Joint Statement

July 2019

Online Harms White Paper: The Duty of Care in our Democracy

Signatory organisations:

CarnegieUK TRUST
CHANGING MINDS • CHANGING LIVES

GL!TCH
Fix the glitch to end online abuse

DEMOS

ISD Institute for Strategic Dialogue

doteveryone

Fawcett
Equality. It's about time.

THE JO COX FOUNDATION

With support from Digital Action

The DCMS Secretary of State has said that, under the Duty of Care, companies 'should be expected to take responsibility' for what they do as platforms. In line with this, we urge the Government to focus regulatory efforts on a proportionate, sustainable model of Duty of Care that embraces issues of platform design and transparency, to strengthen our democracy.

Along with terrorism, extremism, and the exploitation and abuse of children, the White Paper highlights a number of threats which can be grouped together as threats to democracy in the UK: viral disinformation, manipulation of the information environment, and online abuse. These are daily attacks on individuals' fundamental rights to freedom of expression, privacy, and association, which are fundamental to our democracy. They inhibit democratic engagement, corrode civil responsibility, corrupt political discussion, and put at risk those who take part in public debate. In the context of the Duty of Care, it is crucial to note: these harms to our democracy are all exacerbated by system design decisions that the companies make.

Technology companies - like all others, and like all citizens - have rights and responsibilities in our democracy. If applied appropriately and embracing the UN Guiding Principles on Business and Human Rights, the systemic, overarching approach of the Duty of Care could help to ensure that UK democracy is strengthened by the participation of a vibrant tech sector.[1]

Online harms and citizens' human rights in our democracy

- **Disinformation** threatens to distort electoral outcomes, remove transparency from political debate and undermine the public's faith in rational and accountable political decision-making. It is used to disseminate hate speech, and to suppress voter turnout among already-marginalised groups. The prevalence and impact of disinformation – and therefore its impact on our democracy – is, as noted in the White Paper, mediated by the tech platforms themselves.
- **Manipulation of the information environment:** as the White Paper

[1] While the Electoral Commission will also have a role within any defined electoral period, all the harms to democracy identified in the White Paper play out on an ongoing basis, and so would be outside of the Electoral Commission's mandate.

rightly sets out, "[a] combination of personal data collection, AI based algorithms and false or misleading information could be used to manipulate the public with unprecedented effectiveness." Over time, the progressive subdivision of the public into ever more precisely-defined target audiences traps people in "filter bubbles" to whom the platforms' algorithms then feed a steady diet of similar, or progressively more polarising or extreme, content that reaffirms and entrenches pre-existing beliefs. To hold the attention of these groups (so they can be shown more ads and share more content), platform company algorithms help to generate a climate of outrage and sensationalism, normalising what were once extreme views.

- **Abuse and intimidation of public figures, especially women.** As the Prime Minister said last year, this constitutes a threat to the healthy public debate that is essential for our democracy. Black, Asian and Minority Ethnic (BAME) women MPs receive 41% of abusive tweets. Abuse often takes the form of threats of sexual violence, with one UK MP receiving 4000 sexually abusive Tweets per week. This has a direct impact on individuals' rights to expression and participation in democratic processes. It also has what Amnesty UK have identified as a 'silencing effect', particularly on marginalised groups like women and girls, deterring others from participating in public debate or influencing them to self-censor themselves online to reduce the likelihood of abuse. Black women are disproportionately affected, being 84% more likely than white women to be mentioned in abusive or problematic tweets. It is important to note that those with multi-intersecting identities will experience online abuse differently and in most cases be disproportionately impacted.

The Duty of Care and our democracy

The proposed independent regulator should hold companies to their responsibilities under their Duty of Care to:

- Give consideration during the design process to the likely consequences for human rights of design choices (taking into account the likely behaviour of its users); and
- Take reasonable steps to guard against those matters that could be harmful to democracy but can be reasonably foreseen.

In each of our individual submissions you will find more detailed policy recommendations, but in summary, the proposed independent regulator should take measures that would strengthen our democracy in five key areas:

- **Redress:** companies should give users a clear explanation of the user journey for complaints, including the appeals procedure; the regulator should be able to review the user journey against benchmarks, including through qualitative, outcome-focused surveys of complainants. There should also be functions for redress for societal harms, and for harms replicated across large groups.
- **Algorithms:** the proposed regulator should have powers and the in-house expertise to undertake algorithmic audits. To do this, the regulator should be able to: examine the purpose, constitution, policies, and outcomes of the systems; identify and assess what data was used to train the algorithm; and examine the model itself as well as

undertaking “white-box testing” to analyse the source code, or the statistical models in use, including how different inputs are weighted.

- **Data rights:** the proposed regulator must work with the Information Commissioner's Office to ensure regulatory work tackling the complex and opaque ecosystem of data exploitation that enables online targeted advertising and contributes to online harms is approached holistically.
- **Advertising transparency:** ad transparency applies with broadcast and print advertising, and should apply online, too. Monitoring during the European Parliamentary elections found that Facebook and Google were unable to reliably differentiate between political and non-political online advertising. For instance, non-political adverts for companies like Ikea were tagged as political, and political adverts in support of the German far-right AfD were not tagged as political. Therefore transparency should apply to all online advertising, drawing on work by Mozilla and Privacy International.
- **Education and training** that goes beyond ‘empowering users to manage their online safety’ and towards digital citizenship, which should be defined in statute. This approach targets the whole online community, including potential perpetrators and bystanders, and providing particular support for the most vulnerable and marginalised groups. Support should emphasise the need to equip individuals with skills to practice forms of social participation that are respectful of human rights and dignity through the responsible use of technology.

Conclusion

In coming together to make this joint statement on online threats to democracy, we wish to draw attention to the opportunity that the Government has to use the proposed statutory Duty of Care to ensure that the UK is a fair, inclusive and thriving democratic society. We look forward to working with you to develop this approach in more detail.

This statement was coordinated by Digital Action
For more information contact:
Nick Martlew
info@digitalaction.co
www.digitalaction.co