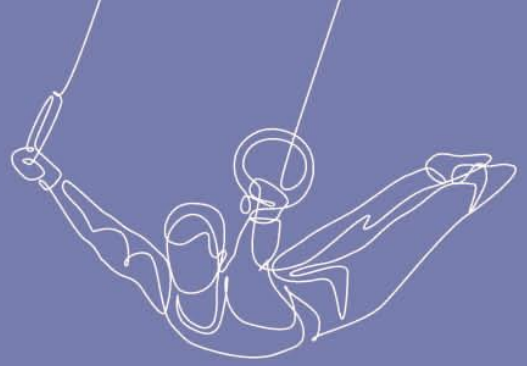
ALARM
embrace risk

THE BALANCING ACT



ALARM CONFERENCE 2021

@alarmrisk alarmrisk.com

ZURICH Municipal

PLATINUM SPONSOR

ALARM
embrace risk

ALARM CONFERENCE 2021

@alarmrisk alarmrisk.com

Platinum sponsors

ZURICH Municipal

Gold sponsors

AON Empower Results®

Kennedys

Maven Public Sector

rmp

Silver sponsors

BLM

dwf

forbessolicitors.

Gallagher

PLEXUS

Bronze sponsors

brownejacobson LLP

DAC BEACHCROFT

PROTECTOR insurance

sedgwick

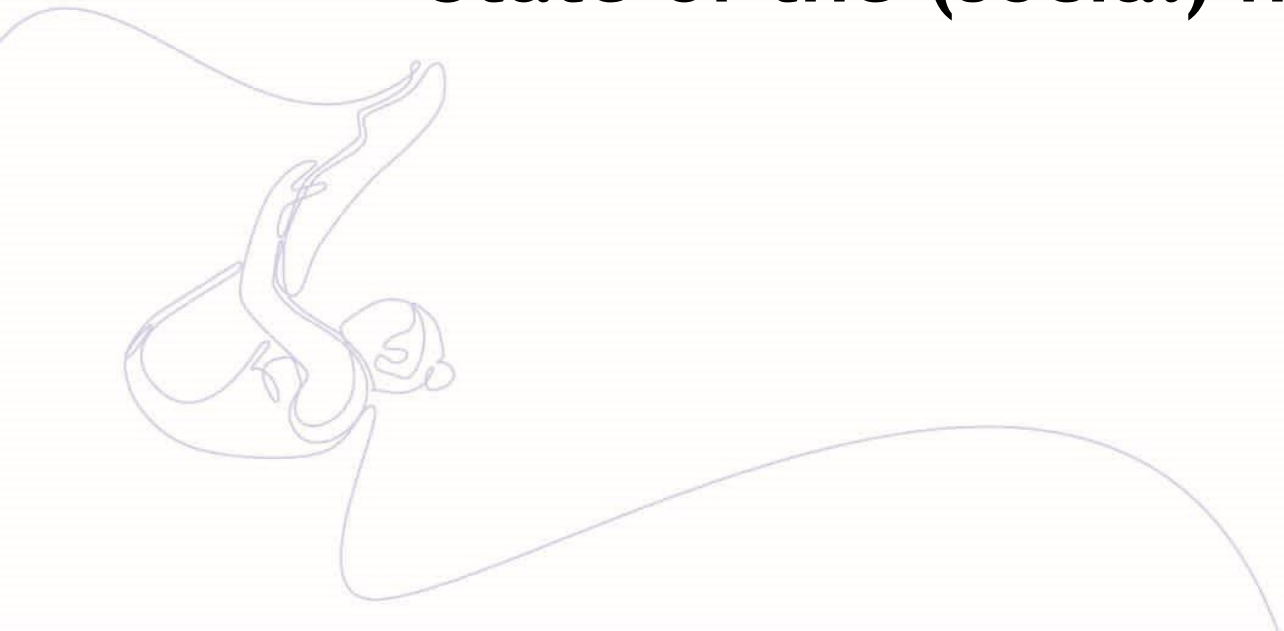
TRAVELERS

THE SOCIAL DILEMMA – ONLINE HARMS AND THE FUTURE OF ONLINE RISK

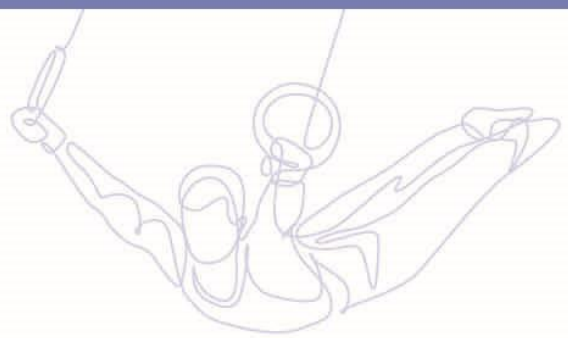
Steve Kuncewicz, Head of Creative, Digital & Marketing

BLM

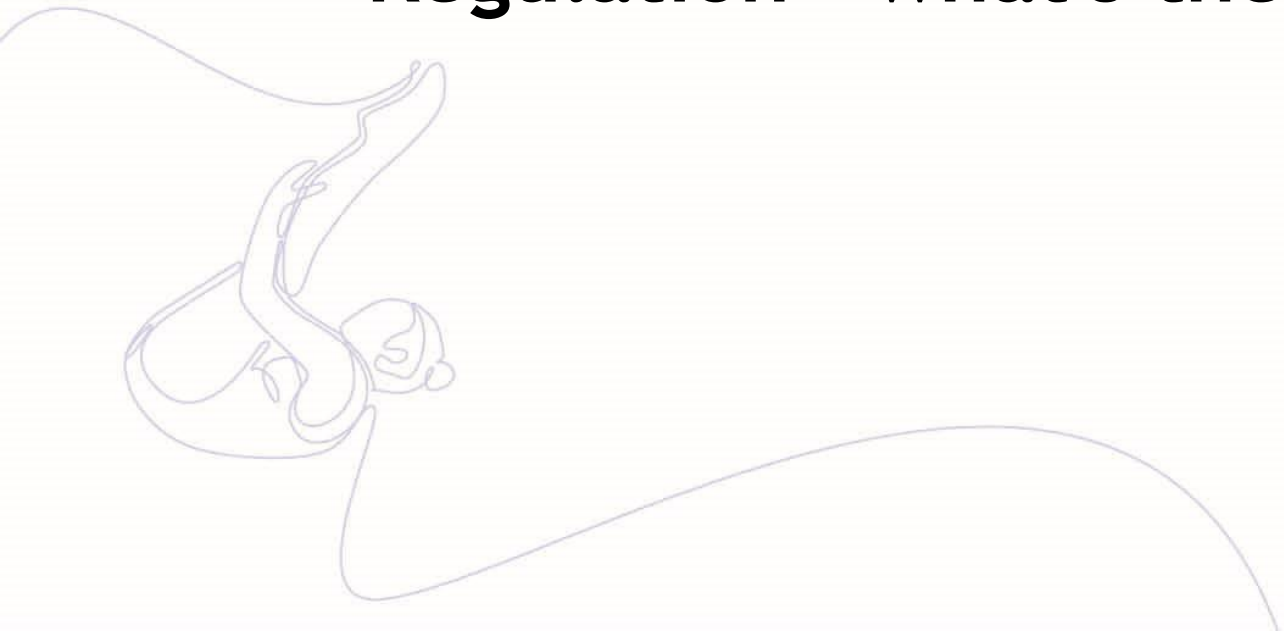
State of the (social) nation



- Digital 2021 Report – 10/2/21 (Hootsuite, WeAreSocial & Kepios)
- UK Population as of January 2021 – 68.05 million
- Internet users in the UK - 65.32 million, or 96% penetration
- Social media users in the UK – 53.00 million, or 77.9 penetration (growth of 2.3m, or 4%)
- Mobile connections in the UK – 67.61 million, or 99.4% of total population (potentially more, as many people may have more than one, but figures show 3.6% decrease)
- Social media adoption surging globally – 13% increase to 4.2 billion users by January 2021
- 1.3 million users join social media every day during 2020, or 15.5 per second
- The average social media user spends 2 hours 25 minutes on social media every day, or roughly one day each week
- Average time spent using mobile devices each day – 4 hours 10 minutes, with 44% spent in social & communications apps, 26% in video & entertainment apps, 9% gaming & 21% "other"
- Mobile phones now account for a greater amount of people's time than live TV
- But, daily time spent using the internet across all devices – 6 hours 45 minutes, with a total of 3 hours 24 minutes spent on social media
- Platform "League" – 1: Facebook, 2 – YouTube, 3 – WhatsApp, 4 – FB Messenger, 5 – Instagram, 7 – TikTok, 16 - Twitter



Regulation - what's the harm?



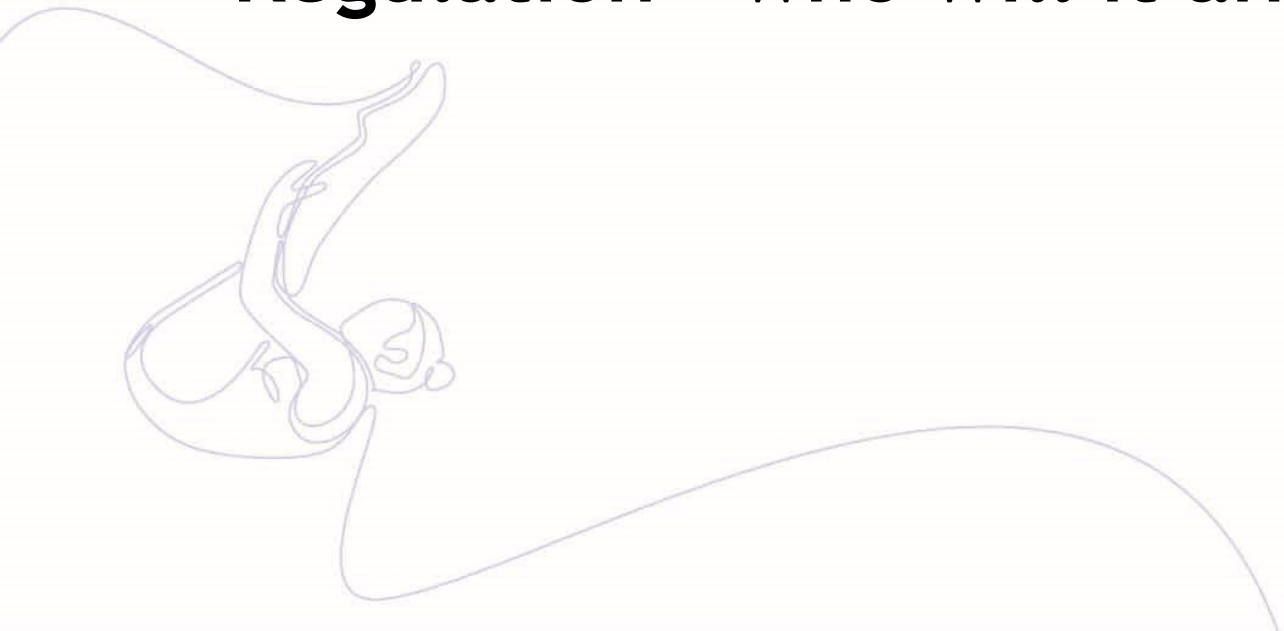
- Online harms white paper launched in April 2019 aiming to create a culture of "transparency, trust and accountability" – responsibility, rather than liability
- New legislation will make companies responsible for their users' safety online, especially children and other vulnerable groups and for tackling Harm caused by content or activity on their services
- Compliance with a new statutory duty of care will be overseen and enforced by an independent regulator
- Consultation closed on 1st July 2019 , with interim response to white paper published in February 2020 noting concerns raised re: freedom of expression (although noting that the new regime doesn't require removal of content, but to introduce appropriate safeguards against harms)
- Much of the work was anticipated to be done through revised platform user terms
- Concern over businesses in scope also addressed, with confirmation that duty of care will only apply to businesses facilitating sharing of UGC; Businesses with a social media presence not necessarily caught
- Regulatory burden on small businesses would be "minimised" – 5% of UK businesses to fall within scope on original estimates?

- December 15, 2020 – "Final Outcome" published by DCMS
- OFCOM to be new online harms regulator (with recruitment underway), funded by regulatory fees payable by companies above a set global annual revenue threshold
- Intention – to prevent proliferation of illegal content & activity online, with emphasis upon protecting children from being exposed to harmful content
- Disinformation & misinformation which could cause harm to individuals will remain in scope
- Systems & processes to improve user safety required, although revised figures suggested less than 3% of UK businesses will fall within scope (and many who are being exempt from regulatory fees)
- Focus on regulating companies where the "risk of harm" is greatest
- Technology will play "crucial role" in improving user safety
- "Proportionate" enforcement through fines of up to £18 million of 10% of global annual turnover, whichever is higher
- Further detail on "business disruption measures" and introduction of criminal sanctions against senior managers who fail to comply with information requests

- Duty of care intended to hold tech giants to account based on a set of guiding principles
- Different levels of expectation dependent upon whether services used by adults or children
- "Tiered" approach – "category 2" will need to take proportionate steps to deal with illegal content and protect children, and "category 1" will include "high-reach" services expected to do more
- New rules will apply to public communication platforms where users expect more privacy (mainly social media platforms)
- Any business in scope will need to consider and explain any impact of measures upon individual privacy
- OFCOM will be empowered to require platforms to use tech to identify CSE, abuse and terrorist content (subject to safeguards)
- Codes of practice will fill in "gaps", and must be complied with or effective alternative approaches identified - interim codes on CSE, abuse & terrorist content already published
- Mechanisms for user reporting of harmful content or activity will need to be established or prioritised, along with appeal procedures
- Online Safety Bill may also implement law commission recommendations on communications offences once published
- 2021 Queen's Speech (11 May): "*My Government will lead the way in ensuring internet safety for all, especially for children [Draft Online Safety Bill] whilst harnessing the benefits of a free, open and secure internet.*"

- Online Safety Bill – published on 12 May 2021
- To be reviewed by a joint committee of MPs (TBC) before formal introduction to Parliament later in 2021
- Evidence to be taken and reported back upon, with non-binding recommendations to follow
- Businesses can submit evidence and lobby – and they will
- Time to start looking at the OSB's content in more detail and think about compliance
- Focus remains on underpinning processes and procedures (like GDPR) rather than removal of specific pieces of content
- OFCOM codes of practice will set out principles, and businesses in scope will be expected to comply or explain why they haven't
- Any departure will need to be based upon "online safety objectives"
- OFCOM will have significant role in developing the new regime and equally significant enforcement powers
- Online Safety is here to stay, and this represents significant intervention based on public support for platform regulation
- But – who's in scope, and what's expected of them?

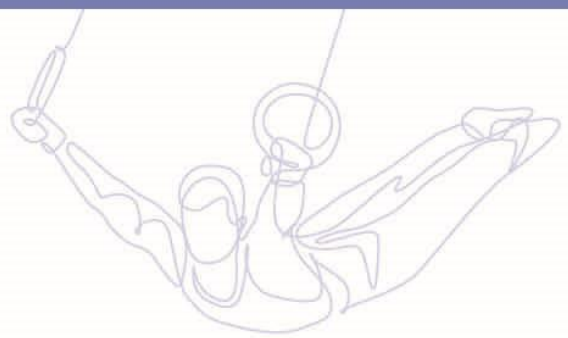
Regulation - who will it affect & how?



- Providers of “user-to-user” and “search services”
- “User-to-user services” – Allow users to share, generate or upload content online which other users can “encounter” online through the service’s functionality
- “Search services” – Search engines (or services which include them)
- “User-to-user” is an especially broad church – e.g. Social media platforms, online marketplaces, dating apps, review sites, forums
- “Functionality” has a particularly wide definition
- Not just about services which allow for wider dissemination of content; those providing means for direct and private interactions between users also in scope
- Extraterritorial Scope – like GDPR, applies to services with “links” to the UK, a significant number of UK users, which actively targets the UK market or capable of use in the UK
- Key issue – does the service give rise to “material risk” of “significant harm” to individuals in UK
- Additional duties imposed on “category 1” user-to-user services meeting stated thresholds in relation to otherwise legal content which can still be harmful to adults, including where of “democratic importance” or “journalistic content”
- Thresholds to be set out in further regulations made by secretary of state in due course, based on size of user base and relevant functionality
- “Illegal” content relates to criminal offences – content which may give rise to a civil claim is excluded from the Bill’s scope
- Most businesses in scope will fall within category 2, based on perceived risk?

- Advertising content largely already subject to self-regulatory codes across social media, but regulation of online advertising market to be reviewed in "first half" of 2021
- CMA already taking a more active role re: Influencers (emphasis on transparency and paid content being identifiable), and many have caused for more action on "scams"
- ASA has been active throughout the COVID-19 pandemic, but CMA may become more interventionist based on existing CPUTR?
- Duty of care – content or activity which givers rise to a "reasonably foreseeable" risk of harm to individuals and has a "significant impact" on users or others
- "Limited number" of "priority categories" to be set out in secondary legislation (original list of "harms" included sexting, child sex abuse, underage access to pornography, revenge pornography, hate crimes, harassment, sale of illegal goods, cyber-bullying, trolling, fake news and disinformation and content that advocates self-harm and suicide)
- New legislation won't change existing liability for individual pieces of content meeting the definition of "harm", but it will require an understanding of the risk & new policies & procedures
- Additional provisions re: disinformation and misinformation, based on activity of "expert working group" to build consensus partly based on the COVID-19 pandemic
- No "one size fits all" approach to compliance, although all businesses will be expected to take action in relation to relevant content and activity

- Emphasis on businesses assessing likelihood of children accessing their services and if so, additional protections must be introduced;
- Far higher burden on very limited number of "category 1" services, mainly intended to address expectation gap between stated safety policies and actual user experience
- Original range of "harms" was dynamic and wide-ranging, leading to some concern amongst respondents to White Paper
- Legislation will define scope as covering reasonably foreseeable risk of "significant adverse physical or psychological impact" on individuals
- IP infringement, data protection compliance, fraud, consumer protection breaches and cybersecurity/hacking breaches will be excluded from scope
- Online fraud "best tackled through other mechanisms", but increasing pressure from which, MSE and others
- Duty of care has been "refined" and split into two parts – duty on businesses and upon OFCOM as the new regulator
- Risk-based compliance will depend upon risk of harm occurring, profile & demographics of users and market share/size of business
- The new legislation won't "eliminate" harms in scope, but should improve user safety
- User reporting and redress at the heart of the new approach
- No new avenues for individuals to sue companies, but legal action should be more accessible to users as the evidence base grows and regulatory rulings can be used in support of claims



Regulation – what's expected of "services"?

- Different duties between user-to-user and search services, notably if in “Category 1”

All User-To-User Services must:

- Identify & assess risks arising from illegal content and legal content, notably which may be harmful to children (if likely to be used by children)
- Mitigate identified risks and put in place proportionate systems and processes to minimise presence of illegal content and remove when notified
- Take into account freedom of expression & privacy when designing and implementing new user safety policies & procedures
- Make TOU accessible, apply them consistently and emphasise how users are protected
- Establish effective user reporting mechanisms in relation to illegal or harmful content
- Ensure effective, easy to use and transparent complaints procedures for users

Category 1 Services must:

- Assess & mitigate risk of legal content which may be otherwise harmful to adults;
- Bear in mind importance of “content of democratic importance” and “journalistic content” when making decisions on users sharing it and deciding how to take action against those doing so, restricting access or taking it down – “diversity of political opinion” must be treated equally
- Set up dedicated, expedited complaints process re: democratic & journalistic content

Search services must:

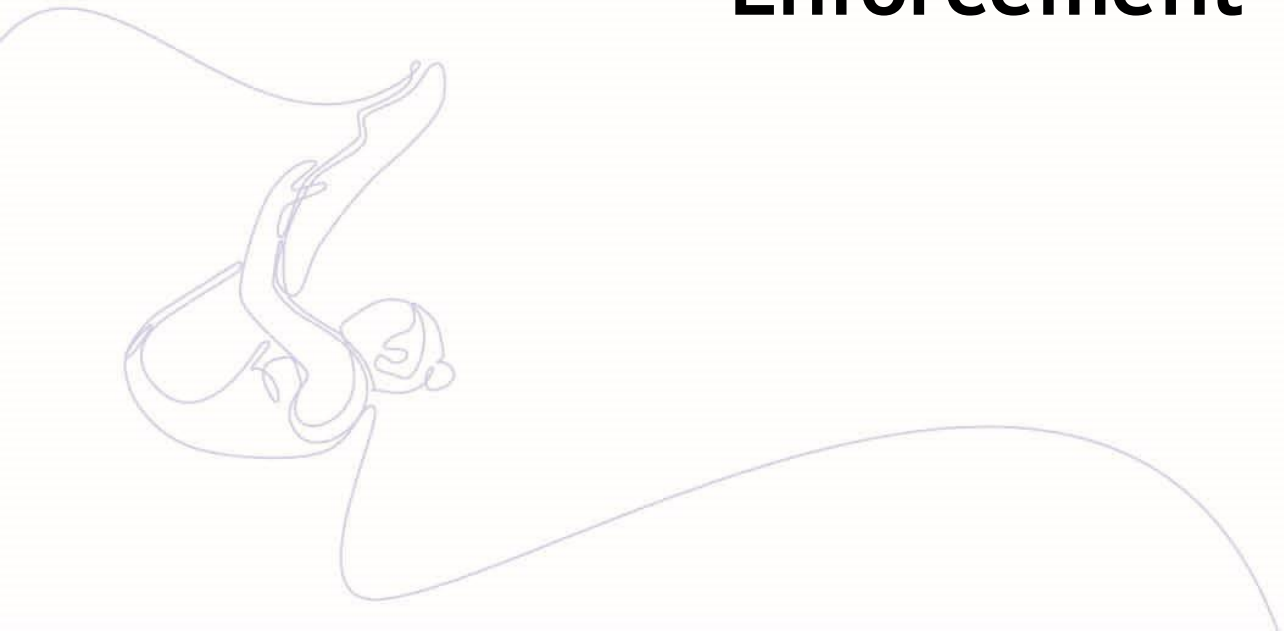
- Comply with user-to-user requirements, but also comply with other duties where their services are likely to be accessed by children to address content potentially "harmful" to them

Various "safety duties" referred to:

- Illegal content on user-to-user services – Proportionate steps to mitigate & effectively manage risks of harms to individuals as identified in most recent "illegal content risk assessment"
- Minimise presence of "priority illegal content", time of availability and extent of dissemination
- "Swiftly" remove such content when notified or made aware
- All to be explained via TOU, which must be clear and accessible and consistently applied
- Freedom of expression – rights of users to FOE within the law to be taken into account, along with unwarranted infringement of privacy when implementing safety policies & procedures
- Category 1 Services to carry out relevant, continually-updated and published impact assessments of policies & procedures on FOE

- Content of democratic importance in Cat. 1 services – must be "protected", along with diversity of opinion
- In scope: content published by news publishers or otherwise regulated and "specifically intended to contribute to democratic political debate in UK (or a region)
- Journalistic content in Cat. 1 services – Protected in similar manner – regardless of whether from "citizen" or "professional" journos, provided that it's generated for purposes of journalism and directed towards UK users in significant number likely to be interested in it
- "Category 1" is clearly aimed at large-scale UGC platforms (Facebook. Google, etc), but confirmation of where businesses in scope fall expected via a register after royal assent
- General duty of care to deter illegal and "harmful" content, but no specific definition of that is actually "harmful"
- Content which has a material risk or adverse physical or psychological impact on child or adult of "ordinary sensibilities", taking into account how many users likely to be exposed to it and how quickly it can be shared
- No reference to financial impact as part of "harm", hence objections over exclusion of "scams" from scope
- "Balancing act" in relation to democratic and journalistic content – dedicated complaints procedures to be introduced for each

Enforcement



- Specific codes of practice already re: illegal terrorist content, CSE & abuse
- Others expect from OFCOM in due course to deal with various other duties of services in scope

"Online safety objectives" are the basis for them, and they refer to:

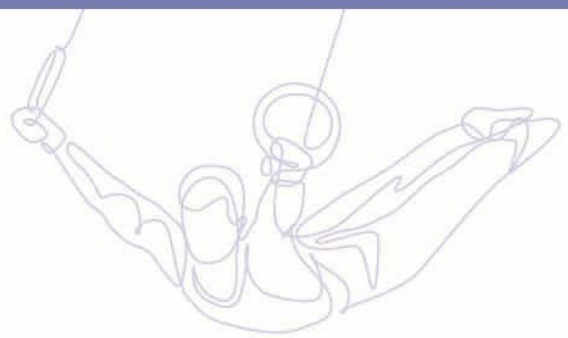
- Effective & proportionate compliance and risk management which are understandable to users, with specific and higher standards to protect children
- Adequate control over access to services by adults & children
- Use of algorithms, functionality and features of services to protect users from harm
- Again, different expectations of user-to-user and search services

Sanctions available:

- Notice of non-compliance
- Financial penalties up to £18 million or 10% of global turnover
- "Business disruption measures" based on court orders including restrictions of available functionality (including payment services) and blocking in their entirety
- Potential criminal liability of Senior Managers for failure to comply with information services, to be introduced at least 2 years after new regime comes into effect

- Codes of practice produced by OFCOM will focus on systems, processes and governance required for compliance, rather than categories of harm
- Initial "gap-bridging" codes already in place, and any new codes will be subject to wide-ranging consultation to capture existing expertise, as well as parliamentary oversight
- Use of automated technology to reduce harms will only be mandated where there's no other alternative method, but CSE content through private channels will be an early focus, alongside terrorism
- No further requirements re: reporting of criminal activity or retention of related data, but this will be dealt with through separate legislation
- *"Where disinformation and misinformation presents a significant threat to public safety, public health or national security, the regulator will have the power to act"*
- Disinformation can be "legal but harmful", and User terms will be expected to emphasise this issue
- OFCOM chosen on the basis that the new regime works to "empower an existing regulatory body" and its role in the AVMS Regulations relating to online video content, as well as a "strong track record of engagement"
- "Logical extension of existing remit" based on experience in broadcasting remit

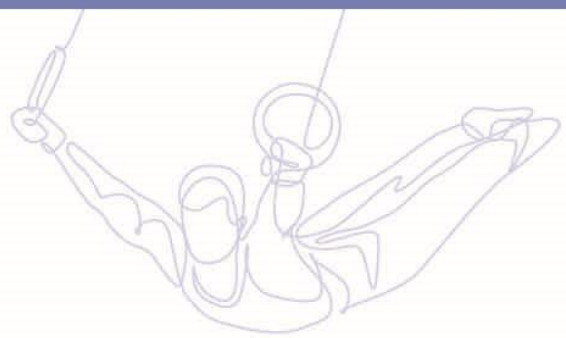
- OFCOM's primary objective will be "to improve safety for users of online services"
- Complaints from users will be accepted, alongside "super-complaints" based on systemic issues affecting large numbers of people
- Codes of practice will set out what businesses need to do to comply with the duty of case, alongside a transparency, trust & accountability framework
- Enforcement will be "prompt and effective", but also "appropriate and proportionate"
- Start-Ups & SMEs will be "supported"
- *"The government recognises the need to balance effective enforcement with protecting the attractiveness of the UK as a tech sector, and also with users' rights. The regulator will strongly encourage compliance with the regime in the first instance and provide clear grounds for any intervention and escalation."*
- Any action against Senior Managers will be a "last resort", and not introduced for at least two years after introduction of legislative framework
- Appeals system will allow for enforcement decisions to be referred to an "appropriate tribunal" based on judicial review procedures or to the High Court through JR proceedings
- International collaboration on online safety will continue, regardless of new UK approach
- Online safety is a "shared responsibility between government, users and companies"
- "Joined-up" approach with ICO & CMA through new "Digital Regulation Co-Operation Forum"



Regulation – will it work?

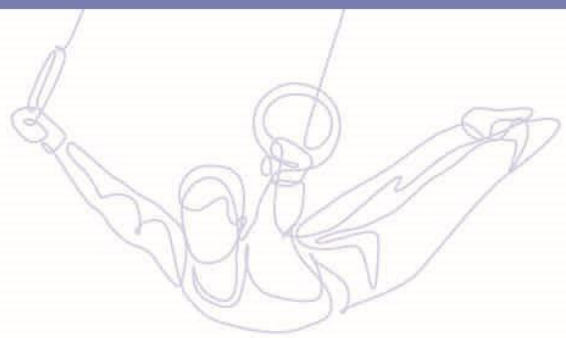
- **Guiding principles (from final response)**
- Improving user safety: taking a risk-based approach that considers harm to individuals
- Protecting children: requiring higher levels of protection for services used by children
- Transparency and accountability: increasing user awareness about incidence of and response to harms
- Pro innovation: supporting innovation and reducing the burden on business
- Proportionality: acting in proportion to the severity of harm and resources available
- Protection of users' rights online: including freedom of expression and right to privacy
- Systems and processes: taking a system and processes approach rather than focusing on individual pieces of content

- Raised awareness of the “online harms” issue has moved it up many businesses’ risk registers
- UK GDPR a useful precedent in terms of training, management and the appointment of a “Harm Officer”
- Conversely, application and enforcement in practice is not currently well-defined and difficult to pin down
- Like cybersecurity, practical yardsticks for minimum best practice will take time to develop and formulate
- How will it be technically enforceable against businesses outside the UK whose content will remain accessible to those whom the legislation seeks to protect?
- Focus on Freedom Of Expression
- “Duty of care” not a product of case law over a period of years, so imprecise
- OFCOM won’t investigate individual complaints, but will consider “individual experiences”
- Statutory appeals process (rather than judicial review)?
- Encourages satellite & group litigation?
- (Eventual) Director liability without involvement in wrongdoing?
- Fines at UK GDPR scale, and initial uncertainty (“phony war”)?
- Estimated cost of compliance to businesses in scope from UK Government - £1.7 billion over 10 years, with £1.2 billion additional content moderation costs?
- Will tech giants lobby effectively enough to water down proposals?
- Will the regulator have enough “teeth”? – What sanctions remain “on the table”?

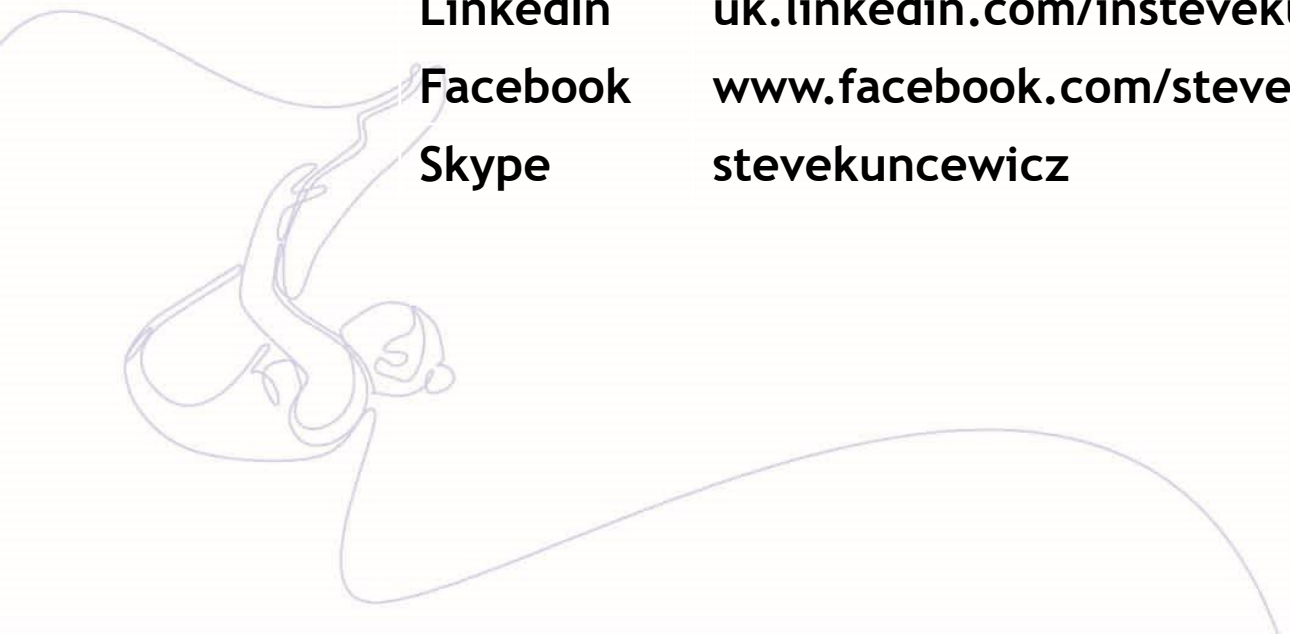


Regulation - where should you start?

- Familiarise yourself with Government papers & consultation responses, final position & draft Online Safety Bill- consider whether you are likely to fall “in scope”
- Build a multi-functional team including legal, human resources, information, technology, compliance and risk management and insurance, consider the implications of being “in scope”
- Consider how this requirement may touch other stakeholders including those in their supply chain and contract terms
- Consider creating a single point of contact with responsibility for dealing with the new regulatory regime – “harm officer”
- Consider to what extent your content and activities fall within the scope of the proposed new regime, and whether you wish to continue providing them
- Under the leadership of the organisation’s data protection officer, carry out a risk assessment, similar to a Data Protection Impact Assessment (DPIA), to get a clear idea of which of their activities may cause “online harm”
- Map current insurance cover to identify any gaps in coverage and any coverage which may protect you from future claims relating to “online harm”, as well as clarifying the scope of cover for regulatory fines
- Watch out for further updates – due later in 2021

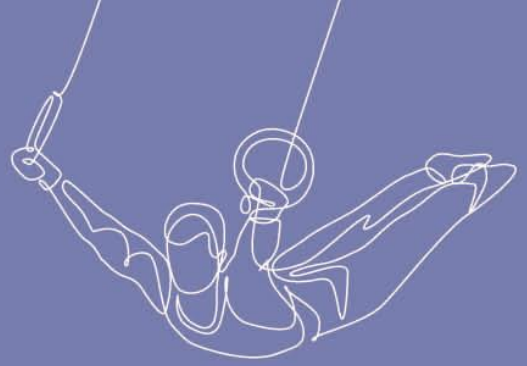


E-mail	Steve.kuncewicz@blmlaw.com
Twitter	@stevekuncewicz
LinkedIn	uk.linkedin.com/instevekuncewicz
Facebook	www.facebook.com/steve.kuncewicz
Skype	stevekuncewicz



ALARM
embrace risk

THE BALANCING ACT



ALARM CONFERENCE 2021

@alarmrisk alarmrisk.com

ZURICH Municipal

PLATINUM SPONSOR