Written evidence submitted by Glitch

Response to DCMS - The impact of COVID-19 on online abuse and harassment

Executive Summary

Glitch is a leading UK charity championing everyone's right to be online safely without discrimination, abuse and violence. Glitch has garnered international acclaim, addressing online abuse through groundbreaking work across the world in education, government institutions and workplaces. Glitch has worked with Parliamentarians around the world developing practical solutions with Governments, NGOs, UN Human Rights Council and tech companies to protect our online public spaces from hate and abuse.

The COVID-19 pandemic has radically changed both the amount of time and the way individuals communicate online. In April 2020, over one third of people globally lived under some form of lockdown restriction due to the pandemic which has resulted in a substantial increase in Internet usage. In the initial days of the lockdown in the UK, day-time Internet usage more than doubled.

There is concern that such a drastic increase in people spending time online, for both professional and personal use, coupled with long-standing issues about the harmful impacts of online abuse, means that online spaces are at risk of becoming even more rife with new and existing forms of abusive content. Prior to COVID-19, multiple reports shed light on the extent of online abuse in the UK and beyond. A 2018 report by Amnesty International analysing tweets sent to 778 UK and US female politicians and journalists found that 7.1% of tweets received by these women were abusive or problematic, with black women in particular 84% more likely to receive tweets that were being abusive or problematic than white women in the study. 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.

Individuals disproportionately targeted with online abuse -- such as women and marginalised communities -- face even greater risks in this current context. For example, cases of online abuse during the pandemic documented by the media and women's rights organisations include experiences of unsolicited pornographic videos being displayed while women participate in online social events, as well as violent threats and sexist and racist content directed at individuals from marginalised communities sharing their experiences about the virus. At the same time, lockdown restrictions due to COVID-19 has also led to many technology companies unable to provide content moderation services on their platforms leaving any abusive and harmful content on these platforms unchecked.

Lastly, the lack of investment and resourcing of digital citizenship education -- which refers to the concept of individuals engaging positively, critically and competently in all digital spaces. -- was also a concern prior to COVID-19. The markable uptake in Internet usage means that this gap in education has become even more acute as more people turn to the Internet to complete everyday activities. An urgent need remains for innovative forms of digital citizenship education delivery to ensure all individuals are able to use online spaces safely, freely and free from abuse or discrimination.

New manifestations of online abuse

New manifestations of online abuse have emerged as a result of COVID-19. Platforms which have become popular since the beginning of the COVID-19 pandemic have seen a surge in online harms and news ways of communicating have inevitably led to new manifestations of abuse in online spaces.

This has been most clearly demonstrated on the video-conferencing application Zoom which went from 10 million daily users to 300 million daily participants, ultimately leading to a new phenomena

called ‘zoombombing’. This term refers to perpetrators hacking into private Zoom video meetings and sharing anything from images of extreme violence to images of sexual child exploitation, racist and abusive comments as well as other shocking content. Charities and organisations representing marginalised communities, as well as individuals who experience discrimination due to their different identities (such as race, ethnicity or gender) seem to be particular targets of such forms of abuse on the platform. For example, in April 2020, a black student defending his dissertation on a Zoom call was interrupted when someone scrawled the ‘n-word’ on the screen, drew an image of genitalia, and shared sexually explicit images during the call. In another instance, a zoom call between a globlal network of Muslim organisations about maintaining spirituality and wellness during the COVID-19 pandemic was hacked and the perpetrator drew a racial slur across one of the slides.

COVID-19 has also led to new challenges for certain sectors and industries that have had to quickly adapt to moving their services online but are ill-prepared to deal with the risks of online abuse as a result. For example, universities and higher education institutions are delivering online lectures but UK universities have reported several cases of online harassment, especially targeting young women, since the beginning of COVID-19. In some cases, students have posted extreme pornography in online lectures and have allegedly made ‘degrading and offensive’ comments about female students in an online group chat.

Misinformation Online

COVID-19 has also led to a proliferation of conspiracy theories and misinformation online which in turn has helped fuel targeted abuse and harassment online.

Far-right extremist groups have grown in online presence since the beginning of the pandemic by circulating harmful conspiracies about the origins of the virus and blaming specific marginalised communities for its spread. Such misinformation has spread rapidly online and has resulted in both online and offline attacks against specific communities. In the UK, police registered a 20% increase in anti-Asian hate crimes since the beginning of lockdown with more than 260 offences recorded against Chinese people in the UK who described being punched, spat at, coughed on as well as being abused both verbally and online. In the UK, 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.

Workplace harassment

COVID-19 has radically re-shaped many workplaces as thousands of companies shift to online and remote working. Prior to COVID-19, research by the TUC showed that women and LGBT people 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. Glitch is concerned that these same groups are at risk of facing workplace harassment in online spaces.

Employers have an obligation to protect their employees and address violence in the workplace under the 1974 Health and Safety Act. However, the sudden shift to remote working means many employers may not have the training, guidance, skills and resources to ensure employee safety in online work environments.

The ILO Convention 190 on Eliminating Violence and Harassment in the World of Work also provides a helpful framework and global standards to end violence and harassment in the world of

work, but has not been ratified by the UK.

Domestic violence, stalking and harassment

Since lockdown restrictions the UK has registered a surge in reports of domestic violence with a 50% increase in calls to the domestic violence helpline Refuge. The lockdown-related increase in domestic violence reports is putting pressure on support services, with reports in the UK showing that refuges for victims of domestic violence are running out of space. Stalking support services and police in the UK have reported a surge in cyberstalking during the first four week of the lockdown via social media, messaging applications and emails with the main stalking behaviours reported to the helpline during the lockdown being unwanted phone calls, emails, text messages and contact over Whatsapp, Facebook and Instagram. The UK has also seen an increasing trend in the posting of intimate and private images without consent and sexploitation with the number of visits to the Revenge Porn Helpline website doubling in the week beginning March 23, 2020.

Content Moderation

COVID-19 has also raised new challenges for content moderation astech giants have come to rely almost exclusively on artificial intelligence (AI) to moderate online content, with Facebook closing all its content moderation offices during the pandemic. As staffing resources are being reduced, there are concerns about the ability of tech companies to carry out their duty of care. The Internet Watch Foundation, a UK charity that identifies child sexual abuse content online, found that the number of URLs containing images of child sexual abuse online taken down has fallen by 89% as both tech companies and law enforcement must operate with reduced staff.

Increased reliance on artificial intelligence to filter out abusive harmful content on social media platforms during the pandemic can lead to erroneous content moderation decisions. Moreover, detailed and disaggregated data about the type of content deleted by platforms remains difficult to access by researchers.

Policy Implications and Recommendations

In April 2019, the UK government released its much awaited Online Harms White Paper (OHWP), setting out proposals to tackle problematic content and behaviours online, ranging from harmful to illegal. The OHWP introduced the concept of "duty of care" in relation to online harms, placing responsibility on tech platforms to ensure sufficient user protection.

Despite commitments by tech companies to curb the online harms arising from the COVID-19 pandemic, abuse and harmful content continues to thrive in online spaces, while new forms of online violence present fresh challenges to both platforms and governments. Multiple reports have shown that women and marginalised communities, who are at higher risk of facing online abuse, have been heavily impacted by the pandemic's effect on online safety.

Despite anecdotal evidence, there remains a lack of evidence and data about the scale, nature and extent of online abuse in the UK since the start of the COVID-19 pandemic. We encourage the DCMS to consider the following recommendations:

Recommendations to the Government

- Glitch calls on the government to urgently undertake research about the heightened risk of abuse in online spaces, any new manifestations and patterns of abuse online, and the increased proliferation of harmful content online as a direct result of increased Internet usage and the COVID 19 pandemic. There is an urgent need for data about the economical, psychological, social and political impact of the crisis on women and marginalised communities in particular.

- Glitch reiterates that women, girls and marginalised communities face a higher risk of online abuse and calls on the government to consult with diverse women's organisations about these risks and include women in the COVID-19 response and recovery decision-making, particularly around how to make online spaces safer for women in the current context.

- Glitch calls on the government to educate citizens about digital citizenship, how they can report online abuse, and how to access related help and services during the COVID-19 pandemic.

- Glitch calls on the government to provide guidance to employers on the measures they must take to ensure employees are protected from online harassment in remote and online workplace environments. Although any measures to protect employees from online harms remain at the discretion of companies, national guidance on best practices to protect employees online are urgently needed.

- Glitch calls on the government to urgently provide digital safety and self care resources to help ensure all digital citizens can safely, freely, equally and competently navigate and use online spaces.

- Glitch calls on the government to implement ILO Convention 190 on Eliminating Violence and Harassment in the World of Work.

- Glitch calls on the government to include “hatred by sex” in its definition of online harms in the Online Harms White Paper.

Recommendations to tech platforms

- Glitch calls on technology companies to provide greater transparency about their content moderation efforts in the current coronavirus context, including allowing researchers and civil society organisations to access anonymised data about content removals and complaints submitted to the platforms. There remains an overall need for data about the gendered dimension of online abuse, hate and harassment on online platforms and how tech companies are responding to such particular risks.

- Glitch calls on technology companies to provide support to civil society organisations working to tackle gendered and other types of abuse and harassment online and fund digital citizenship education initiatives and provide greater visibility to organisations seeking to prevent online harms. Since the beginning of the crisis, companies such as Facebook have taken steps to highlight scientific content from established institutions (e.g WHO) in users’ feed and have provided advertising credits to increase the visibility of scientific content in an effort to tackle disinformation. While these efforts have had a positive reception, they fall short of addressing the scale and proliferation of hate and abuse on the platforms during the coronavirus crisis.

Glitch will be available to provide further information on any of the above points and attend future meetings to answer questions and or provide an oral statement.

Fixtheglitch.org