THE UK IS CHANGING THE INTERNET, BUT WILL IT BREAK IT?

Online content is changing society. People need protection – but will law really do that?

The UK's child protection agency estimates that, on average, an online abuse offence against a child was recorded every 16 minutes in England and Wales. That is around 90 cybercrimes against children every single day. Hate can permeate online spaces, and technology can propagate it in a way that simply wasn't possible before the advent of the internet, allowing it to grow and become more harmful.

The internet, therefore, is not a safe place. But nor is the world at large.

American activist, Cameron Kasky, used online platforms to advocate against gun violence. On the one hand, social media and the internet helped him to develop support. But it also exposed him to virulent hate speech and threats of graphic violence. Kasky, speaking to *The Washington Post*, said "People say horrible things to me: That's their right. And I just have to sit there and take it."

For Kasky, online harm is just as inevitable as playground bullying. Except the internet is so vast that maybe nobody will ever see it or do anything. Playground bullying is not tolerated and parents and teachers do everything they can to prevent it, but the internet poses infinitely more complex challenges than a playground.

Getting tough on tech

What to do? Naturally, regulate. In April 2019, the UK government published an Online Harms White Paper to help protect people – especially vulnerable people and children – from online harms. On 12 February, the government published its initial response to a nearly year-long public consultation.

The proposal introduces a new duty of care on companies to monitor harmful content. Services in scope of the regulation will need to ensure that illegal content is removed expeditiously and that the risk of it appearing is minimised. A new regulator, potentially Ofcom, will hold organisations accountable. It will also be able to hold senior managers personally liable for major breaches, and be equipped with audit and fining powers.

Blocking companies' platforms from being accessible in the UK is on the table, but only for the most egregious cases.

Phillip Souta, Head of Public Policy at Clifford Chance said, "The government is clearly trying to strike a balance here – between developing a policy that will place a significant onus on platforms like Facebook, and fostering free expression and making the UK as competitive as possible in the tech and

digital space. They have clearly erred on the later side, citing proportionality to take a so-called iterative approach. This puts the ball in tech companies' courts and gives the government room to do more if they feel that the target companies are dragging their feet."

Being transparent

Companies in scope will have to issue annual transparency reports, both in terms of reporting and moderation practices.

The active requirement to provide these transparency reports will, however, require organisations to proactively monitor that they are being properly implemented. Many in-scope companies already produce content moderation and community guidelines on a voluntary basis. Now these transparency and content guidelines will be held to public and regulatory scrutiny.

Digital and civil rights campaigners warn the plan will have a chilling impact on online speech and privacy. Concerns focus on the monitoring of private communications and application of filtering technologies to comply with very broadly defined concepts of harm.

Some think this will break the internet. The danger that the UK and any government faces is that online turf wars between regulators and global content platforms may not be the most effective way to reduce online harms.

Where does the UK fit in?

Countries around the world are waking up to the problem of online harms.

Governments have a tendency to regulate when they see a problem, and so the UK's contribution to the debate is part of a wider shift in online content rules globally. This is also a classic example of a global challenge that would benefit from international cooperation – like climate change or international tax policy. It is a challenge that could potentially be harmed by a fragmented – and possibly contradictory – approach.

Germany passed the so-called NetzDG law, which allows for social media companies to be fined up to 50 million euros for failing to remove unlawful content, and requires transparent complaints procedures. In 2018, France published a law allowing judges to authorise immediate removal of online disinformation. The operational implications of these laws reflect the possible harm. However, some are concerned about their workability – laws have to be enforceable.

Upcoming EU legislative proposals, if implemented, will require social media platforms to delete extremist content within an hour of being notified of its existence. New EU copyright rules to be implemented in EU countries will require platforms to ensure copyright infringing content is not hosted on their sites. Previous EU legislation only required the platforms to take down such content once they had been made aware of it. Other countries have similar online content regulation, including Australia and Russia.

These wider regulatory shifts have led to requests for the UK to broaden the scope of these content rules to go beyond harmful content, to, for example, fraud and intellectual property.

Have platform holders paid much attention? In short, yes. Andrei Mikes, a content moderation expert at Clifford Chance, said, "A challenge for any regulation is meaningful enforcement. Sceptics argue that cash-rich, large platforms are not triggered into compliance just because of potential fines and investigations. But we have seen that the EU content rules have provoked

platforms to act, including by recruiting additional moderators in countries which have introduced regulation, publishing detailed transparency reports, and updating their community guidelines."

There are important reputational aspects too. "Most platform users want to interact in safe, inclusive environments", says Mikes. "Users really want to trust how platforms maintain high standards on what constitutes valuable speech, which will mean doing more than just paying lip service to the duty of care."

So, post-Brexit, will the UK's emphasis on proportionality be a genuine differentiator for businesses with UK operations?

Dessislava Savova, a Tech partner at Clifford Chance in Paris said, "platforms face the tricky task of complying with new regulations without being excessively cautious or allowing moderators to make snap judgements on what is and isn't unlawful content". The initial response paper is sympathetic to this, which does align with the EU's risk-based approach to regulation.

Regulatory overreach, or necessary intervention?

The discussion remains open. The working assumption for many commentators is that the regulation will apply to all online businesses. The entire internet. Every comment, every like. Journalists too? The UK has confirmed this is not the case. Government research currently suggests only 5% of UK platforms would be covered.

To be in scope, a business would have to operate its own website with functionality that enables the sharing of user generated content, or user interactions (likes, comments, etc.).

Andrew Glover, Chair of the Internet Services Providers' Association has welcomed the targeted approach and emphasis of the UK government's response. "It is important for interventions to be targeted at a specific part of the internet ecosystem."

The recent response confirms that business-to-business platforms are not in scope. Herbert Swaniker, a Tech lawyer at Clifford Chance said, "Whilst the residual impacts of these rules will trickle down to all kinds of companies, their direct bite won't touch most." He adds that, "Frankly, overregulating this area could divert industry from making meaningful changes. Intervention makes sense for the most dangerous spaces, where harm is genuinely likely. The government seem very aware of this."

Radical enough?

The UK is breaking up with its EU partner on the cusp of its golden anniversary. The UK Home Secretary, Priti Patel, said that, "as we leave the EU, we have an incredible opportunity to lead the world in regulatory innovation". So the UK wants to position itself as a policy leader, as also indicated by the UK data protection regulator, the ICO, which just last month published a robust age-appropriate design code.

Jonathan Kewley, Co-Head of Clifford Chance's Tech Group said: "The intent is certainly there post-Brexit to be bold agenda setters, but is this too little, too late? These proposals must address societal and ethical tech risks, which are some of our biggest generational challenges. Whilst welcome, these proposals don't significantly set the UK apart from our European friends."

Irrespective of how the rules are implemented, there is muscle memory among board members who know that ethical moderation and use of content

underpins trust. Compliance should not be a unique selling point. But it is certainly a strong basis for building trust with consumers.

Enough law, more action

Critics say online harms regulation assumes that the offline world is automatically safe. A large survey of young people who had been cyberbullied found that 37% were depressed and 26% had suicidal thoughts, which is higher than for 'offline' bullying – a stark reminder that a single instance of harm can go viral on the internet, hugely amplifying the potential damage.

This chalks the line for regulation to step over. Commentators have pointed out that the UK's existing laws apply to online behaviour and speech, including human rights and anti-discrimination laws. However, the UK body responsible for keeping English law under review and reforming it found that there are some ambiguities and technical issues with existing UK law in this area, with considerable room for reform.

Criminal liability provides a system where individuals and corporations are dealt with after an offence has already been committed, and the damage has been done. Regulation, however, is much more focused on making sure organisations proactively anticipate harm and prevent it from happening in the first place.

Will this break the internet?

Some suggest that the UK's online rules threaten to break the internet, crushing freedom of expression. However, the government confirmed that it recognises how important freedom of expression is not only as a right in itself, or a means to an end – but also as an "essential enabler" of other human rights protected by UK and international law.

If the content is legal, the UK government does not propose to require companies to remove specific pieces. This obviously leaves a grey area as to what content or conduct may be legal, but unethical or arguable (just take, for example, use of closed languages, acronyms and slang within hate groups). Legal content may still cause harm.

In short, the tension between interference versus free speech continues. Leo Rees, a senior consultant at global policy and communications advisory firm, Milltown Partners, said, "It's interesting that DCMS addresses stakeholder concerns around freedom of expression right at the top of its response to the consultation findings." Rees continued, "Perhaps this is a sign that the new government is acknowledging the characterisation of the debate put forward by some of the tech sector – that overly onerous definitions of harm could inadvertently jeopardise free speech."

Who will enforce this?

The original White Paper was silent on who would take on responsibility for enforcing the new rules. The UK government has confirmed that the UK's communications watchdog, Ofcom, is preferred. This is unsurprising, given Ofcom's relationships with major players in the online area, and the UK government has itself identified this as a driver for the recommendation.

The statistics from the response paper suggest that the majority of stakeholders were not particularly concerned about who took on this role, but questions did arise on cost and resourcing.

This is where the effectiveness of the regulation could stand or fall. Ofcom has obligations to enforce media and telecoms regulation in the UK, and online harm filters into many areas. A cooperation mechanism with other authorities – particularly those focused on data, competition and consumer protection – will help balance the scales. It is to be seen how this will be handled.

What's next?

The most recent response deferred substantive commentary on some of the most controversial aspects of the White Paper, including whether senior managers will be held liable for breaches of the proposed statutory duty of care. The government confirmed that it is considering the consultation responses on this and will set out its final policy position this spring.

The response paper confirms that the government is working with law enforcement and other bodies to present interim codes of practice. These will focus on harms where there is a risk to national security or child safety.

For now, the government expects companies to take immediate action to tackle harmful content or activity on their services.

The challenge for organisations is whether they can do enough to satisfy governments, because it is ultimately governments who have the power to regulate, and impose criminal liability for corporations and individuals – it is that threat that governments are relying on to force companies to do better in this space. Either the companies will do enough and the government response will be light-touch, or they will not; there will be more scandals, and the government responses will be very tough indeed.

CONTACTS

Herbert Swaniker
Lawyer, London

T +44 207006 6215
E herbert.swaniker
@cliffordchance.com

Andrei Mikes
Lawyer, Amsterdam

T +31 20 711 9507
E andrei.mikes
@cliffordchance.com

Phillip Souta
Head of UK Public Policy

T +44 207006 1097
E phillip.souta
@cliffordchance.com

Dessislava Savova
Partner, Paris

T +33 1 4405 5483
E dessislava.savova
@cliffordchance.com

Jonathan Kewley
Partner, London

T +44 207006 3629
E jonathan.kewley
@cliffordchance.com

Midori Takenaka
Lawyer, London

T +44 207006 1593
E midori.takenaka
@cliffordchance.com

Gail Orton
Head of EU Public Policy

T +33 1 4405 2429
E gail.orton
@cliffordchance.com

Samantha Ward
Partner

T +44 207006 8546
E samantha.ward
@cliffordchance.com