CDEI calls for overhaul of social media regulation

The CDEI publishes recommendations to make online platforms more accountable, increase transparency, and empower users to take control of how they are targeted. These include:

- New systemic regulation of the online targeting systems that promote and recommend content like posts, videos and adverts.

- Powers to require platforms to allow independent researchers secure access to their data to build an evidence base on issues of public concern – from the potential links between social media use and declining mental health, to its role in incentivising the spread of misinformation

- Platforms to host publicly accessible online archives for 'high-risk' adverts, including politics, 'opportunities' (e.g. jobs, housing, credit) and age-restricted products.

- Steps to encourage long-term wholesale reform of online targeting to give individuals greater control over how their online experiences are personalised.

The CDEI recommendations come as the government develops proposals for online harms regulation.

The Centre for Data Ethics and Innovation (CDEI), the UK's independent advisory body on the ethical use of AI and data-driven technology, has warned that people are being left in the dark about the way that major platforms target information at their users, in its first report to the government.

The CDEI's year long review of online targeting systems – which use personal information about users to decide which posts, videos and adverts to show them – has found that existing regulation is out of step with the public's expectations.

A major new analysis of public attitudes towards online targeting, conducted with Ipsos MORI, finds that people welcome the convenience of targeting systems, but are concerned that platforms are unaccountable for the way their systems could cause harm to individuals and society, such as by increasing discrimination and harming the vulnerable. The research highlighted most concern was related to social media platforms.

The analysis found that only 28% of people trust platforms to target them in a responsible way, and when they try to change settings, only one-third (33%) of people trust these companies to do what they ask. 61% of people favoured greater regulatory oversight of online targeting, compared with 17% of people who support self-regulation.

The CDEI’s recommendations to the government would increase the accountability of platforms, improve transparency and give users more meaningful control of their online experience.

The recommendations strike a balance by protecting users from the potential harms of online targeting, without inhibiting the kind of personalisation of the online experience that the public find useful. Clear governance will support the development and take-up of socially beneficial applications of online targeting, including by the public sector.

The report calls for internet regulation to be developed in a way that promotes human rights-based international norms, and recommends that the online harms regulator should have a statutory duty to protect and respect freedom of expression and privacy.

Roger Taylor, Chair of the Centre for Data Ethics and Innovation, said:

> Most people do not want targeting stopped. But they do want to know that it is being done safely and responsibly. And they want more control. Tech platforms’ ability to decide what information people see puts them in a position of real power. To build public trust over the long-term it is vital for the Government to ensure that the new online harms regulator looks at how platforms recommend content, establishing robust processes to protect vulnerable people.

Dr Bernadka Dubicka, Chair of the Child and Adolescent Faculty at the Royal College of Psychiatrists, said:

> We completely agree that there needs to be greater accountability, transparency and control in the online world. It is fantastic to see the Centre for Data Ethics and Innovation join our call for the regulator to be able to compel social media companies to give independent researchers secure access to their data.