Five Online Safety Act Common Misconceptions – Debunked

Author: Nadia Tymkiw, Senior Associate, RPC

The UK's *Online Safety Act 2023* is one of the more divisive pieces of legislation to be introduced in recent years and will fundamentally shape the way the internet operates. It will also inevitably influence the development of online safety law around the world.

Online safety campaigners suggest it doesn't go far enough; digital rights groups are concerned about the significant impact it could have on freedom of expression online and user privacy. The fierce debate risks leading to misconceptions around the legislation.

We dispel some of the common misconceptions below.

1. Only the large online platforms need to be concerned

Not correct. The new legislation applies to any service that targets the UK and operates a website allowing user-to-user engagement or a search engine. There are limited exemptions including email and texts services or services that allow engagement *only* through comments or reviews on content published by the service provider (e.g. product reviews). There are also more burdensome duties applying to higher volume or higher risk services – precisely which companies fall into that category is to be determined in regulations set by the Secretary of State. But the scope of the legislation is extremely broad and almost every service allowing user-to-user engagement or operating a search engine in the UK will need to start implementing appropriate measures to tackle illegal content.

2. The legislation mandates steps to be taken by online platforms to tackle specific pieces of content

Not entirely. The legislation has been described as a "systems" act – introducing statutory "duties of care" and targeting algorithmic processes and technologies used by platforms and search engines rather than individual pieces of content. Platforms and search engines will need to undertake risk assessments to identify the likelihood of users encountering illegal content and, in the cases of services likely to be accessed by children, the likelihood of children encountering content harmful to them – and to put in place measures to mitigate the risks identified. But the legislation doesn't specify the steps or measures to be taken by online platforms to tackle illegal or harmful content. Those measures will be detailed in Codes of Practice produced by Ofcom over the next year. A service provider will be treated as complying with a relevant duty if the provider takes or uses the measures described in a code of practice which are recommended for the purpose of compliance with the duty in question – but it may choose to take alternative measures if it can justify (and keeps a record of) how alternative measures demonstrate compliance.

3. The legislation makes all that is illegal offline, illegal online

The position is more nuanced.

Illegal content under the Act is content which amounts to a criminal offence, rather than anything that could result in civil liability (e.g., defamatory content or privacy-infringing content).

The Act distinguishes between "priority illegal content" (which is that deemed to be higher risk) and "illegal content" and slightly different duties apply to each type.

"Priority offences" are recognised in Schedule 5, 6 and 7 (child sexual abuse offences, terrorism offences, and "other" priority offences) – these criminal offences are already in existence offline and the legislation recognises they can also be committed online (and are deemed "priority illegal content") to the extent (a) the content consists of words, images, speech or sound which amounts to a priority offence or (b) the possession, viewing or accessing of the content, or its publication or dissemination amounts to a priority offence. The Act also recognises that there could be other criminal offences committed online under existing statute. These are deemed to constitute a relevant offence and can amount to "illegal content" under the Act, provided the victim or intended victim of the offence is an individual.

The Act doesn't introduce new sanctions for users who post illegal content or priority illegal content – any action against them would be assessed and taken in accordance with existing criminal law. Instead, the focus is on regulating online platforms' approach to this type of material – requiring services to take proportionate measures to prevent individuals from encountering priority illegal content, to mitigate the risk of services being used to commission or facilitate a priority offence, and to mitigate the risk of harm to individuals posed by all illegal content. That said, the Act does introduce some new criminal offences for users – the majority of which are deemed "communications offences" – for example sending threatening communications or cyber-flashing.

4. The legislation will put an end to end-to-end encryption in the UK

Uncertain, but looking unlikely. The draft Bill never explicitly prohibited end-to-end encryption, but serious concerns were raised about the implications of provisions allowing Ofcom to require companies to use specific technology to identify and take down terrorism or child sexual abuse content. The concern was that this could permit state-backed surveillance of the private correspondence of UK citizens which would infringe privacy and pose a threat to UK national security. Secure messaging services including WhatsApp and Signal threatened to withdraw their services from the UK if the Bill was passed with the provisions included. Following ongoing objections, the government recently acknowledged that Ofcom would only be able to require companies to scan their networks for offending content when a technology had been developed capable of accurately identifying only offending content (which does not yet exist) and, in any event, Ofcom would need

to take into account data protection and human rights law before issuing a notice. The government has stressed that its approach has not changed – and the provisions of concern remain in the legislation – but in practice it looks like they will not be effective until accurate and privacy-preserving technology is brought into existence.

5. Senior managers could be criminally liable for any failure by a company to comply with the Act

Not correct. Whilst the circumstances under which senior managers can be held criminally liable for non-compliance have expanded during the Bill's passage through Parliament, individual criminal liability is still confined to specific areas in the legislation. This includes instances where an in-scope service fails to comply with an information notice which names a senior manager; and where a criminal offence under the Act is committed by the body corporate with the consent, connivance, or neglect of the corporate officer. It's correct that tech executives can be held criminally liable where a company fails to comply with its duty to protect children from harmful content online, but only if Ofcom has undertaken an investigation resulting in a "confirmation decision" requiring the platform to take certain steps to ensure compliance with a child safety duty and the company fails to do so both without reasonable excuse *and* with the officer's consent, connivance or neglect. So, there's no wholesale introduction of senior manager criminal liability which will only arise in specific circumstances.

Event Report: CAMLA's Fireside Chat Illuminates Online Safety

Belyndy Rowe (Senior Associate), Bird & Bird and Chair of CAMLA Young Lawyers Committee

CAMLA's Fireside Chat on Online Safety was hosted at Thompson Geer on 7 December 2023. Attendees enjoyed a dynamic exploration of the ever-challenging landscape of online safety.

Host Justin Quill, Partner at Thompson Geer, set the tone for a thoughtful discussion with special guest Morag Bond, EM Industry Regulation and Legal, eSafety Commissioner.

The eSafety Commissioner stands as a unique regulator, being the first of its kind globally, dedicated to online safety. In line with the Australian Government's commitment to shielding citizens from online harm, the eSafety Commissioner plays a pivotal role in safeguarding the digital experiences of Australians.

Morag Bond brought a wealth of experience to the discussion, offering a unique perspective on her remarkable career and the vital work of the eSafety Commissioner. She delved into the Commissioner's oversight and enforcement of the Online Safety Act, along with industry codes regulating online content to address issues related to harmful material. As the Commissioner faces an important and busy time with new industry codes coming into effect, Morag explained how these codes will empower the Commissioner to combat serious online abuse and tackle illegal and restricted online content.

The conversation expanded to cover the eSafety Commissioner's comprehensive approach, encompassing regulation and enforcement, policy development, and complaint handling. Morag provided valuable insights into the Commissioner's efforts to protect against harmful content, spanning from child sexual exploitation to online bullying and non-consensual sharing of intimate images.

CAMLA would like to thank Morag Bond for generously sharing her knowledge and experience with us and Thompson Geer for hosting this important discussion.