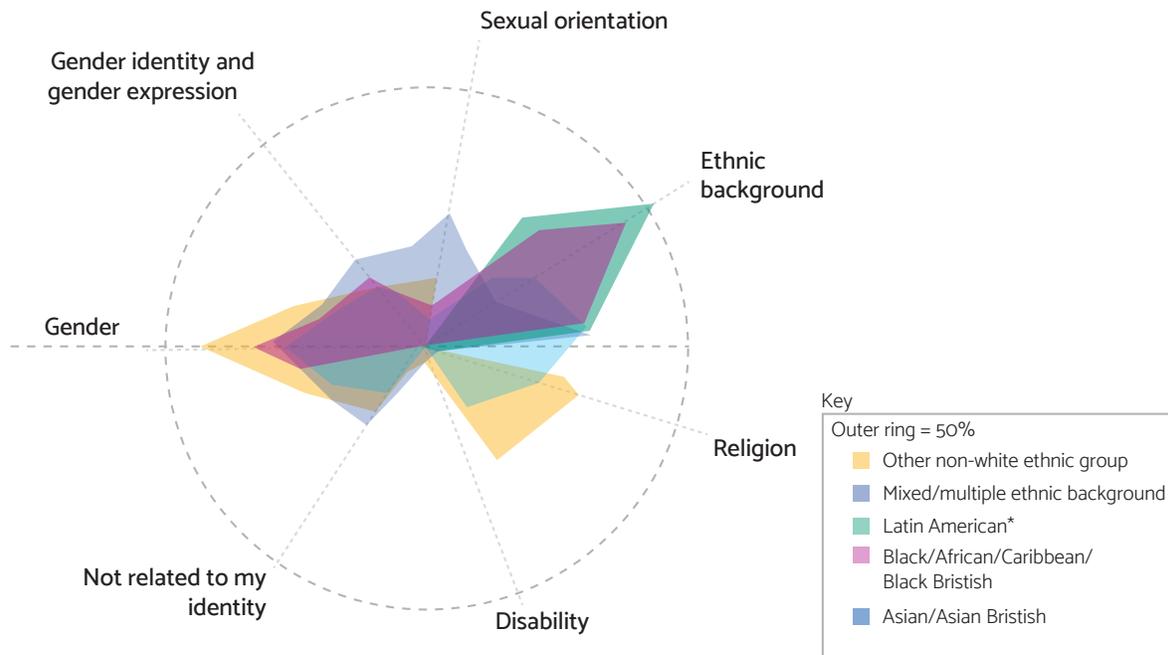


Figure 3.2 Online abuse about ethnic background and gender were the most prevalent among non-white ethnicities



Women of non-white ethnicities only accounted for 13% of the sample (N=64)

* One Latin American woman only reported abuse about their ethnic background (100%), however the scale is up to 50%

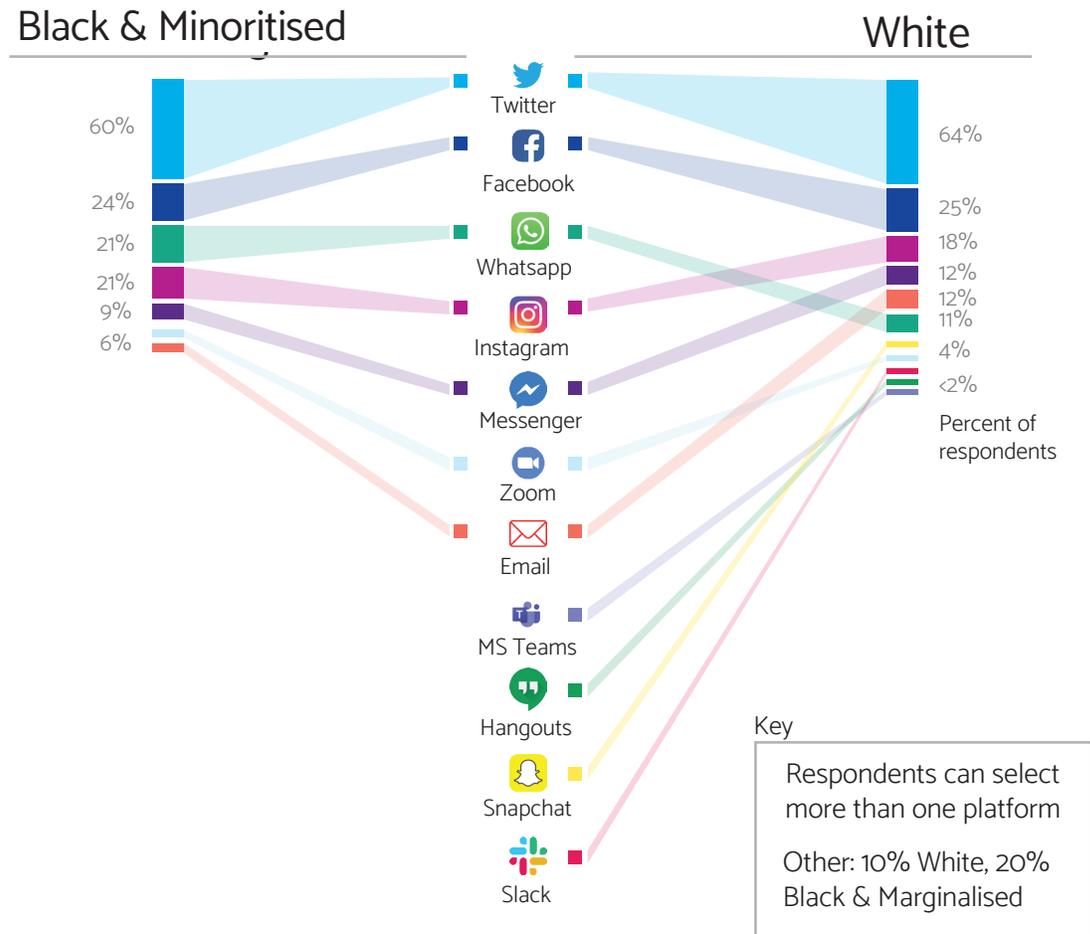
While data samples broken down by specific Black and minoritised communities are too small to draw statistically significant conclusions, anecdotal evidence from the data sample gathered via our survey showed that respondents who identified as Black British, Asian British and from mixed backgrounds suffered experienced online abuse related to gender, ethnic background, sexual orientation, as well as their religion.

The small data sample we were able to collect highlights the difficulties of conducting research about the experiences of minoritised communities and the need for more funding for this type of study. This investigation - the most ambitious attempt at documenting the impact of COVID-19 on gender-based online abuse in the UK - was limited in time and resources and more follow-up research is needed (see Recommendations).

Platforms, perpetrators and patterns of online abuse

Online abuse recorded by the survey overwhelmingly took place on large social media platforms. Twitter, Facebook and Instagram were the three platforms on which respondents reported facing the most online abuse, followed by messaging applications. Around 64% of respondents who experienced online abuse reported experiencing abuse on Twitter.

Figure 4. The major social media platforms served as the source of online abuse for all women



Platforms on which respondents experienced online abuse (percentages - multiple answers)

Some 25% experienced online abuse on Facebook, 18% on Instagram and 17% on messaging applications including WhatsApp and iMessage.

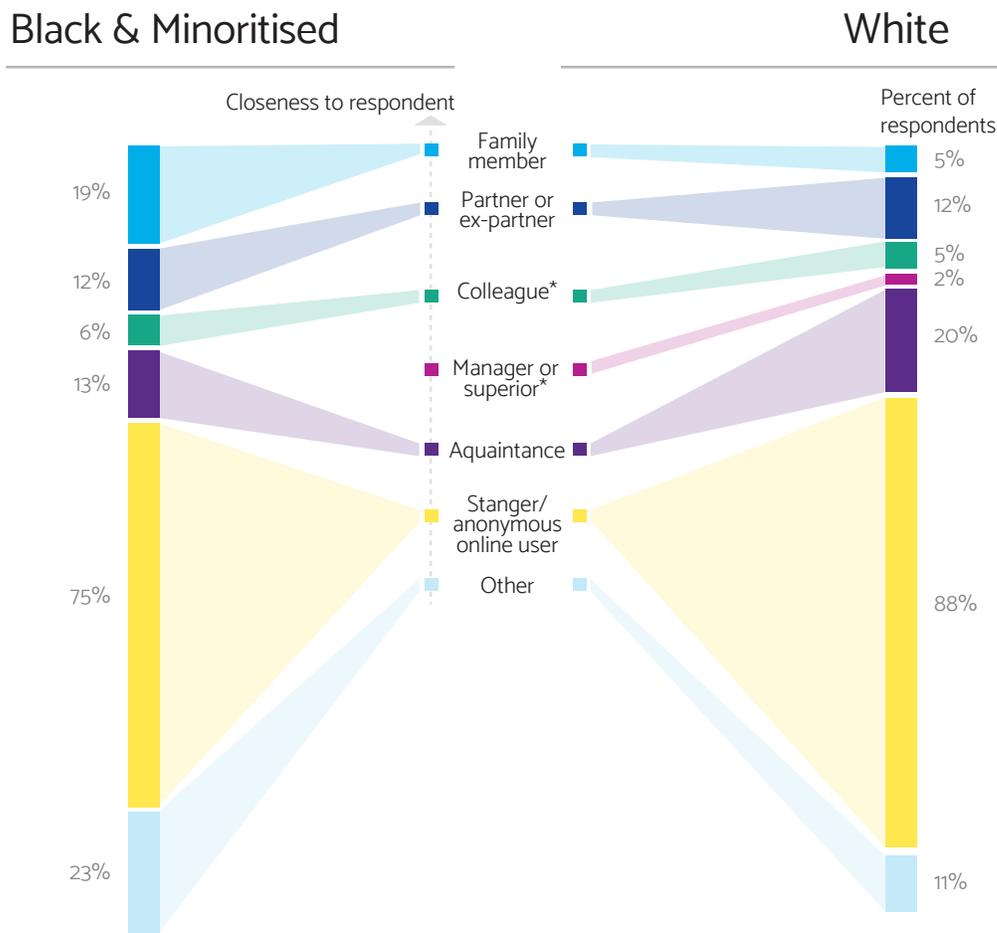
Under 5% of respondents experienced abuse on platforms frequently used in professional contexts, including Zoom, Google Hangouts, Slack, Microsoft Teams and ASANA. While the results of our survey suggest that tech platforms used at work are less often the site of online abuse, media reports of cases of zoombombing have highlighted the risk of abuse on emerging and growing platforms. More research is needed to understand the role these platforms play in online abuse.

These figures varied for Black and minoritised women

and non-binary people. 60% of Black and minoritised respondents experienced abuse on Twitter and 24% on messaging applications, ahead of Facebook and Instagram (both 21%). These findings suggest that specific responses need to be implemented to address the risk of abuse against Black and minoritised communities on certain platforms, and that tech companies and governments must take into account the role of ethnicity in determining risks.

The majority of online abuse reported by respondents was perpetrated by strangers - accounts or people that respondents did not know prior to the incident. Some 16% experienced online abuse from acquaintances, 11% from a partner or ex-partner and 9% from a colleague or superior at work.

Figure 5. Online abuse was perpetrated most often by strangers



Perpetrators of online abuse (percentages - multiple answers)

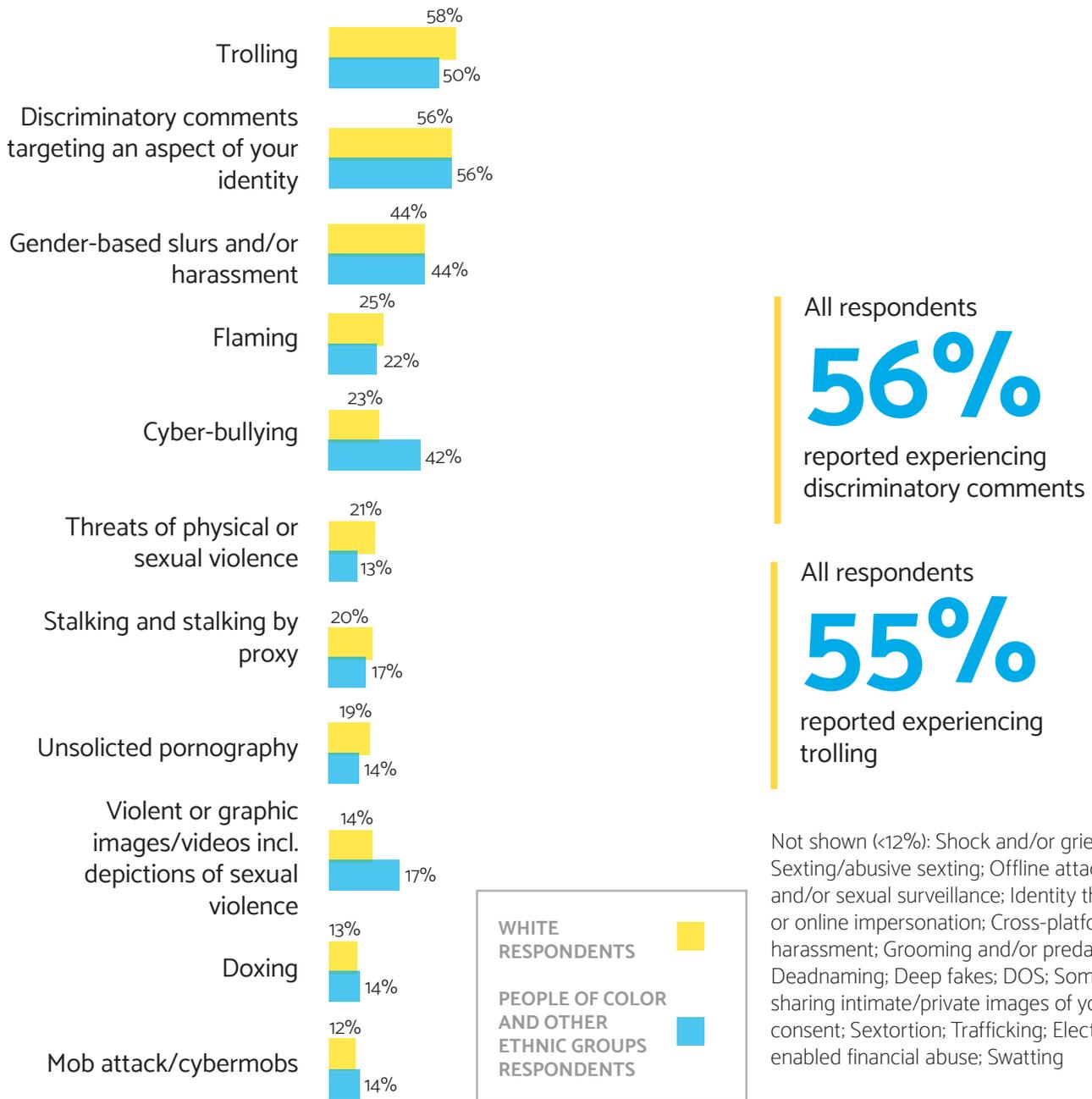
These findings correlate with previous studies about online abuse. Research conducted in 2017 by Pew Research Center in the United States showed that over half of Americans who had suffered online harassment (54%) said their most recent incident involved a stranger or someone whose identity they did not know.²⁸

The proportion of respondents who experienced abuse from colleagues or superiors at work highlights the need for robust workplace policies on gender-based violence and harassment, including in online working spaces.

Respondents were also asked to provide detail about the type of abuse they had suffered. The survey detailed 27 types of online abuse: sextortion, stalking and staking by proxy, doxing, identity theft and/or online impersonation, spying and/or sexual surveillance, deep fakes, grooming, trafficking, swatting, discriminatory comments, violent or graphic images, trolling, Google bombing, cyberbullying, gender-based slurs, threats of physical or sexual violence, DOS, electronically-enabled, dead-naming, flaming, mob-attacks, shock and/or grief trolling, sexting and/or abusive sexting, unsolicited pornography, cross-platform harassment and offline attacks.

²⁸ Maeve Duggan, "Online Harassment 2017," Pew Research Center, 11 July 2017 <https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/>

Figure 6. Online abuse is experienced in many forms with a larger breadth of experiences reported by Black and minoritised women



Type of abuse experienced by respondents (percentages - multiple answers)

Discriminatory comments, trolling, gender-based slurs and cyber-bullying represented the most common forms of online abuse: 56% of respondents experienced discriminatory comments, 55% experienced trolling, 47% said they had faced gender-based slurs and/or harassment and 29% cyber-bullying. Sexual violence was often reported, with threats of physical and sexual violence being reported by 21% of respondents and unsolicited pornography by 17%.

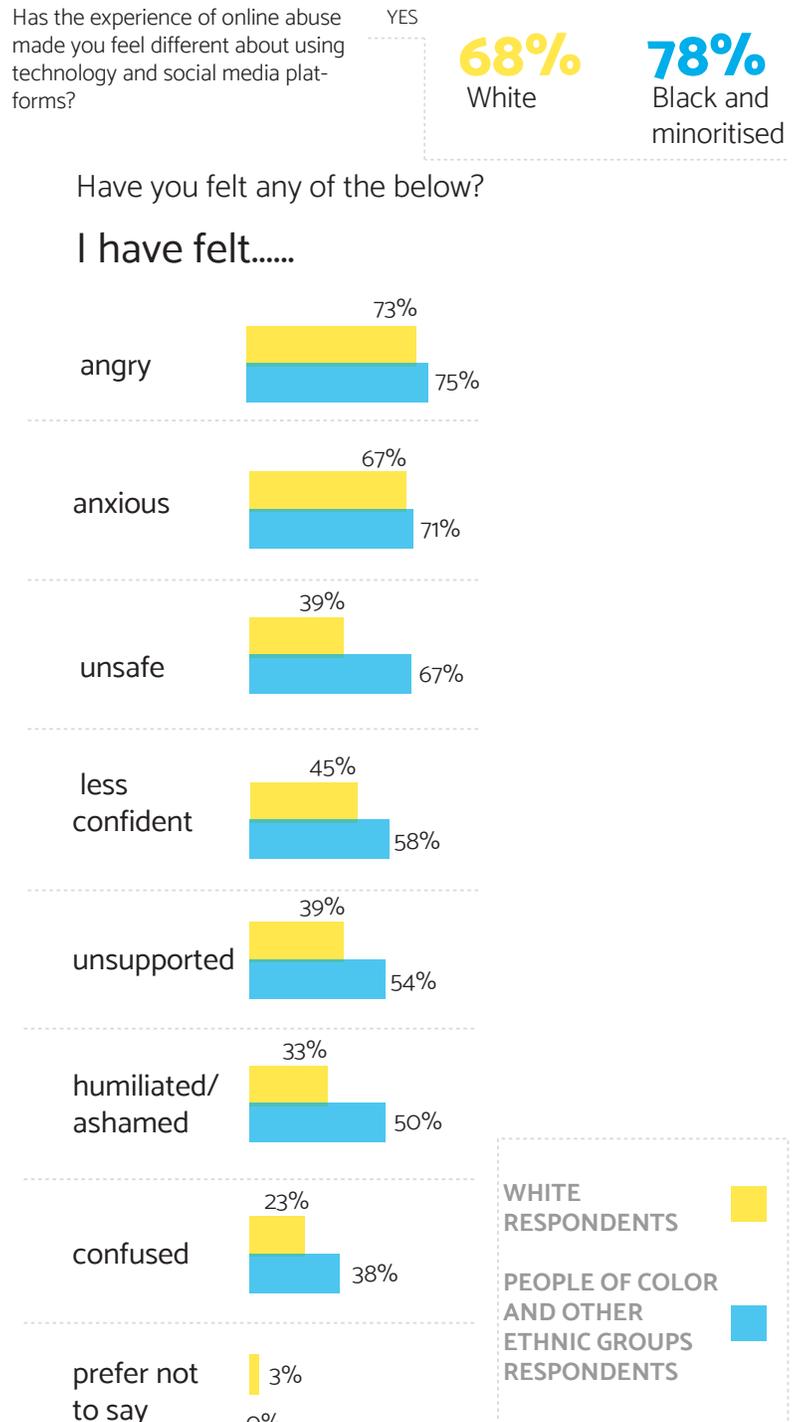
Impacts of online abuse on respondents

The findings of the survey demonstrate the negative impact of online abuse on respondents. Some 34% of respondents reported that the experience of online abuse had had a professional, social or financial impact on them. Black and minoritised women and non-binary people were more likely to face professional, social or financial consequences, with 48% reporting having done so.

“I try to spend less time online but I live alone and my health isn’t great so it means really becoming isolated and depending on a few trusted friends to stay in contact with rather than connecting with my community more widely. I definitely feel my performance at work has suffered and I feel at risk of sanction or not having my contract renewed due to the impact on my ability to focus and my mental health,” a respondent wrote.

The experience of online abuse had a deep impact on respondents’ relationship with technology and social media. 68% of white respondents reported that the experience of online abuse had made them feel different about using technology and social media. This figure increased to 78% for Black and minoritised women and non-binary people.

Figure 7. Most women reported feeling a multitude of strong emotions after experiencing online abuse



Behavioural change and self-censorship online

Respondents reported experiencing negative emotions as a result of the online abuse they had suffered. Anger and anxiety were the most frequently experienced emotions, with 73% of respondents feeling angry and 69% anxious following incidents of online abuse. Black and minoritised respondents were slightly more likely to report feeling anxious than white respondents: 70% compared to 67%.

A number of respondents described the emotional impact of online abuse in testimonials included alongside the survey. “When I shared a positive message and picture of my son and me, we received a torrent of racial abuse after trolls picked up the photo. I felt afraid and vulnerable,” one respondent wrote. “It does make me anxious and angry,” another said. “It’s made me so anxious, I am still on anti-depressants and if [social media] wasn’t used to connect to some good voices and work, I would leave.”

The psychological and emotional impact of online abuse upon those affected is considerable. Research has consistently shown that victims of online abuse report psychological distress and lower self-esteem as a result of their experiences. Research by Amnesty International showed that 55% of women who had experienced online abuse or harassment suffered stress, anxiety or panic attacks and 67% felt apprehensive when thinking about using social media.²⁹

The experience of online abuse led a majority of respondents to modify their behaviour online and adopt defensive mechanisms to avoid experiencing abuse. This adjustment in online behaviour mirrors women’s “safety work” offline. Liz Kelly and Fiona Vera Gray define safety work as the set of strategies that women adopt to avoid experiencing violence from men³⁰ 87.5% of Black and minoritised respondents said they had modified their behaviour online following incidents of online abuse, compared to 72% of white respondents.

Civil society organisations and human rights activists have documented the silencing effect of online abuse, particularly on Black and minoritised groups. In its work, Glitch gathered many testimonials from women rethinking a career in public life after witnessing the abuse meted out to politicians who look similar to them.

Social media platforms are often critical spaces for individuals to exercise the right to freedom of expression. Online abuse is a direct threat to this freedom of expression, which hinders progress towards gender equality and democratic societies. After suffering online abuse, many women and girls are forced to abandon their profiles and leave social media. Research by Plan International showed that 43% of girls admitted to holding back their opinions on social media for fear of being criticised.³¹

²⁹ “More than a quarter of UK women experiencing online abuse and harassment receive threats of physical or sexual assault - new research,” Amnesty International, 20 November 2017

<https://www.amnesty.org.uk/press-releases/more-quarter-uk-women-experiencing-online-abuse-and-harassment-receive-threats>

³⁰ In Vera-Gray and Kelly’s words, “women learn to adapt their behaviour and movements, habitually limiting their own freedom in order to prevent, avoid, ignore, and ultimately dismiss what they experience as ordinary.” Fiona Vera-Gray and Liz Kelly, “Contested gendered space: public sexual harassment and women’s safety work,” *International Journal of Comparative and Applied Criminal Justice*, 2020 <https://www.tandfonline.com/doi/full/10.1080/01924036.2020.1732435>

³¹ “Almost half of girls aged 11-18 have experienced harassment or bullying online,” Plan International, 14 August 2017 <https://plan-uk.org/media-centre/almost-half-of-girls-aged-11-18-have-experienced-harassment-or-bullying-online>

Section 3: Findings

Respondents to our survey shared testimonials about the impact of online abuse and how they modified their behaviour as a result of their experiences. A respondent who suffered sexist abuse on Twitter after sharing a picture of themselves said they would no longer post any personal content on the platform. “I don’t normally share personal information on Twitter as I have very tight control on my Instagram and Facebook accounts. I have realised Twitter just isn’t capable of that much control and have adjusted my own behaviour and settings.”

Another respondent shared similar feelings. “With Twitter, it has made me feel like a specific group of people can get access to you and your information and I have been advised by other users to lock my account when I am not on it so they can’t access my information.” While the most common behavioural change consisted of blocking (76% of respondents reporting doing so), muting (64%) or reporting (53%) another user, the fourth most common action taken by respondents was simply to spend less time online.

41% of white respondents reported spending less time online after facing online abuse, as opposed to 48% of Black and minoritised respondents. These findings suggest that many women and non-binary people, especially from Black and minoritised backgrounds, are being driven away from certain platforms because of the abuse they face. Several respondents wrote about not feeling safe online and avoiding mainstream social media platforms.

One respondent said: “The sheer amount of abuse aimed at women - horrendous in its level of violence and misogyny - and the failure for any of the social media platforms to address in

any real or meaningful way (possibly because they are male dominated?) has had a real impact on my mental health. I’ve had to take a real step back from participating in certain groups or forums, from following certain accounts or hashtags.

“Seeing others seemingly emboldened by abuse levels to join ‘witch-hunts’ that drive women off social media, or silence them. I, like many, no longer freely post, hyper aware that my comments or opinions, no matter how benign or uncontroversial, may attract the attention of somebody who in turn may attack or threaten me. I worry about doxing. I worry I may unwittingly say something to enrage a misogynistic type who decides I need to be ‘punished’ by harassing employers or colleagues or friends to ‘cancel’ me. I feel silenced. Because only by being silent can I guarantee to be safe.”

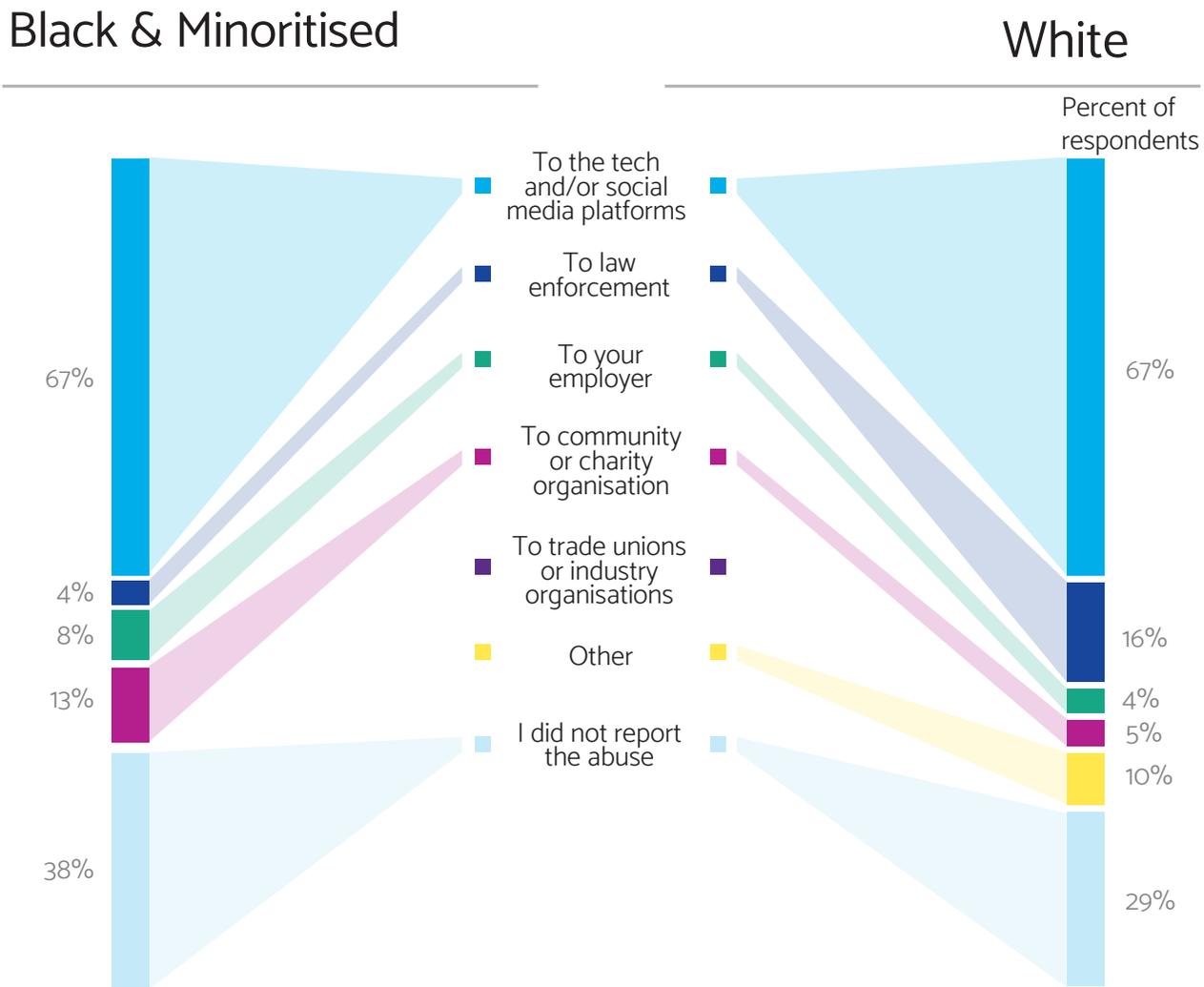
In particular, testimonials from respondents who identified as lesbian/gay or bisexual highlighted the emotional toll of online abuse.



“I live alone and am housebound because of my physical disability so the internet is my only contact with the outside world. I no longer participate in online communities because women, especially lesbians, receive vile abuse simply for discussing ourselves, our lives, and our needs/rights. These men and their supporters have created a situation where women can only talk to one another about our own lives if we’re able to cope with constant abuse and threats. They dominate the social media platforms, coordinate attacks on women, and it’s reached the point where it’s better for my mental health to be completely isolated with no social contact than to try and socialise online.”



Figure 8. Most women reported online abuse to the tech and/or social media platform



Data about who respondents reported online abuse to (percentages - multiple answers)



“I don’t normally share personal information on Twitter as I have very tight control on my Instagram and Facebook accounts. I have realised Twitter just isn’t capable of that much control and have adjusted my own behaviour and settings.”



Reporting

One of the key objectives of the survey was to understand whether victims reported online abuse and how effective reporting was in addressing the problem. Respondents who experienced online abuse were asked if they had reported the incident(s) and to whom. 63% of respondents reported the abuse to social media platforms, 12% to law enforcement, 7% to community organisations or charities and 5% to their employer. However, 35% said they had not reported the abuse. Black and minoritised respondents were more likely to report the abuse to charity organisations (12.5%) than to law enforcement (4%).

Responses to our survey highlighted the limitations of reporting and the perceived lack of support provided to victims from law enforcement, tech companies and other stakeholders. Of respondents who reported the online abuse, the overwhelming majority felt their complaint had not been properly addressed. Some 84% of respondents said their complaint had not been properly addressed, a figure which increased to 94% for Black and minoritised women and non-binary people.

All respondents

63%

reported the abuse to social media platforms



“The sheer amount of abuse aimed at women - horrendous in its level of violence and misogyny - and the failure for any of the social media platforms to address in any real or meaningful way (possibly because they are male dominated?) has had a real impact on my mental health. I’ve had to take a real step back from participating in certain groups or forums, from following certain accounts or hashtags.”



Written testimonials provided by respondents highlighted several key takeaways, namely:

> **Tech companies are not doing enough to address online abuse, and too often no action is taken.**

“Facebook does absolutely nothing. Twitter does suspend accounts, but then it lets them back on again after no time, and they just carry on as before.”

“One male sent a lot of inappropriate photos of themselves without my consent and after reporting them to the proper Facebook authorities, they did nothing about it. No action by Facebook was taken.”

> **There remain technological obstacles to addressing online abuse and lack of transparency over processes, content moderation policies and what meets the threshold of dehumanising language.**

“Posts are never taken down because they don’t include words that trigger the bots. There needs to be more human interaction between platforms and users. There was no opportunity to explain why the post was offensive other than ticking boxes.”

“Because these platforms have such strict guidelines for what counts as abuse, they often won’t see things like gas-lighting or general name calling as abuse.”

“The people who are abusing others on the internet are hard to find. Their identity is almost always fake and they are hard to track.”

> **Replies from social media companies are often non-existent, unhelpful and come too late, in contradiction to the platforms’ duty of care towards users.**

“The response I received was a pro-forma and did not give a sufficient detail given the nature of the threats I received. I see so many people getting this kind of abuse - I say people but it’s women and trans people mostly - and there is no punishment. If accounts get suspended, they come back with a new one straight away.”

“Other than the perfunctory automated response, I have not heard back from Twitter.”

“When you report a tweet, Twitter encourages you to block the sender. While that’s no doubt well meant, it does mean that you can’t verify what action Twitter says they are taking. It can take ages to get any sort of response by email, and by the time you do get something the offending account is often still there.”

> **Content moderation on social media platforms is not properly enforced.**

“While I was notified that the account in question violated Twitter’s policy, the account was not suspended, even though they are a known harasser who targets many people in my community with threats, trolling, spamming and dogpiling.”

“Abusive accounts remain active. Other women experiencing similar attacks or defending other women are banned for speaking about the abuse. Pile-ons and ‘cancelling’ campaigns against women are increasing in frequency and in levels of hostile abuse. Explicit and violent language, images and threats aimed at women are routinely allowed to stand by the social media platforms.”

> **Victims of online abuse are not taken seriously by law enforcement.**

“As is usual with sexual harassment, the police officer I spoke to did not understand my anger at being sexually objectified. I feel as though this kind of harmful abuse which perpetuates racism and sexism is simply not taken seriously and there are no meaningful consequences for the perpetrators.”

“I reported an incident to the police and there was no action taken.”

“The police said Twitter would deal with it. I said it was hateful conduct and racialised sexual harassment, and should be followed up. I believe the police should be calling out and naming sexual harassment and racist abuse online, rather than saying they might have difficulty identifying the perpetrators.”

Abuse in the virtual workplace

The COVID-19 pandemic has dramatically changed working patterns. Figures from the ONS showed that as of April 2020, 46.6% of people in employment did some work at home. Of these, 86% did so as a result of COVID-19. For hundreds of thousands of employees, the shift from office work to online remote working took place within a matter of days. As COVID-19 continues to spread around the world, UK businesses and organisations have remained reluctant to bring staff back to the office.

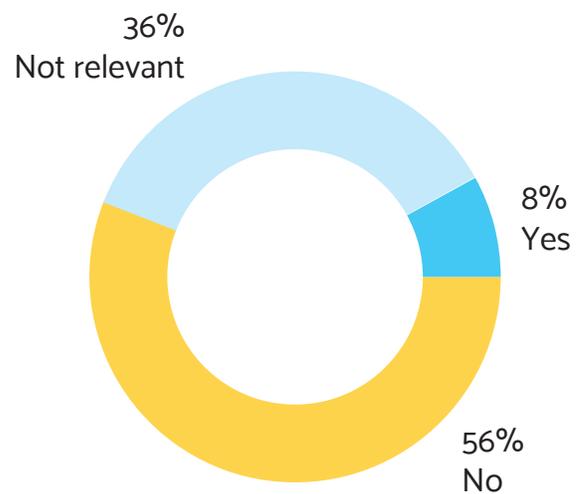
This rapid increase in remote working has had deep implications for employees' safety and wellbeing. Homes have turned into improvised workplaces, while video conferencing systems and co-working platforms such as Zoom, Google Meet and ASANA have gained millions of new users in the space of a few months. Safety concerns have emerged around platforms frequently used for work during the pandemic, with numerous instances of zoombombing receiving media attention.

Our survey aimed to assess the impact of the widespread shift to remote working on the online safety of women and non-binary people, and understand how employers have been responding to this change.

Respondents were asked if they had received updated guidance on staying safe online while working from home. Only 8% of respondents said they had received specific safety training or guidance, while 56% of respondents said they had not. The question was irrelevant to 36% of respondents.

These figures show that safety in online working spaces remains a blind spot for too many employers at a time when employees spend more and more time online and vulnerable groups face a greater risk of online abuse.

Figure 8. Prevalence of training or updated guidance about the risk of online abuse

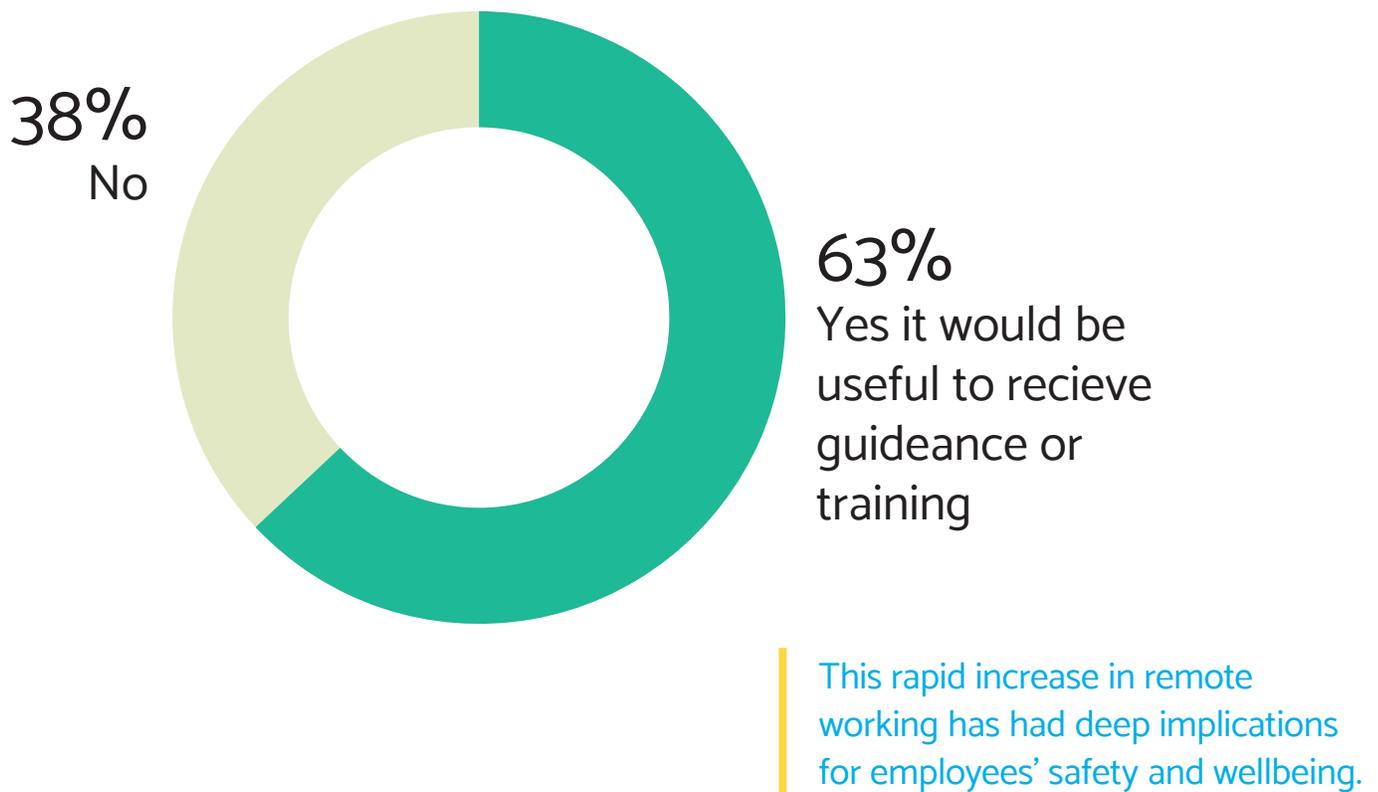


Percentage of respondents who received online safety training from employers or similar entities

³² "Coronavirus and homeworking in the UK: April 2020," ONS, 8 July 2020 <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/coronavirusandhomeworkingintheuk/april2020>

³³ Emily Bary, "Zoom, Microsoft Teams usage are rocketing during coronavirus pandemic, new data show," Marketwatch, 1 April 2020 <https://www.marketwatch.com/story/zoom-microsoft-cloud-usage-are-rocketing-during-coronavirus-pandemic-new-data-show-2020-03-30>

Figure 9. Most women would like to receive guidance from their employer or volunteering supervisor about the risks of online abuse



Employers' obligations to their staff under UK law are determined by a range of legislation pieces, including the Health and Safety at Work Act (1974) and the Workplace (Health, Safety and Welfare) Regulations (1992). In practice, this means that employers need to "take as much care for employees and others affected by the business as is reasonably practicable" but in the absence of clear governmental guidance, these obligations are not always clearly understood in relation to online safety, making comprehensive governmental guidance necessary. not include any recommendations for employers On 11 May, the UK government unveiled its plan for a phased lifting of social restrictions related to

COVID-19. Governmental guidance, however, does about the safety of staff who work from home. In the absence of governmental regulation or guidance, training on digital safety and wellbeing remains at the discretion of individual companies, and would remain so in the event of a potential national lockdown or localised lockdowns.

Responses to our survey show the majority of employees feel updated training would be useful to them. 62% of respondents who did not receive any guidance from employers said that training or guidance about online abuse would have been useful.

Testimonials

To compliment the findings from the survey, we carried out more detailed interviews with four respondents who agreed to provide further details about their recent experience of online abuse. These testimonials are presented below. Minor edits have been made to the testimonials for clarity while preserving the full meaning of the respondents' testimonial. Details that would allow a person to be identified have been removed to protect the respondents' privacy and anonymity.

Testimonial 1

The respondent received misogynistic and racist abuse online after sharing a post on the rise of domestic abuse during lockdown and posting a picture of their son on social media.

"I shared a post on the rise in domestic abuse during lockdown and received dozens of misogynistic messages telling me I deserved to be abused, calling me a liar and a feminazi. My scariest experience, however, was when I shared a photograph of my young son and me. It was picked up by someone I assume to be on the far right, who retweeted it. Subsequently, throughout the day I received dozens of racist messages and threats directed at my son, at his father, and at me. It was terrifying. I am normally very private with my social media profiles and don't share photos of my son or information about myself.

The attacks left me feeling violated and invaded. I felt under threat and unsafe. I knew rationally that they were a bunch of sick bullies but it really scared me, even though I was in my home. My son and I have been racially abused in public; some men shouted racist abuse at us as we walked down the street. It felt just the same even though it was online, it still hurt as deeply and was as scary. I don't think people realise that. I reported the abuse we received in public to the police but I don't know if I can do that online? I reported each abusive message to Twitter, changed my profile settings, removed the photo and blocked multiple accounts.

(Testimonial 1 continued) I have always been guarded about sharing personal information but after some of the experiences I have had, I am much more guarded. I have all my profiles set to private and I don't speak as confidently or share opinions as publicly as I used to. Trolls want to silence women and minorities, and their abuse works. It has made me think badly of companies like Twitter and Facebook. I use Facebook way less than I used to, maybe once or twice a week, as some of the views on there are just hate speech.

I've used Twitter's filters to try and block people out but they don't do enough to moderate and kick out these people off the platform. When you look at some of these people's profiles, you can see they make vile comments and threats all day long. Twitter has never followed up with me to let me know what action they took. Likewise, I have reported hate speech on Facebook and they haven't let me know what's happened. It's not good enough. If people take the time to report, you should take the time to let them know the outcome. It's worse than doing nothing at all."

Testimonial 2

The respondent experienced misogynistic abuse in the comments section of BBC Have Your Say after sharing their opinion on political issues.

"I have been subjected to misogynist written abuse on BBC Have Your Say but as this site is monitored, I was able to get the BBC to take down the abusive comments quickly (within a few minutes).

I do feel social media isn't a safe space for women. Because I'm interested in politics, I've noticed that female politicians have tended to suffer misogynist and other abuse, for example racist abuse on social media.

(Testimonial 2 continued) I think this abuse is likely to deter women from becoming or remaining politicians and this is very bad for women, racial equality and for democracy. I haven't wanted to be on social media because I don't want to be subjected to abuse, but the fear of abuse is silencing me, which is presumably what the abusers want, and I feel regret that they have silenced me on certain platforms which I haven't joined because of potentially being abused. I've noticed that women are generally subjected to abuse on social media and particularly if women have strong opinions like I do."

Testimonial 3

The respondent faced online abuse during the Black Lives Matter (BLM) protests in the UK and received racist and sexist abuse from a troll account after posting a picture of themselves in support of BLM.

"The incident made me feel vulnerable, vulnerable to the absolutely relentless male sexualising and porn-sick gaze, sickened by the sexism and racism, angry at the entitlement of this man to barge into my mentions to cheapen a political protest and resigned to there being no consequences for sexual harassment.

Tech platforms replied agreeing that it was offensive and the abuse was removed, but it had already been seen by hundreds of people. It was up for days. Simply deleting a tweet or an account for violating platforms' standards does not do enough to send signals to men about why their conduct is unacceptable. He will just set up a new account and carry on being a racist sexist. The platforms could have asked me if I wanted them to send him a message about why his comment was unacceptable, copying me in and asking him to apologise through them to me.

I also think they should be keeping records of whose accounts are routinely targeted (it will be black women as we know, more than any other group) and being proactive about monitoring those accounts and contacting trolls personally, immediately."

Testimonial 4

The respondent is an influencer in their community and has received considerable abuse as a result of their activism.³⁶

“As a semi public figure and vocal campaigner, I am the target of ongoing low-level harassment both online and offline. I get emails, tweets, Facebook messages, and comments on newspaper articles telling me I am shaming my community, denigrating my looks, denying my experience etc.

At one point someone trawled an old forum I had used to find out personal information and then messaged me on Facebook with threats to release this and other information about me. When these things happen it feels unsafe. The line between online and offline abuse is virtually non-existent.

I am a relatively public figure within my community. It’s not hard to find out where I live. I am always on guard. It’s not a case of just logging off or uninstalling an app. The internet is a way to be heard in the real world, and it is a way to abuse and harm women in the real world too.

Since this kind of abuse began, I am far more careful with my personal safety, both online and offline. I have recently removed Facebook from my phone and have to log in using a web browser if I want to use it. My first consideration when posting something is always ‘will this make me unsafe?’”

³⁶Details and names of platforms have been amended to protect the respondent’s identity.

Conclusion and recommendations

The findings of our survey show that COVID-19 has exacerbated the risk of online abuse for women and non-binary individuals, especially from Black and minoritised backgrounds. The majority of online abuse continues to take place on large mainstream social media platforms despite tech companies' commitments to making their platforms safe spaces for all.

Survey findings and testimonials have highlighted the psychological, emotional and social impact and silencing effect of online abuse, as well as the lack of action taken by tech companies and law enforcement when victims report instances of online abuse.

The deficit in digital citizenship education - already notable before the pandemic - could continue to have a deep effect on the risk of online abuse. Employers have taken limited action to provide training to employees on how to stay safe online and to inform them of their rights and responsibilities.

As the COVID-19 pandemic endures and we continue to rely more on technology and social media in our lives, we need an ambitious multi-sectoral response to the risk of online abuse targeting women and minoritised communities.

Our recommendations to employers, government, tech companies and civil society are outlined below.

Recommendations for employers

Employers should put in place specific training to ensure their employees feel as safe online as possible. Employers have a statutory duty of care for people's health and safety at work and should provide appropriate guidance to staff working from home, including on digital safety. In the absence of national guidance on digital safety and wellbeing best practices, employers should make any reasonable effort to provide updated training to employees and share guidance with their staff. As the findings of Glitch's survey show, only a very small proportion of employees (9%) reported receiving training and the vast majority of employees who did not receive training felt that it would have been helpful. These statistics highlight the need for more training from employers and similar entities.

Employers need to make all reasonable practical provisions to prevent online abuse in the workplace and adopt a workplace policy on gender-based violence and harassment, in consultation with employees and their representatives where possible. Employers need to conduct a robust risk assessment in relation to online abuse and harassment at work, and take measures to prevent these threats. This includes sharing accessible information on the risks of online violence and the rights and responsibilities of employees. 9% of respondents to Glitch's survey experienced abuse from a colleague or superior at work - a figure which shows that employees can also be perpetrators of online abuse.

Recommendations for the government

The government should provide clear recommendations to employers on how to keep their employees safe online and publish national guidance on digital safety, particularly when working from home. Employers have an obligation to protect their employees from harm under UK legislation. However, COVID-19 and the sudden widespread shift to remote working means many employers do not have sufficient training, skills and resources to ensure employees' safety in online working environments. Governmental guidance, and a roadmap for Digital Health and Safety at work, is therefore needed.

The government needs to implement a comprehensive public health approach to tackling online abuse. The government should adopt international standards to address harassment in the workplace, including the International Labour Organisation (ILO) Convention 190 on Eliminating Violence and Harassment in the World of Work, which provides an international framework for addressing workplace abuse and ensuring employers meet their obligations towards their employees. Employers and employees' obligations should be codified in legislation. The government should also ensure that law enforcement officials and frontline workers receive updated training and appropriate resourcing to handle cases of online violence. Testimonials provided by respondents to the survey show that complaints are too often not taken seriously by law enforcement. One respondent said: "I reported the online harassment to local law enforcement, as there

were physical threats via Facebook and Instagram from a stranger. There was no follow-through from the police." (see Testimonials for additional examples).

The government needs to show greater leadership in tackling online harms and make the fight against online abuse a political priority. The publication of the government's Online Harms White Paper (OHWP) in April 2019 showed willingness in tackling online abuse but the proposal includes a number of gaps. The government should ensure that civil society and experts' responses to the paper's consultation are reflected in legislation. As the results of Glitch's survey show, women and non-binary people, particularly from Black and minoritised backgrounds, are facing a greater risk than ever of experiencing online abuse. To adequately address the specific risks that women and minoritised groups face online, "hatred by sex" should be included in the government's definition of online harms.

The government should put pressure on tech companies to do more to tackle online abuse. The government's Digital Services Tax, which came into effect on 1 April 2020, imposes a 2% tax on tech giants including Facebook, Google and Twitter. Ringfencing at least 1% of this new tax annually is needed to fund efforts to effectively address online abuse. This income should be used to enforce existing legislation on online abuse, increase police resources, educate the public on digital citizenship and fund the work of civil society organisations working to end online abuse.

The government should fund further research into the impact of online abuse on women and Black and minoritised communities and intersectional online abuse. Glitch's survey has highlighted a notable increase in online abuse targeting women and non-binary people, particularly Black and minoritised people during COVID-19 but this research was limited in time and scope. In particular, the sample of non-binary and specific minoritised communities was too small to draw significant conclusions. This shows the difficulties in conducting research on minoritised communities and the need for appropriate funding to conduct more in-depth research. Further research is also needed to understand the economical, psychological, social and political impact of COVID-19 on different minoritised groups, and to inform appropriate political responses.

The government should work closely with and consult women's organisations about the risk of gender-based and intersectional online abuse and work with them to inform decision-making. Decision-makers should consult expert organisations working to end abuse against women and people with intersecting identities both online and offline. Gender-based abuse should be also included in the government's digital policy strategy and inform its COVID-19 response and recovery decision-making, particularly around how to make online spaces safe for women.

The government should invest more resources into digital citizenship education in the UK, including how to stay safe online, how to respond to online abuse and how to be an active online bystander. Digital citizenship programmes remain severely underfunded in the UK. As COVID-19 pushes citizens to spend more time at home and rely increasingly on the internet and social media for work, socialisation and volunteering, greater investment in ambitious digital citizenship programmes and support to civil society organisations carrying out this work is vital.

Recommendations for tech companies

Tech companies need to provide greater transparency about their content moderation efforts, including by allowing trusted research institutions and civil society organisations to access anonymised and disaggregated data about content removals and complaints submitted to the platforms, including the type of action taken, the time it takes to review reported content and increased transparency around appeals processes. The findings of the survey show that a majority of complaints about online abuse go unaddressed. Respondents to the survey reported frequent absences of responses to complaints or prolonged response times, while testimonials showed that many have been discouraged from reporting incidents of online abuse due to the perceived lack of action of tech companies. Tech companies need to be transparent about their investment in and resourcing of content moderation, and must invest more resources in human content moderation. Content moderators should be provided with comprehensive training about different tactics of online abuse and how abuse specifically targets women, Black and minoritised communities and users with intersecting identities.

Tech companies should provide more transparency about their policies related to dehumanising language based on gender, ethnicity and other protected categories. Policies should be regularly reviewed and updated to address new trends, patterns and manifestations of online abuse, including violence against women and people with intersecting identities. The COVID-19 pandemic has shown that manifestations of online abuse keep evolving and require companies to keep monitoring their platforms.

Tech companies need to provide more financial support to civil society organisations working to tackle gendered and other types of abuse and harassment online and fund digital citizenship education initiatives. Funding is particularly vital to civil society organisations working with marginalised communities. Large social media companies should also cooperate with anti-racist, LGBTQ+ and women's advocacy organisations to fund research into the impact of gender-based and intersectional online abuse. Partnerships between data scientists and social science researchers are needed to carry out research projects about how gender, gender identity, sexual orientation and ethnicity play a role in online abuse.

Tech companies need to do more to address gender-based intersectional abuse on their platforms, in particular abuse targeting Black and minoritised women. As the findings of Glitch's survey show, Black and minoritised women and non-binary people have been disproportionately targeted by online abuse since the beginning of lockdown and are more likely to report that their complaints are not properly addressed. Reporting processes should be improved and made easier for users of the platforms. Survey participants reported that responses to complaints are not timely enough and highly abusive content remains on the platforms hours - sometimes days - after being reported.

Tech companies need to do more to identify repeat offenders and make it more difficult for accounts that have been banned from platforms to resurface. IP addresses linked to permanently deleted accounts should not be able to recreate accounts for a significant period of time. Companies should also provide users with greater control and filters over their online experiences to ensure that they have greater agency and decision-making power over the type of content they see on social media and which users can communicate with them.

Recommendations for civil society

Research and civil society organisations working to end online abuse and harassment need to do more to understand the specific risks faced by minoritised communities. This survey and research highlighted the difficulties in obtaining significant datasets about particular minorities communities. While the survey gathered the largest dataset of responses about the impact of COVID-19 on online abuse targeting women in the UK, the data sample of non-binary respondents remained too small to draw statistically significant conclusions - although we were able to gather anecdotal insights. More targeted research is needed to document the online experiences of these communities.

Civil society organisations, charities and NGOs, particularly those with a strong brand presence online, should be at the forefront of digital health and safety in the workplace and should implement an online code of conduct that places online safety at its centre.

Civil society organisations working to end online abuse, gender-based violence, structural racism and other inequalities need to work together and create partnerships to implement responses and action programmes. While many initiatives attempting to tackle online abuse against women and people with intersecting identities have emerged in the UK, existing projects too often remain siloed. Civil society organisations need to build synergies and combine their respective expertise in research, training and interventions to ensure a more comprehensive response to the problem.

Appendix

* 1. Has your Internet usage increased during COVID-19?

Yes

No

2. If you have responded yes, please tick which reasons are relevant to you. (Please tick all that apply)

Increased internet usage for work

Increased internet usage for socialising

Increased internet usage for news

Increased internet usage for volunteering (including mutual aid)

Other (please specify)

* 3. What is your employment status in COVID-19? (If you have had several working situations, please select the one which you think reflects your situation most accurately)

Not working

Furloughed

Working from home

Working in my usual workplace

Volunteering

Self-employed or freelance

Stay-at-home parent/Looking after family members or relatives/Caring responsibilities

Other (please specify)

YOUR EXPERIENCE OF ONLINE ABUSE DURING COVID-19

Glitch uses the phrase “online abuse” as an umbrella term to capture a plethora of tactics and harmful acts experienced by individuals online. Online abuse can include - but is not limited to - offensive or discriminatory comments and insults, threats of physical or sexual violence, stalking, harassment, bullying, impersonation, defamation, denial of service attacks, online impersonation, deadnaming, or violations of privacy such as “doxing” (posting private details online such as a person’s address or phone number with the aim to cause alarm or distress) or sharing intimate and private images of a person online without their consent.

* 4. In the last 12 months, and prior to COVID-19, had you experienced online abuse?

Yes

No

* 5. Since the beginning of COVID-19, have you faced online abuse?

Yes

No

6. If you have experienced online abuse in the last 12 months, would you say this has increased during COVID-19?

Yes

No

Not relevant

7. Who have you experienced online abuse from? (Please tick all that apply)

Colleague from work or while volunteering

Manager or someone in a superior position at work or in your volunteering

Family member

Partner or ex-partner

Acquaintance

Stranger/anonymous online user/other person not known to me

Other (please specify)

8. On which platform(s) did you experience online abuse? (Please tick all that apply)

Facebook

Twitter

Instagram

Snapchat

Zoom

Slack

Microsoft Teams

Google Hangouts

ASANA

Email

Facebook Messenger

Messaging services such as WhatsApp and iMessage

Other (please specify)

9. What type of abuse have you experienced? (Please tick all that apply)

Sextortion (a form of blackmail in which sexual information or images are used to extort sexual favours)

Stalking and stalking by proxy (repeated following and harassment, directly by perpetrator or third party)

Doxing (disclosing personal information online)

Identity theft and/or online impersonation

Spying and/or sexual surveillance

Deep fakes (AI-generated videos or recordings aimed at manipulating what a person said)
Grooming and/or predation
Trafficking
Swatting (hoax call to emergency services to bring large number of armed police officers at your address)
Discriminatory comments targeting an aspect of your identity
Violent or graphic images or videos including depictions of sexual violence
Trolling
Google bombing (SEO effort to move a website or search term to the top of search-engine results, often with malicious intent)
Cyber-bullying
Gender-based slurs and/or harassment
Threats of physical or sexual violence
DOS
Electronically-enabled financial abuse
Someone sharing intimate and private images of you without your consent
Deadnaming (calling a transgender person by the name they went by prior to their transition)
Flaming (posting insults and/or profanity or other offensive language)
Mob attack/cyber-mobs
Shock and/or grief trolling
Sexting/abusive sexting
Unsolicited pornography (being sent sexual images without your consent)
Cross-platform harassment
Offline attacks
Other (please specify)

10. What was the abuse related to? (Please tick all that apply)

Gender
Gender identity or gender expression
Sexual orientation
Ethnic background
Religion
Disability
Not related to my identity
Prefer not to say
Other (please specify)

THE IMPACT OF ONLINE ABUSE

11. Has the abuse led you to change your behaviour online?

Yes
No
Unsure

12. If you responded yes to the last question, please specify how. (Please tick all that apply)

Deleted at least one social media account

Locked at least one social media account

Changed notification settings on at least one platform

Deliberately spending less time online/on at least one platform

Deliberately hiding you're online

Blocked someone

Muted someone

Reported someone

Avoided reading messages online

Deleted at least one social media account or application from mobile device

Not relevant to me

Other (please specify)

13. Has the experience of online abuse made you feel different about using technology and social media platforms?

Yes

No

14. Can you please tell us about the psychological impact of the incident(s)? Have you felt any of the below? (Please tick all that apply)

I have felt anxious

I have felt humiliated/ashamed

I have felt unsafe

I have felt less confident

I have felt angry

I have felt unsupported

I have felt confused

Prefer not to say

Other (please specify)

15. Has the experience of online abuse had a professional, social or financial impact on you?

Yes

No

Unsure

Prefer not to say

16. Did you report the abuse? (Please tick all that apply)

To the tech and/or social media platform(s)

To law enforcement

To your employer

To trade unions or industry organisations

To community or charity organisations

I did not report the abuse

Other (please specify)

17. If you reported the abuse, did you feel that your complaint was adequately addressed?

Yes

No

18. If your answer is no, can you explain why you did not think the complaint was adequately addressed and what could have been done to address it?

19. When you faced online abuse, did you know what your rights were and what your options were to report the incident(s)?

Yes

No

20. Is there anything more you would like to tell us about your experience of online abuse during COVID-19? Please provide as much detail as possible. You may want to touch on the following (this list is not exhaustive):

- how the incident(s) made you feel); - if you changed your behaviour online or offline as a result of the incident(s), and if so, in what way?; - if the incident(s) changed your feelings when spending time online, and in what way; - if it has had an impact on your professional and social life, and in what way; - if it had a direct or indirect financial impact on you (e.g loss of income; - if you had any positive or negative interactions or experiences in the aftermath of the incident(s) (e.g support, helpful interactions when reporting...etc)?

* 21. Have you received any training or updated guidance from your employer or volunteering supervisor about the risk of online abuse when working from home?

Yes

No

Not relevant to me

22. If your answer is no, do you believe that training and/or updated guidance about the risk of online abuse when working from home by your employer or volunteering supervisor would have been useful?

Yes

No