2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Online Harms Team
DCMS
100 Parliament Street
London
SW1A 2BQ

Which? Response to the Online Harms White Paper

Summary

- Which? supports the White Paper proposal for a duty of care. Which? believes it is right that companies enabling the sharing of user-generated content or online interaction should take care of their users.

- Which? believes the proposed scope of the duty of care is too narrow, not future-proofed and would be a missed opportunity to improve the confidence and safety of consumers online. We recommend that the proposed regulatory framework be broadened to include online consumer harms. The scope of harms covered by the regulations should be broad, since the regulator will have the ability to prioritise its activities as the digital marketplace evolves and new online harms emerge. This will future-proof the statutory duty of care.

- Scams and fraud are significant and growing consumer harms that can result in considerable financial and emotional impact on victims. They are also illegal and many scams occur online on the platforms within the scope of the proposed regulator. We therefore are calling for scams to be included within the scope of the online harms regulatory framework proposed by the White Paper.

- The online sale of unsafe products, which are unlawful because they fail to meet legal safety requirements, should also be within the scope of the proposed regulations. Where a product is sold through an online intermediary, their responsibility is currently limited. For this reason, we are calling for the online sale of unsafe products to be included as an online harm.

- Fake reviews should be included in the proposed scope as they are an example of disinformation with intent to harm. A vast majority of consumers rely on online reviews to help make a purchase, but thousands of fake reviews on online platforms mean they are tricked into buying poor quality products and services that are unfit for purpose.

- We would support transparency requirements so that consumers are more aware of the potential harms associated with using online services. Publication of the measures being taken against harmful content and to protect users would also allow organisations, like Which?, to highlight issues and inform consumers.

- We consider it crucial that there is an effective redress system for internet users. We are also interested in the proposal to designate certain organisations with super-complaint powers, but we question how this is envisaged to work. It is not clear if it will be designed to act in a similar way to the existing super-complaint powers under the Enterprise Act 2002 or if it is intended to enable representative actions. If consumer harms are brought into scope, Which? would want to be designated with these powers.

Detailed response

People should be able to access online content and use online services safely and trust that the content is lawful, legitimate and will not harm them. We are pleased to see the proposal for a duty of care for platforms that enable users to share or discover user-generated content or interact with each other online. We believe such a duty of care would shift the incentives and responsibilities of large online companies to the benefit of users and add a layer of responsibility at the level of the online platform to protect users from harmful content.

However, the scope of the White Paper is too narrow. The list of harms it proposes to tackle does not reflect the range of real harms that consumers face online. The government should ensure platforms take greater responsibility for a broad range of online harms, not a selective list.

<u>Broadening the scope</u>

We agree that a new regulatory framework could help protect individuals from harmful and illegal content online. However, the current scope limits the harms that companies will need to consider and address. Since the proposed regulator will have the ability to prioritise the harms it tackles and develop codes of practice to help address them, its remit and scope should be broad. This will enable the regulator to respond flexibly and promptly as new or different online harms emerge or escalate.

Our particular focus is on harm caused to consumers, usually with financial consequences. Consumers should be able to expect the same level of protection and regulation online as offline. If something is considered illegal or is banned offline, then the same approach should be extended to when it occurs online. While some online harms may fall under other legislative frameworks, the existing piecemeal approach to regulation of these harms is ineffective, does not provide adequate protection and is confusing. The responsibility of online intermediaries for protecting their users from online harms is presently unclear, and Which? agrees with the overall ambition of the White Paper to introduce a comprehensive approach to address online harms. Which? also agrees with the proposals to increase

transparency about harm encountered when consumers are using online services as this is very opaque at present.

We set out below some additional online harms which cause significant harm to consumers and which should be included in the scope of the White Paper's proposals. However, we believe these should be incorporated in a broad and flexible scope, rather than as part of an exhaustive list. We also encourage proposals for greater transparency so that consumers can be made more aware of potential harms on competing sites. Greater transparency would also enable organisations to easily access the data in order to inform consumers and draw attention to problem areas.

Which? also recently responded to DHSC and DCMS's consultation on further advertising restrictions for products high in fat, salt and sugar to protect children, as part of the wider childhood obesity action plans. We strongly supported the proposals to strengthen controls over digital advertising, as well as broadening broadcast restrictions. We recognise that this ongoing initiative to address this specific type of online harm is referenced in the White Paper, and it is essential that the government follows up on the consultation with effective controls that address the use of children's data by advertisers and the risks this may pose.

Scams & Fraud

Scams and fraud are a significant and growing consumer problem that is harmful and illegal and occurs over online platforms. We find no evidence that the Joint Fraud Taskforce's work programme overlaps with the proposed online harms regulations and therefore do not believe the Taskforce's existence justifies the exclusion of scams from the White Paper proposals. Some victims of scams lose life-changing sums of money. Even for lesser amounts, the financial impact can still take its toll on the victims, and often there can be more than just a financial cost as victims feel ashamed, can become depressed and lose trust in themselves and the community at large.[1] To give an idea of the scale of the problem, between April and September 2018, from incidents of fraud reported to Action Fraud, the total value of losses was £923m.[2] According to the ONS[3], 306,126 fraud and computer misuse offences in England and Wales were referred to the National Fraud Intelligence Bureau by Action Fraud in 2018. In the same period, 54 percent of incidents of fraud were flagged as cybercrime, that is, where the internet or any type of online activity was related to any aspect of the offence.

Many online scams involve user-generated content on large online platforms. These online platforms will be captured by the proposed regulations in relation to other online harms; logically this duty of care should extend to content which is part of a scam (and therefore fraudulent and illegal).

[1] ABC News (2017), "Psychology of scams: The emotional traps to watch out for": https://www.abc.net.au/news/2017-02-27/psychology-of-scams/8306060
[2] Action Fraud Data (2018), "National Fraud Profile": https://data.actionfraud.police.uk/cms/wp-content/uploads/2019/01/National_Fraud.pdf
[3] Office for National Statistics (2019), "Dataset: Crime in England and Wales: Additional tables on fraud and cybercrime": www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

Examples of scams that involve the use of online platforms

Investment scams advertised via social media, often with fake celebrity endorsements:
A scammer can pay for an online platform to run adverts, which are in fact scams, such as fake investment opportunities. Additionally, fraudsters often post on social media to promote "get rich quick" online trading platforms and these posts frequently use fake celebrity endorsements and link to professional-looking websites where consumers are persuaded to invest.[4] These convincing adverts and posts catch consumers' attention and lead them to being scammed. Which? recently published a story about a case where a woman saw a Facebook ad for a fake investment opportunity involving bitcoin and which referenced support from a Dragon's Den episode.[5] This had previously hit the news as a scam and yet the advert was still on Facebook and unfortunately the woman had not seen the news about this scam. The woman authorised a debit card payment of £300, but the scammers then took another £8,500 from her debit card through four further transactions. It took seven months to get the money back from her bank. If Facebook had a duty of care to its users under the proposed regulations, this ad may never have been permitted onto the website.

Buying counterfeit goods online:
This is an example of what is known as an e-commerce scam. This is where scammers pose as genuine sellers on online marketplaces. Consumers then pay for goods, which may turn out to be counterfeit or poor quality, or they may never arrive.[6] In June 2018, Electrical Safety First published that some of the most popular e-commerce sites are being misused by sellers and exposing buyers to thousands of substandard, counterfeit and suspected recalled electrical goods.[7] Further investigation uncovered dangerous electrical goods for sale across a range of e-commerce sites including Amazon, Amazon Marketplace, eBay and Fruugo. Electrical Safety First found that 92% of British people surveyed believe e-commerce platforms regulate and monitor third party sellers to protect buyers from purchasing counterfeit products.[8] This is clearly an incorrect assumption and highlights the discrepancy between consumers' perception of safety on such platforms and the reality.

Being scammed for goods on eBay:
Internet users can be scammed, even when they are the one selling a product. For example, Which? was contacted by an individual who listed a mobile phone handset on eBay and was quickly contacted by a woman over the platform. She explained she would like to buy the product and was based in Nigeria. The seller requested payment via

[4] Action Fraud (2019), "Over £27 million reported lost to crypto and forex investment scams": https://www.actionfraud.police.uk/news/over-27-million-reported-lost-to-crypto-and-forex-investment-scams
[5] Which? Consumer Rights (2019), "Renewed warnings about Bitcoin investment scams with fake celebrity endorsements":https://www.which.co.uk/news/2019/03/renewed-warnings-about-bitcoin-investment-scams-with-fake-celebrity-endorsements/
[6] Consumers International (2019), "Social Media Scams: Understanding the consumer experience to create a safer digital world", p.7: https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf
[7] Electrical Safety First (2019), "Conline: 18 Million Brits Fall Victim To Counterfeit Electrical Goods Online": https://www.electricalsafetyfirst.org.uk/media-centre/press-releases/2018/06/conline-18-million-brits-fall-victim-to-counterfeit-electrical-goods-online/
[8] Ibid.

Paypal. The seller then received a text from Paypal stating the funds had arrived in his Paypal account including extra for express shipping, and he received an email from the buyer stating the same. He posted the product and paid the express shipping, but later checked Paypal to find that no money had been received. The text had "spoofed" Paypal. The seller contacted eBay about the case. eBay showed no interest in closing the scammer's account. In this case, eBay was the online platform that connected a seller and a scammer, and if scams are included under the proposed new regulations, we would hope that eBay would have an incentive to remove scammers from its platform to meet its duty of care.

<u>Romance scam via dating site/app:</u>
Action Fraud sets out that romance fraud happens when a person thinks they have met the perfect partner through an online dating website, app or social media, but actually a scammer is using a fake profile to form a relationship with them.[9] Action Fraud also reports that 4,555 reports of romance fraud were made in 2018 with losses of over £50 million. Beyond the financial impact on victims, the emotional impact can also be significant and 42% of victims described falling victim to romance fraud as having a significant impact on their health or financial well-being.[10] Online dating websites and apps fall under the White Paper's definition of companies in scope: that is, they are companies that allow users to share or discover user-generated content or interact with each other online. We therefore think that the proposed duty of care should apply to these websites and apps and that they should be incentivised to protect their users from being scammed via their platforms.

<u>Fake holiday accommodation:</u>
Which? provides advice on spotting holiday scams, as we know that scammers use the popularity of sites like Airbnb and Holiday Lettings, to make money by tricking people into booking fake holiday listings. In April 2018, Action Fraud published that losses from holiday fraud in 2017 totalled £6.7 million from 4,700 reported incidents. Action Fraud says that "fraudsters are making full use of the internet to con holidaymakers by setting up fake websites, hacking into legitimate accounts and posting fake adverts on websites and social media".[11] The proposed regulation could incentivise better protection for users from coming into contact with such fake holiday adverts.

When companies act as a platform that connects consumers with scammers, the online harm regulations and duty of care should apply to incentivise the companies to be more rigorous in their checks and to ensure that their users are not being harmed by scams. It may be possible to protect consumers and prevent some of these scams happening in the first place by using the proposed regulations to encourage online companies to take action to prevent their platforms being used to the advantage of scammers.

[9] Action Fraud (2019), "Don't invest your heart in a fauxmance: victims lose over £50 million to romance fraud": https://www.actionfraud.police.uk/news/dont-invest-your-heart-in-a-fauxmance-victims-lose-over-50-million-to-romance-fraud
[10] Ibid.
[11] Action Fraud (2018), "Action Fraud reports show £6.7 million lost to holiday booking fraud": https://www.actionfraud.police.uk/news/action-fraud-reports-show-6-7-million-lost-to-holiday-booking-fraud

Unsafe products

The White Paper proposes to include the sale of illegal goods and services, such as drugs and weapons, within the scope of the regulations. It is not clear whether unsafe consumer products, which are unlawful because they fail to meet product safety legal requirements, are included. Given their unlawful nature and ability to cause harm to those who purchase them online, these should be included in the scope of the new regulatory framework.

Consumers are increasingly buying consumer products through online marketplaces and social media platforms. A recent Which? survey[12] found that 9 in 10 (89%) of UK consumers say they have done so, and 44% in the last month. A quarter (25%) of UK consumers have made a purchase through a social media platform, such as Facebook or Instagram. When consumers buy products from an online marketplace they are buying through an intermediary and may not be aware of the seller's identity. Amazon Marketplace, Facebook Marketplace, eBay and Etsy are all popular examples of online marketplaces. These types of marketplace are no longer novel ways of shopping; they have become normal practice for millions of people. However, consumer protections have failed to keep pace.

Research and testing by Which? has found a succession of unsafe consumer products being sold to people via different online marketplaces, including carbon monoxide and smoke alarms[13,14], child car seats[15], slime[16], and halloween costumes[17]. One of the unsafe carbon monoxide alarms was listed as a bestseller on Amazon. There is also concern that up to 50 lookalike alarms, which may be identical to the unsafe models but packaged differently, were being sold on Amazon and eBay. People can buy these alarms easily and cheaply online and think they are making their homes safer, when in fact there could be dire consequences.

While the traders are ultimately responsible for ensuring that their products comply with product safety requirements, marketplaces currently have no responsibility until they become aware of illegal content when the Electronic Commerce Regulations 2002 require "expeditious" removal. Including online purchase of unsafe products as an online harm in the proposed regulations would incentivise online marketplaces, as well as their sellers, to better protect their users and would enable the number of unsafe products sold online to be reduced. It would also ensure their rapid removal from listings when they are identified, appropriate recall and ensure consumers are given clear information about any unsafe products they have bought and action needed.

We are aware of recent attempts to tighten up the regulatory framework around unsafe products, through the EU Market Surveillance and Compliance Regulation. However, there

[12] Populus, on behalf of Which?, surveyed 2105 UK adults online between 24th – 25st April 2019. The data has been weighted by gender and age to be representative of the UK population.
[13] https://press.which.co.uk/whichpressreleases/silent-alarm-unsafe-carbon-monoxide-alarms-found-for-sale-on-amazon-and-ebay/
[14] https://www.which.co.uk/news/2017/08/unsafe-smoke-alarm-revealed-by-new-which-tests/
[15] https://press.which.co.uk/whichpressreleases/cheap-and-deadly-which-warning-on-the-killer-car-seats-still-on-sale/
[16] https://www.which.co.uk/news/2018/12/hamleys-smyths-and-argos-sell-slimes-containing-chemicals-up-to-four-times-higher-than-eu-safety-limit/
[17] https://www.which.co.uk/news/2018/10/halloween-kids-costumes-from-bm-and-ebay-fail-flammability-testing/

is still a need to clarify responsibilities and ensure the effective oversight of the safety of products sold through online platforms. There is also a question of whether these regulations will be carried forward following the UK's exit from the EU. Therefore, we feel strongly that the online sale of unsafe consumer products should be included in the scope of the proposed online harms regulations.

Fake reviews

"Disinformation" is within the scope of the White Paper's proposals and we agree that inaccurate information can be harmful. The White Paper provides some examples of disinformation and fake news that could threaten public health and safety and undermine democratic values and principles. We consider that fake reviews also fall under disinformation, since they are created with the deliberate intent to mislead consumers, usually for financial gain. We agree with fake reviews being in scope and recommend that they remain in scope as part of disinformation.

We conducted a survey of 2073 adults in September 2018, which found that 97% of shoppers rely on online customer reviews to help make a purchase.[18] A Which? Investigation also found thousands of fake customer reviews on popular products for sale on Amazon.[19] The CMA found that £23 billion of spending in 2015 was potentially influenced by online reviews. This relates to six product and service categories (travel, electronics, books, music, home improvement, beauty products) and since this estimate was made there has been substantial growth in e-commerce. Increasing this estimate by the annual growth in online sales from March 2016 through to March 2019 gives an annual figure of £38bn. Fake reviews therefore have the ability to influence a huge amount of spending and can cause harm both by misleading consumers and reducing consumer trust.

The new online harms regulations could incentivise large online marketplaces to develop more robust systems to prevent and identify fake reviews and prevent consumers being tricked into buying poor quality, or even completely unfit for purpose, products and services.

Super-complaint powers and redress

As a means of obtaining redress for users, the White Paper proposes that the regulator may designate certain bodies with super-complaint powers to raise issues on behalf of users. We currently have super-complaint powers under the Enterprise Act 2002 ('the 'Act'), along with other public interest bodies. These are a very valuable tool in helping to bring issues of consumer harm to the attention of regulators. If consumer harms are brought into scope of the proposed regulatory framework, we would want to be designated with the super-complaint powers in respect of those harms. However, it is not clear to us whether or not these proposed super-complaint powers would work as set out in the Act. It is important to note that super-complaints do not provide an individual means of appeal or redress (for

[18] YouGov, on behalf of Which?, surveyed a nationally representative sample of UK adults in September 2018. Results published in Which? Magazine (Dec. 2018) "Can you trust online customer reviews?".
[19] Which? (2019), "Thousands of 'fake' customer reviews found on popular tech categories on Amazon": https://www.which.co.uk/news/2019/04/thousands-of-fake-customer-reviews-found-on-popular-tech-categories-on-amazon/

example, compensation to users) nor are the designated bodies the destination for the resolution of such complaints.

Our super-complaint powers enable us to raise super-complaints where “any feature, or combination of features, of a market in the UK for goods or services is or appears to be significantly harming the interests of consumers”. We are also aware of The Police Super-complaints (Designation and Procedure) Regulations 2018, which allow designated bodies to make complaints setting out the feature, or combination of features, of policing that is or appears to be significantly harming the interests of the public. These both differ from the provisions under Article 80 General Data Protection Regulation, which allow for a representative to raise a complaint on behalf of an individual on either an opt in (Article 80(1)) or opt out (Article 80(2)) basis[20]. Whether the proposal is intended to reflect the provisions of the Enterprise Act or the GDPR, we would welcome the opportunity to input into discussions and further developments of the super-complaint proposals.

The proposed regulatory framework would also require online companies to have in place an effective complaints process for users. We understand that if this was inadequate, the regulator may have some enforcement powers against the online company. However, more detail is needed about how the regulator will be held to account and what protection internet users will have if the regulator is ineffective at ensuring the companies meet their duty of care. Which? feels strongly that redress should be available for users and we would be keen to be involved in discussions of redress options for the new framework.

About Which?

Which? is the largest independent consumer organisation in the UK with more than 1.3 million members and supporters. We operate as an a-political, social enterprise working for all consumers and funded solely by our commercial ventures. We receive no government money, public donations, or other fundraising income. Which?'s mission is to tackle consumer detriment by making individuals as powerful as the organisations they have to deal with in their daily lives. Which? empowers consumers to make informed decisions and campaigns to make people’s lives fairer, simpler and safer.

For further information please contact Stephanie Borthwick, Senior Policy Adviser, Which? at stephanie.borthwick@which.co.uk.

28 June 2019

[20] Article 80(2) was not implemented in the UK.