Online abuse: addressing new forms of control

With the average user now spending 24 hours per week online\(^1\) doing everything from shopping and sharing photos to building new relationships, the internet encompasses and intersects with almost every aspect of life. The team at Glitch argue that digital interactions are so fully intertwined with relationships and wellbeing that conversations about harm and abuse will remain incomplete if they do not engage with the challenge of cyberspace’s toxicity.

**By the Glitch team**

Over the past decade, the rise of social media platforms has, sadly, created more tools and spaces for perpetrators of domestic abuse — and other forms of violence against women and girls (VAWG) — to target victims.

We have all encountered, and many of us have dealt firsthand with, ‘trolls’ who thrive off conflict and intentionally spread hate online. This is only the tip of the iceberg. There is more that, unless reported, stays hidden in direct messages, closed groups and member-only forums.

Women are most at risk. Published in December last year, Amnesty International’s Troll Patrol study\(^2\) found women who are active in public life are abused every thirty seconds on Twitter, and women of colour, LGBTQ+ identities or women affected by disabilities encounter more extreme and specific forms of hate online. The internet, despite its potential to connect and illuminate, can be intensely unpleasant.

Abuse online not only mirrors offline forms of abuse, but it is also perpetuated and amplified more rapidly and on a greater scale. To effectively combat it we must understand its many forms and recognise online abuse as a category of domestic abuse and VAWG more broadly.

For example, stalking (and stalking by proxy, through the use of fake accounts and profiles), is made simple with the internet. Stalking is a common strategy for abusers to initiate or escalate harassment, and to exercise control over victims. Online, users may be followed across different sites and platforms, or even find themselves bombarded with offensive, often personal, images and messages. 2018 saw the first UK conviction for stalking using a smart home device after a woman was targeted and spied on through her iPad by an estranged partner. The internet provides easy access to a wealth of data; it can be used to gather information on victims’ offline lives too. This violation of privacy can result in doxxing, which
is a word derived from the word document that describes when a user's personal information is published in detail online and weaponised against them.

The internet makes the perpetuation of abuse easy by offering tools and platforms that can be used to target others with gender and race-based slurs, threats of violence, deadnaming (deliberately disrespecting transgender identities), shaming or policing women's behaviours and appearances and more, all with little chance of abusers being held to account. Revenge porn, for example, is a form of abuse that involves shaming and humiliating victims by distributing sexually explicit images or footage of them without their consent. Images can spread rapidly online, causing victims extreme distress. Figures from 19 of 43 police forces in England and Wales show the number of cases of revenge porn investigated by officers more than doubled in the last four years — from 852 in 2015-16 to 1,853 in 2018-19. However, the figures also reveal the number of charges fell by 23% during the same period.

There remain severe challenges with police capability and resourcing that limit the extent to which new and evolving forms of VAWG can be addressed. Sadly, often criminal justice responses encourage victims to reduce their online presence, which is a form of victim-blaming and does little to address underlying problems. The internet can quickly compound domestic abuse and broader VAWG, nudging it beyond the reach of legislation. We must address what happens in digital spaces, beginning by broadening conversations about abuse to include the online interactions that expose women to harm. Civil society organisations are already driving progress in this area, with Refuge's tech abuse project, and Women's Aid's 2017 guidance on the safe use of digital technologies. Glitch's Toolkit, designed to help facilitate and prompt discussion of ways to address online gender-based violence, has been downloaded worldwide since its launch in February. Glitch also delivers digital resilience training for women in public life and works to help young people practice healthy digital citizenship.

However, the scale and pace with which online ecosystems evolve pose significant challenges. As the internet becomes more embedded in, and connected with, our surroundings and devices through the Internet of Things (IoT), new avenues for abuse will emerge; stronger coordination and awareness of challenges here will be needed. An example of an online community growing at a large scale and fast pace is the Alt Right movement. This group is made up of mostly young, white men, who feel disenfranchised by modern society. They have found a way to cope through weaponising online spaces, using memes to help recruit new members. The Alt Right has become a gateway to Incels, which stands for “involuntary celibate” and has violent tendencies, actively praising men who have killed women and celebrating when women are harmed. With many of their members being digital natives, these groups are very internet-savvy and we will require ambitious and effective policy, not to mention increased police resourcing, to stay ahead of the curve.

January saw the publication of the government's draft domestic abuse bill, which acknowledged the serious social, economic and personal costs of domestic abuse and proposed measures to address it. Notably, the bill introduced the first ever statutory definition of domestic abuse to include non-physical manipulative abuse, economic abuse and more.

Forms of abuse outlined by this definition are perpetuated online as well as off but in its current state, the bill fails to engage fully with this reality. The proposed Domestic Abuse Protection Order (DAPO) brought forward in the bill will prohibit perpetrators from making offline and online
contact, however, perpetrators who breach current orders often face no consequences. More robust enforcement is needed to ensure survivors are truly safe across the plethora of online spaces.

Research for the bill revealed that between 2016 and 2017, domestic abuse cost England and Wales £66bn, with £47bn arising from the physical and emotional harm of domestic abuse. Without addressing online abuse, these costs will remain high and may even increase, while investments focused solely on offline abuse could be undermined if harms perpetuated online go unchecked. With profit-making internet platforms increasingly serving as core infrastructure for navigating and networking in our social, professional and civic lives, proposals need to carefully consider how abusers exploit the lack of accountability and regulation online and to ensure parity across online and offline standards.

It was not long ago that the domestic sphere and relationships rooted within it were considered too private and personal to be seriously investigated and subjected to legal scrutiny. From the late 1960s, the feminist call for the personal to be recognised as political has enabled issues formerly dismissed as private to be firstly acknowledged, and ultimately examined and addressed through legislation. It is time to do the same with online activity.

Challenging the lack of accountability online requires a deep dive into how online and offline worlds are connected. Abuse that begins offline can be continued online, but the reverse is also true. Unchallenged, hate online can inspire violence offline, which feeds a slow undercurrent of misogyny that threatens to corrode decades of progress made on women's rights and equality. In the short term, people get hurt. In the long term, a silencing effect could see women withdraw from online ecosystems. This would prove devastating for representation, and impoverish democracy, narrowing perspectives that inform policy and further reducing opportunities for women to be heard. Amnesty International's 2018 research reveals that, alarmingly, women are already censoring themselves online, and even withdrawing from social media platforms.

Fortunately, there is a growing consensus within the tech sector that change is urgently needed. In February this year, Twitter co-founder Jack Dorsey admitted progress in improving safety on the platform has been ‘scattered and not felt enough’ and has ‘put most of the burden on the victims of abuse’. Currently, Facebook relies heavily on contract workers, whose difficult working conditions and low pay evidences a lack of investment to regulate content. It is not enough to expect social media companies to make their platforms safer. Systematic change is needed, not only to respond to abuse but to also prevent it happening in the first place. Further, it is needed to empower women to recognise and respond to abuse’s many forms.

Where to begin? The internet — fragmented, intangible and ever in flux — might seem too complex to regulate. Digital ecosystems have developed so rapidly that policy is left to catch up. In April, the government published its first proposals to improve online safety in the Online Harms White Paper. The paper sets out the government's plans for a world-leading package of measures to keep UK users safe online, with a view to making the UK the safest place in the world to go online. It proposes a new duty of care towards users, which will be overseen by an independent regulator.

This is welcome progress and hopefully the foundation for far-reaching change. Smarter policy will be crucial for structuring and embedding long-term change, to lift standards and communicate that abusive
behaviour is as unacceptable online as it is offline. An intersectional approach that includes marginalised and vulnerable groups will be key to getting this right.

This must start with acknowledging the disproportionate impact of abuse on individuals facing intersectional discrimination. For example, a Survation poll, commissioned by Level Up last month, found that 56% of women under 25, and 40% of women from a black and minority ethnic (BME) background, said they had been harassed at least once on Facebook. It will also be important to include many diverse civil society groups working on online harms and tech-related violence, and learn from their insights and expertise. More broadly, fostering healthy digital citizenship will require all users of digital space to be engaged, whether innovators, perpetrators of abuse, or bystanders.

Beyond this, to improve parity between the treatment of online abuse and offline abuse, more investment will be needed to support frontline services with expertise on tech-related violence, and to improve the coordination of law enforcement, civil society groups and tech companies to work on the unique intersections of domestic abuse and technology.

The internet will become what we make it or what we let it grow into; we all have an interest in ensuring online spaces reflect progress made offline. You can support the call for change by supporting and sharing Glitch’s tech tax campaign, a call for 1% of revenues from the tax on tech companies to be ring-fenced for funding initiatives to make the internet safer.

You can also help drive a cultural shift to ensure that future conversations about domestic abuse are complete in discussing online abuse. Further, being an active bystander — someone who speaks out or intervenes where they see abuse being perpetrated — will challenge abusers and support victims. This could involve checking in with the person being targeted and expressing support for them, as well as reporting abuse where you see it. More broadly, demonstrating positive digital citizenship could break the silence that lets trolls go unchallenged – you can find more resources at https://fixtheglitch.org/glitchukresources/.

**Glitch is a small but ambitious not-for-profit organisation that exists to end online abuse.**

**Follow us on Twitter @GlitchUK**

### Notes


