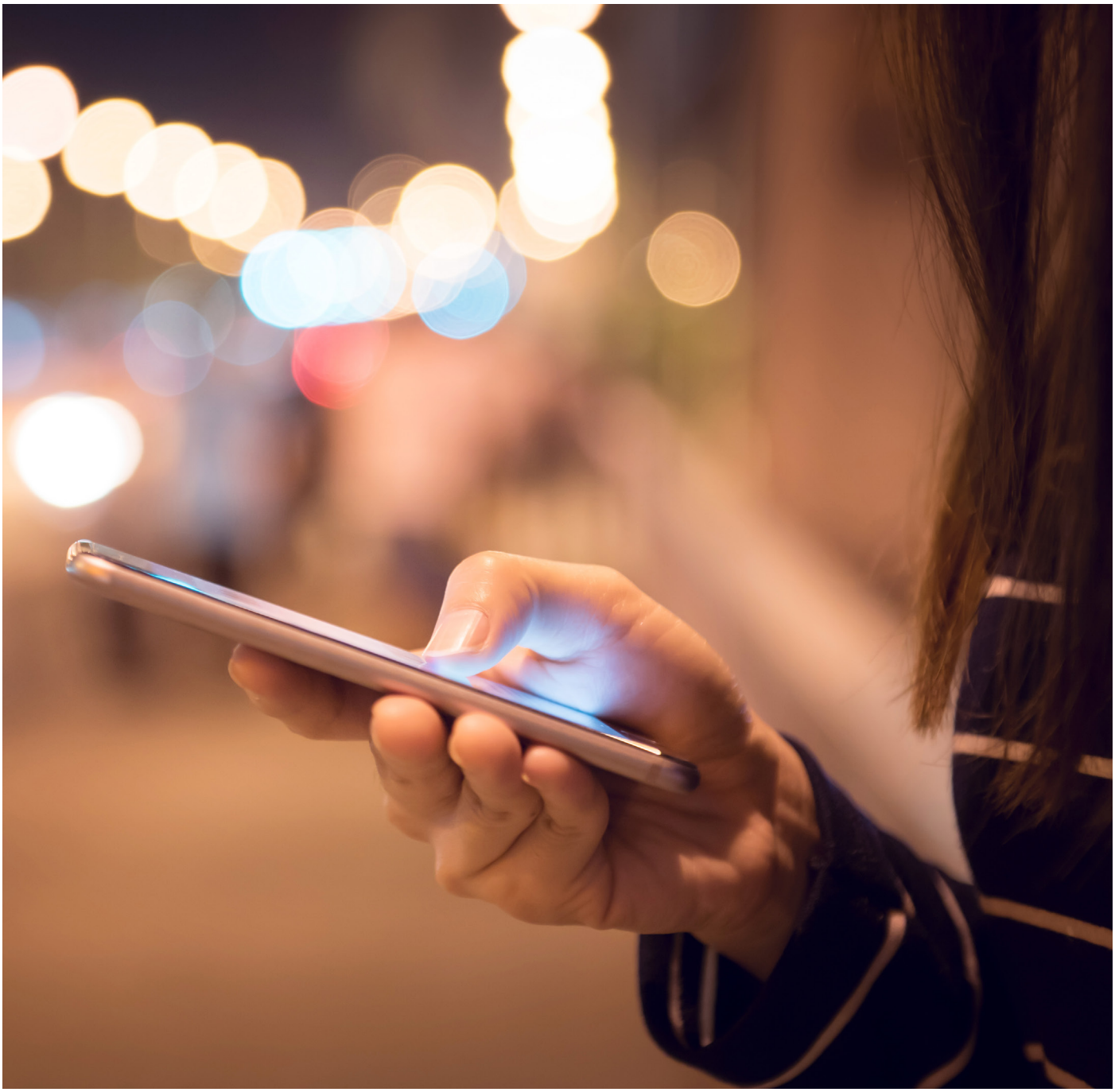
techUK

Tackling Online Harms

Principles that should underpin smart policy and practice



Background

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow More than 900 companies are members of techUK. Collectively they employ approximately 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium-sized businesses.

Introduction

This year the World Wide Web turns thirty. Over the last three decades the web and the internet have enabled profound change, bringing huge benefits to people and societies around the globe. But that rapid change has also inevitably brought with it new and unpredictable challenges. The need to understand how we can maximise the benefits of new technology whilst minimising risks and harms has become more urgent as digital technologies have become more present in our lives. To achieve the promise that existing and future technologies hold we have to mitigate against the unintended consequences or risks of deliberate misuse that can harm individuals and undermine societies. This means innovating with safety, security and privacy in mind – something that industry is already alive to and active on.

techUK believes that this work should be underpinned by a clear understanding of the problems to be addressed. The policy-making process should also be guided by a consensus amongst stakeholders, a recognition of the wider issues that are involved, a strong evidence base and a principles-based approach that ensures smart and timely action to address issues that government acknowledges are fast-changing and complex.

There is an ever-increasing volume of literature from think-tanks, regulators and third-sector organisations on the subject of online harms. Most notably Ofcom's discussion paper: Addressing harmful online content; doteveryone's Regulating for Responsible Technology; and, the wide-ranging paper from the Institute for Global Change calling for A New Deal for Big Tech. techUK has reviewed all of these contributions and this paper reflects on some of the ideas they put forward for discussion.

This contribution looks at what is currently being done to address some known harms. It then sets out principles that must underpin any additional action coordinated by Government in order to ensure that it is both effective and meets the Government's twin goals of making the UK the best place to start and scale digital companies and making the UK the safest place to be online. Finally, this paper sets out a number of guiding principles to inform new public policy and practice, recognising that any new framework must be flexible, agile and respectful to the diversity of the sector.

Online Harms – a constantly evolving landscape

We live in an era where digital technologies underpin almost every aspect of our lives. From the jobs we do and the way we keep in touch with family and friends to the way in which our society and economy functions. These digital technologies are driving rapid change and bringing positive benefits to people's lives.

It is misleading to suggest that these technologies and services operate in a 'Wild West' beyond the general law and without governing norms or rules. As well as being governed by the general law and legal principles that apply in the 'offline' world, over time further frameworks, guidance and self-regulation and technical standards have been developed to support the digital economy to work effectively and securely. The tech industry recognises that good regulation and standards can be, and are, effective enablers of innovation and commerce. But if Government is minded to introduce new legislation or regulation this must be proportionate and necessary, and align with other government objectives for innovation and growth in the UK digital sector.

From the very early days of the world wide web, digital businesses have been actively engaged in seeking to address the misuse of technology. In 1996, for example, the predecessor of the Internet Watch Foundation – the Safety Net Foundation - was formed to tackle child sexual abuse content online. Numerous industry initiatives and international partnerships - as well as new legislation and regulation at both a national and EU-level where needed - have built on this foundation to address new challenges.

But as technology changes so do the challenges and nature of harms and there is clearly a need for policy and practice to evolve to ensure appropriate protections are in place to safeguard individuals and the values that we hold important.

There is consensus that policy must achieve the right environment for continued growth and innovation as well as address the online harms where they exist. Government has committed to these two goals in the Government's Digital Charter - to make the UK the best place to start and scale digital companies and to make the UK the safest place to be online.

Spectrum of Online Harms

As in the offline world, there is a broad spectrum of online harms that range from the illegal to the harmful but not illegal. There are also variations in the prevalence and impact of harms on different platforms and services. It is important that government effectively maps the harms and where they occur before affirming government policy to address them. techUK is pleased that research in underway to do this.

A guiding principle should be that Government intervention or regulation must only be considered where it can deliver better outcomes than existing initiatives at national and international levels.

As a starting point, there is a need for clear definitions of the harms and recognition that these harms will require different policy responses. techUK has consistently called for this. Only when stakeholders have a shared understanding can they collectively debate what additional actions and interventions may be required. Such measures must be proportionate and effective and deliver better outcomes than what is already in place at national or international level.

In their recent report on Addressing Harmful Content Online Ofcom published their taxonomy of harms:

- **illegal content** – such as hate speech, child exploitation or incitement to terrorism.
- **age-inappropriate content** – such as adult sexual material, disturbing or violent content.
- **other potentially dangerous content** – which poses a significant risk of personal harm, such as videos or images promoting self-harm or violence.
- **misleading content** – including 'fake news', the use of fake accounts and misleading political advertising, which may have undue influence on the democratic process.
- **personal conduct that is illegal or harmful** – such as bullying, grooming and harassment.

This is a useful starting point for thinking about these issues; however, their taxonomy quickly runs into obstacles. For example, personal conduct can be both illegal and/or harmful based largely on context. Each harm is very different – some harms are illegal whilst others sit in the 'harmful but not illegal' category. Moreover, some "harms" will be more harmful to specific groups whether due to age or other criteria.

A company's response, aside from technical capability and resource, is determined by how confident they are in knowing where on the spectrum a harm sits. A harm that is clearly illegal can be tackled with very little constraint, as harms move across the spectrum – towards harmful based on context/target, legal uncertainty increases thereby making it more challenging for a company to act quickly and authoritatively.

techUK believes there is more work to be done to understand this spectrum and act as a solid basis for precise responses that are set within a clear and understandable policy framework.

Guiding principles

The UK tech sector has a long history of effective self and co-regulation. The creation of the Internet Watch Foundation and the UK Council on Internet Safety are just two examples of where the sector has led in self-regulation, working together to improve internet safety and tackle some of the harms found online.

However, there is a constant need to respond and adapt to evidence of online harms as it emerges and techUK believes that those actions should be underpinned by five key principles.

1. Acknowledge the differences between online services

From its size or demographics to the service it provides and the different challenges and harms that present themselves, every platform is unique. Any new system must acknowledge this uniqueness and ensure that policy proposals are proportionate both to the likelihood of the specific harm on the platform, but also the nature of the service and its user base. For example, whether it is targeted at the professional community (e.g LinkedIn), specific communities (e.g. Mumsnet), or young people (e.g. the student room).

Size is of particular relevance. There are significant differences in the capabilities that companies have to address online harms. For example, the very largest players may be able to develop and deploy AI-based solutions that smaller firms do not have the capability or capacity to develop. There is a clear role for shared and open-source technology across platforms.

The limits of technology are also important. Technical tools do exist; however, the technology is nascent for many of the harms being discussed here because the assessment of harm or legality is language-based and context-specific. Each platform's specific characteristics will mean these tools would need to be significantly adapted etc. Moreover, many of the tools already available, for example PhotoDNA (that aids in finding and removing known images of child exploitation), still require a human element. Smaller companies may need time to develop the resources or skills to service this requirement. Therefore, any new approach must have proportionality built-in, allowing companies to act according to their capabilities and stage of development whilst incentivising the transfer of knowledge and capability between companies to help the diffusion of good and workable technology solutions.

techUK recommends a principles-led approach that acknowledges the diversity of the platforms in operation and accounts for the differences in size and therefore resources. We welcome government's acknowledgement that a one-size fits all, inflexible solution is unlikely to be effective.

2. Acknowledge and act based on a robust evidence base

Most online harms are the result of the actions taken by the users of an online platform. Therefore, action in this space has a direct relationship with individual rights.

Government has a dual duty to both protect citizens and safeguard their rights. These foundational legal principles require policy to be carefully considered and aligned with the general law and international commitments the UK has made. Parliament, rather than a government agency or regulator, should deliberate and decide on how these norms should be upheld and with their continued oversight.

Government must avoid erroneously regulating by anecdote and calling for action based on our mere perception of a harm. Policy must be informed by a comprehensive evidence base for different harms, to identify what is an appropriate response varies depending on the harm's nature, prevalence and cause.

For example, while there is much discussion about the dangers related to the total amount of screen time on physical and mental health of young people, the evidence base is incomplete, with some research finding it to be beneficial. This is why efforts should be focused on issues where there is the strongest evidence for their harm against individuals and their society and reflect their prevalence on platforms. techUK welcomes new evidence informing this debate, for example the recent guidelines published by the Royal College of Paediatrics and Child Health (RCPCH) to help parents decide what works best for their family and their children with regards to screen time.

Over time unforeseen harms will emerge, as seen with the issue disinformation following the 2016 US Presidential election. It is vital that a new regulatory system acts solely on the base of evidence in this regard and does not seek to develop new policy or propose new requirements for industry based on anecdote alone.

This is not to say that industry practice cannot evolve in the interim. A strong evidence base also informs company innovation.

techUK welcomes the recently commissioned research and recommends that the Government commissions further research to build an evidence base of harms to ensure that policy interventions are targeted in the most appropriate manner. The Internet Safety Strategy Green Paper response made a number of commitments with regards to gathering evidence from experts, techUK hopes this evidence is both published and used to inform the White Paper.

3. Retain liability limitations

techUK welcomes the Government's commitment to safeguarding fundamental freedoms and ensuring incentives to innovate and invest are preserved. The White Paper must build on these commitments.

Moreover, the debate around limitations to liability with regard to content regulation often fails to recognise that this is a widely adopted legal principle, not exclusive to the online world. Yet, in no other sector has there been a discussion about modifying limitations to liability, such as in banking to address fraud in the system.

Undermining or weakening limitations liability would serve to chill existing innovation and would distort incentives in the operation of open platforms which have hitherto driven significant economic growth.

There has been debate as part of the online harms discussion about whether policy in this area should adopt principles of traditional regulation, such as broadcasting regulation, in this regard. There is wide agreement within the industry that such frameworks are not scalable or appropriate for the open architecture of the internet and the platform model. A different approach is needed which acknowledges that limitations to liability is foundational to the internet and the base on which to build policy and practice for managing online harms and content and for meeting the dual goals of the Digital Charter and government's commitment to safeguard users' wider rights.

techUK recommends that government retain the current framework for limitations to liability, and build upon it by consulting on further policy and practice which can enhance efforts to combat specific harms. As the Government examines what improvements can be made it must be alive to the unintended consequences these changes could have on the wider digital economy and in other sectors or areas of Government policy.

4. Provide clear legal definitions and boundaries

Companies find it useful to understand what are effective and fair practices and techUK welcome the Government's intention for the Online Harms White Paper to provide a framework to help build an environment that encourages company and industry efforts to this end.

The Law Commission's recent report into abusive and offensive online communications highlighted these issues further. In particular, the Law Commission concluded that online crime was sometimes criminalised to even a greater degree than equivalent offline offending, and that ambiguous terms such as "gross offensiveness" "obscenity" and "indecency" don't provide the required clarity. Moreover, it spotlighted the "endemic challenges" posed in policing this space listing issues of jurisdiction; accessing evidence; technical and resource capabilities etc.

Layering new expectations on subjective or unclear definitions provides no legal certainty and inappropriately increases liability for third party content and conduct. It is important any new system presents narrow legal definitions and boundaries for companies, enabling them to act as consistently and clearly as possible.

techUK recommends that government should consider the findings of the Law Commission review and ensure legal clarity and unambiguous legal definitions is a guiding principle of the White Paper.

5. Reflecting on the global nature of the internet

When looking at how to tackle online harms it is important to bear in mind the global nature of the internet and open platforms. Countries of all hues across the globe are grappling with these issues.

If the UK were to endorse new policies and practices which would expect companies to treat harmful content in the same way as illegal content, we must consider how these actions could be interpreted by other countries. It is crucial that interactions between government agencies and companies are supported by appropriate safeguards which protect rights and respect for the general law. It is such safeguards that would make UK government policy worthy of emulation overseas and avoid the inappropriate copying of heavy handed approaches as we have seen with the NetzDG for example.

It should be a guiding principle of the White Paper to **develop government policy which stands up to external scrutiny and meets the highest international standards of transparency and accountability and maintains an open an innovative environment that promotes freedom of expression.**

6. Recognising the pace of technological change and the limits of policy interventions

Government policy must take note of the rapid pace of technological changes and look to the future. Policy-making must avoid looking back and drawing on analogue approaches and look broader to novel approaches, both domestic and international.

New technologies can help us tackle many of the harms this paper explores, however government policy must also prepare for new challenges. We are already beginning to see the emergence of distributed and federated platforms like Mastodon which have been used to disseminate illegal content. Moreover, as mature companies improve techniques to discover and remove illegal content undoubtedly this content will migrate to other platforms that could be harder to intervene on, as we have already seen with the drugs and weapon trade moving on to the dark net.

Regulation becomes significantly more challenging when dealing with bad actors who use technology to act illegally and are operating in hard to reach online spaces that are, for example, no longer hosted by a single company and control is distributed.

Government should recognise these challenges coming down the line and anticipate the need to develop new and inventive operational methods to identify and disrupt illegal activity.

techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow.

Over 900 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups.

The majority of our members are small and medium sized businesses.

techUK.org | @techUK | #techUK