



HERBERT SMITH FREEHILLS

Race to Regulate: Online Harms

Interactive map

- Terrorism
- Pornography
- Violence
- Hate speech
- Political advertising
- Fake news
- Bullying & harassment

- Terrorism
- Pornography
- Violence
- Hate speech
- Political advertising
- Fake news
- Bullying & harassment

- Terrorism
- Pornography
- Violence
- Hate speech
- Fake news
- Bullying & harassment

- Terrorism
- Pornography
- Violence
- Hate speech
- Fake news
- Bullying & harassment



- Terrorism
- Violence

- Terrorism
- Pornography
- Political advertising

- Pornography
- Political advertising
- Fake news
- Bullying & harassment

- Pornography
- Violence
- Hate speech
- Fake news
- Bullying & harassment

- Terrorism
- Pornography
- Hate speech

- Pornography
- Violence
- Hate speech
- Bullying & harassment

- Terrorism
- Pornography
- Violence
- Bullying & harassment

- Pornography
- Violence
- Hate speech
- Fake news
- Bullying & harassment

PROGRESS

- Draft Law
- Law
- Research
- Commitment






Name	The Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019
Type	Terrorism Violence
Status	Law
Sanctions	Criminal penalties for tech companies and executives of up to three years plus financial penalties up to 10% of a company’s global turnover.
What does it mean?	<p>The act introduces two criminal offences:</p> <ul style="list-style-type: none"> • the failure by internet, content or hosting service providers to refer ‘abhorrent violent material’ which they are aware is accessible in Australia through their services to the Australian Federal Police ‘within a reasonable time’; and • the failure by content or hosting service providers to ‘expeditiously’ remove ‘abhorrent violent material’ from their services. <p>The Act was rapidly introduced and passed in the aftermath of the March 2019 Christchurch terrorist attacks and aims to tackle terrorist and violent content online.</p> <p>The Act reflected a growing frustration with the manner in such content has proliferated online (in particular, the live-streaming, and continued accessibility, of video of the Christchurch attacks on several platforms), and sought to ensure that technology companies take active steps to address this.</p> <p>More broadly, the Act can be seen as part of a broader, and growing, sense of public discontent with digital platforms and in particular their claim to be neutral platforms or aggregators rather than ‘publishers’ of content for which they are responsible.</p>
What does the future look like?	<p>The Act, fast-tracked through Parliament and passed with minimal industry consultation, has been heavily criticised, principally on the grounds that it could harm the tech sector and innovation and poses risk for privacy and legitimate whistle-blowing activities.</p> <p>However, global momentum for similar regulatory action elsewhere appears to be growing, and as such these criticisms could be seen to relate more to the manner in which the Act was implemented (and its particular form) rather than its intent or subject matter more generally.</p>



Race to Regulate: Online Harms










Name	Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018
Type	Pornography Bullying & harassment
Status	Law
Sanctions	<p>The eSafety Commissioner’s office can issue companies with 48-hour “takedown notices”, and can issue fines of up to A\$525,000 for corporations and A\$105,000 for individuals who fail to comply with such notices to the extent that the person is capable of doing so (£285,000).</p> <p>The office can also fine individuals up to A\$105,000 for posting the content, as well as obtain a civil penalty of up to five years’ imprisonment (seven years if the conviction follows three or more civil penalty orders).</p>
What does it mean?	<p>The Act was introduced in order to reinforce, and further address, criminal state-based regulation addressing the issue of ‘revenge porn’, or the sharing of intimate images of others without their permission. The Act amended the existing Criminal Code, as well as the earlier Enhancing Online Safety Act 2015, and in addition to granting additional powers to the eSafety Commissioner to enforce its provisions, sought to:</p> <ul style="list-style-type: none"> • expressly prohibit the posting (or threatened posting) of intimate images without consent; and • create new, aggravated offences targeted at those who menace, harass or cause offence through making private sexual material available (or distributing, publishing, advertising or promoting it).
What does the future look like?	<p>Following the adoption of the Act, there have been several successful criminal convictions against individuals for sharing private sexual material. In addition, although the criminal offences introduced by the Act do not apply to service providers, those entities will face fines of up to half a million dollars if they fail to take reasonable steps to remove intimate images promptly after receiving a take-down notice. In the current climate of regulatory and public mistrust of many large technology service providers, we may expect more such notices to be issued.</p>
Contact	<div style="display: flex; justify-content: space-between;"> <div style="text-align: center;">  <p>Julian Lincoln Partner julian.lincoln@hsf.com T +61 3 9288 1694</p> </div> <div style="text-align: center;">  <p>Kwok Tang Partner kwok.tang@hsf.com T +61 2 9225 5569</p> </div> <div style="text-align: center;">  <p>Anna Jaffe Senior Associate anna.jaffe@hsf.com T +61 3 9288 1152</p> </div> </div>



Race to Regulate: Online Harms






Name	Proposed Digital Services Act
Type	 Terrorism  Pornography  Violence  Hate speech  Political advertising  Fake news  Bullying & harassment
Status	Research
Sanctions	Details unclear at this stage (although likely to include mandatory “notice and take down” orders in respect of illegal content)
What does it mean?	<p>The EU are exploring the development of uniform and binding rules to oversee content on digital platforms. These rules are likely to include the removal of illegal content such as illegal hate speech across the EU and a set of fundamental rights safeguards.</p> <p>With the aim being to develop a more effective and multi-jurisdiction accountability framework for content moderation at scale, notice-and-action rules may be tailored to the type and size of the service provider and as such their obligations may differ.</p> <p>These rules are intended to provide a legally binding set of rules for the EU single market, so that Member States will not have to impose national level regulations. While much of the discussion surrounding this proposed act is still speculative, it is suggested that a clear distinction will be made between illegal and harmful content when it comes to exploring policy options.</p> <p>These rules are likely to replace the current EU e-commerce directive.</p>
What does the future look like?	The Act is likely to cover all digital services including online platforms, internet service providers, data storage services and cloud providers. A centralised committee within the European Union is envisaged with the power to enforce rules on illegal content.
Additional reading	Please see our Horizon Scanning: Digital Regulation timeline to read further about, and track the progress of, digital regulation across the UK and EU (including developments relating to the Digital Single Market).



Race to Regulate: Online Harms



Name	Recommendation on measures to effectively tackle illegal content online
Type	 Terrorism  Pornography  Hate speech
Status	Research
Sanctions	If there is evidence of a serious criminal offence or a suspicion that illegal content is posing a threat to life or safety, the Recommendation states that companies should be legally obliged to promptly inform law enforcement authorities.
What does it mean?	<p>On 1 March 2018, the Commission issued a Recommendation on measures to effectively tackle illegal content online because of concern that the removal of illegal content online is not effective enough and that issues such as incitement to terrorism, illegal hate speech, or child sexual abuse material, as well as infringements of Intellectual Property rights and consumer protection online need a strong coordinated EU-wide approach.</p> <p>This Recommendation translates the political commitment of an earlier Communication on “tackling illegal content online into a (non-binding) legal form and encourages Member States to establish the appropriate legal obligations to enable quick and proactive detection, removal and prevention of the reappearance of illegal content online. The Recommendations aim to ensure that online platforms in particular are more responsible in content governance.</p>
What does the future look like?	<p>Member States are encouraged to establish the appropriate legal obligations on online platforms in particular in order to ensure quick and proactive detection, removal and prevention of the reappearance of illegal content online with:</p> <ul style="list-style-type: none"> • Clearer ‘notice and action’ procedures: Online platforms are to set out easy and transparent rules for notifying illegal content. Content providers are to be informed about such decisions and have the opportunity to contest them in order to avoid unintended removal of legal content. • More efficient tools and proactive technologies: Companies are to set out clear notification systems for users and have proactive tools to detect and remove illegal content, in particular for terrorism content and for content which does not need contextualisation to be deemed illegal, such as child sexual abuse material or counterfeited goods. • Stronger safeguards to ensure fundamental rights: To ensure that decisions to remove content are accurate and well-founded, especially when automated tools are used, companies are to put in place effective and appropriate safeguards, including human oversight and verification, in full respect of fundamental rights, freedom of expression and data protection rules.



HERBERT
SMITH
FREEHILLS


Race to Regulate: Online Harms

 European Union

What does the future look like?

- **Special attention to small companies:** The industry should, through voluntary arrangements, cooperate and share experiences, best practices and technological solutions, including tools allowing for automatic detection. This shared responsibility should particularly benefit smaller platforms with more limited resources and expertise.
- **Closer cooperation with authorities:** If there is evidence of a serious criminal offence or a suspicion that illegal content is posing a threat to life or safety, companies are to promptly inform law enforcement authorities.



Name	Code of Practice on Disinformation Action Plan against Disinformation
Type	 Fake news
Status	Commitment
Sanctions	<p>There are no codified sanctions as such as the Code of Practice against Disinformation (CoP) is self-regulatory. The signatories instead commit to do the following:</p> <ul style="list-style-type: none">• support good faith independent efforts to track Disinformation and understand its impact, including the independent network of fact-checkers facilitated by the European Commission upon its establishment which will include sharing privacy protected datasets, undertaking joint research, or otherwise partnering with academics and civil society organizations if relevant and possible;• not to prohibit or discourage good faith research into Disinformation and political advertising on their platforms;• encourage research into Disinformation and political advertising; and• convene an annual event to foster discussions within academia, the fact-checking community and members of the value chain.
What does it mean?	<p>The Code of Practice was published on 26 September 2018 and the European Commission is currently conducting an assessment of the initial 12 month period which is due to be published on 31 December 2019. On 5 December 2018 the European Commission published an Action Plan against Disinformation. The four online signatories published implementation reports setting out the measures taken by each of them to comply with commitments under the CoP on 29 January 2019. Facebook, Google and Twitter pledged to report monthly on measures taken ahead of the European Parliament Elections in May 2019.</p> <p>The European Commission has championed the CoP as being the first time worldwide that the online platform and advertising industries have voluntarily agreed to a collective strategy to fight disinformation. The CoP is a self-regulatory document with which the signatories have undertaken to comply on a voluntary basis. It has been signed by major online platforms including Facebook, Google, Twitter and Microsoft as well as influential advertising trade associations such as the European Association of Communications Agencies and the Interactive Advertising Bureau. The CoP is designed to improve the transparency and accountability of the key players in the online platform and advertising space when it comes to ensuring fair and trustworthy online campaign activity.</p>



Race to Regulate: Online Harms

 European Union

What does the future look like?

The CoP will impact online platforms and advertising industry stakeholders.

The CoP includes a wide range of commitments to be undertaken by its signatories including in relation to monitoring and closure of fake accounts, increasing transparency of political advertising and prevention of purveyors of disinformation from profiting from their actions. It also includes a commitment by the signatories to use reasonable efforts towards devising ways of disclosing “issue-based advertising”, (advertising which advocates for or against a particular issue, particularly where that issue is being contested as part of an election or referendum) which may include who has paid for the relevant advertising which is particularly relevant in the context of recent elections and referenda won on the back of one or two key issues.






The signatories to the CoP have also committed to invest in and implement products, technologies and programs designed to:

- help individual users assess the authenticity and trustworthiness of information sources they encounter online;
- be able to critically evaluate the information provided by those sources;
- understand why they are seeing particular content or advertisements; and
- be able to access a diverse range of perspectives on particular public interest topics.



Race to Regulate: Online Harms





Name	Proposal on preventing the dissemination of terrorist content online		
Type	 Terrorism	 Violence	
Status	Research		
Sanctions	Providers will have to remove terrorist content or disable access to it within one hour from receiving a removal order from authorities. If a hosting service provider fails to comply with removal orders, they may be liable to a penalty of up to a maximum of 4% of their global turnover for the previous year.		
What does it mean?	The proposed regulation, which followed a consultation on how to tackle the issue of illegal content online, is aimed at protecting EU citizens by preventing the misuse of hosting services for the dissemination of terrorist content. The new rules apply to all hosting service providers offering services in the EU, whether or not they have their main establishment in a member state.		
What does the future look like?	<p>If adopted, the proposed regulation would impose a considerable burden on hosting service providers to put in place measures to protect users from terrorist content on their services and will also include taking proactive measures to address the reappearance of content that has previously been removed as well as the requirement for hosting providers to establish effective mechanisms allowing users whose content has been removed to submit a complaint.</p> <p>The new binding removal orders which will require hosting service providers to remove terrorist content online within one hour of it being uploaded are stringent as are the potential penalties for failure to comply with these orders.</p>		
Contact	 Hayley Brady Consultant hayley.brady@hsf.com T +44 20 7466 2079	 James Balfour Associate james.balfour@hsf.com T +44 20 7466 7582	 Anna McGowan Professional Support Lawyer anna.mcgowan@hsf.com T +44 20 7466 2228



Race to Regulate: Online Harms

France

Name	Proposition de loi visant à lutter contre les contenus haineux sur internet (Bill to combat hate content on the internet)
Type	 Terrorism  Pornography  Hate speech
Status	Draft Law
Sanctions	<p>Refusal or delay to remove clearly illegal content, its representative is liable to a criminal offence punishable by one year's imprisonment and a fine of €250,000.</p> <p>In the case of a legal person, the fine may be increased to €1.25 million. The French Audiovisual Council (CSA) may also impose an administrative penalty of up to 4% of worldwide turnover.</p> <p>Abusive reporting is punishable by one year's imprisonment and a fine of €15,000.</p>
What does it mean?	<p>The bill was introduced on 20 March 2019 by MP Laetitia Avia. The text of the law was adopted by the National Assembly at first reading by 434 votes in favour, 33 against and 69 abstentions.</p> <p>The proposed law covers a wide selection of clearly illegal content to be removed under Article 1. Website operators covered include social networks, collaborative platforms and search engines that exceed a certain threshold of unique visitors per month.</p> <p>Website operators must remove the content concerned within 24 hours of being reported. Once masked, illegal content must then be kept for a maximum period of one year for the purposes of research, observation and prosecution of criminal offences. In addition, website operators will have to set up a directly accessible and uniform notification system allowing any person to notify illegal content in the language in which the service is used.</p> <p>This law has of course been the subject of many criticisms, in particular the fact that decisions to remove content are taken by a private operator without the intervention of the judicial judge, the risk of excessive removal and the delimitation is considered too broad of the clearly illegal content designated by the proposed law.</p> <p>On 23 August 2019, the government responded to these criticisms by stating that the 24-hour deadline will not apply to content that raises questions of appreciation, and will only apply to clearly illegal content.</p>



HERBERT
SMITH
FREEHILLS

Race to Regulate: Online Harms

 France

What does the future look like?

The bill will be examined by the Senate in September. If adopted, the text would have to enter into force on 1 January 2020. In addition, if the text is adopted, the French Audio visual Council, instead of the French National Data Protection Registrar (CNIL), will take control of requests concerning child pornography or terrorist signs, from 1 January 2021.

Contact



Alexandra Neri
Partner
alexandra.neri@hsf.com
T +33 1 53 57 78 30






Sébastien Proust
Of Counsel
sebastien.proust@hsf.com
T +33 1 53 57 73 89





Race to Regulate: Online Harms

Germany

Name	Network Enforcement Act (Netzwerkdurchsetzungsgesetz)
Type	Terrorism Pornography Violence Hate speech Fake news Bullying & harassment
Status	Law
Sanctions	<p>Victims of such violations can inter alia demand immediate deletion from the social network.</p> <p>Companies then have a 24 hour deadline to remove illegal content.</p> <p>Violations of these duties can be punished with individuals fined up to €5 million and companies up to €50 million.</p>
What does it mean?	<p>In order to force social networks to process complaints, especially from users, about hate speech and other criminal content more quickly and comprehensively, the act introduces statutory compliance rules for social networks.</p> <p>It provides for a statutory reporting obligation for social networks on how to deal with hate speech and other criminal content, effective complaint management and the appointment of a domestic “complaints officer”. These obligations must be met by social networks with more than two million registered users in Germany.</p>
What does the future look like?	<p>According to former Minister of Justice Heiko Maas, the Network Enforcement Act was a “necessary and overdue” step to enforce existing laws. Nevertheless, there is also criticism of the law in Germany. It is claimed that it restricts the fundamental rights of freedom of speech and freedom of the press too far. Due to the “increasing right-wing hatred”, the current Minister of Justice Christine Lambrecht even wants to tighten up the Network Enforcement Act. Even though the law is broadly endorsed, the discussion about its scope therefore remains topical and interesting.</p>
Contact	<div style="display: flex; justify-content: space-between;"> <div style="text-align: center;">  <p>Marius Boewe Partner marius.boewe@hsf.com T +49 211 975 59066</p> </div> <div style="text-align: center;">  <p>Marcel Nuys Partner marcel.nuys@hsf.com T +49 211 975 59065</p> </div> <div style="text-align: center;">  <p>Florian Huerkamp Counsel florian.huerkamp@hsf.com T +49 211 975 59063</p> </div> </div>



Name	The Christchurch Call
Type	 Terrorism  Violence
Status	Commitment
Sanctions	NA
What does it mean?	<p>The Christchurch call is a commitment by Governments (in Australia, New Zealand and Europe, but not currently including the US) and tech companies (including Amazon, Daily Motion, Facebook, Google, Microsoft, Qwant, Twitter and Youtube) to eliminate terrorist and violent extremist content online.</p> <p>The Christchurch Call sets out a number of broad objectives for government and tech companies. These commitments are worded in a way which leave lots of discretion on implementation.</p> <p>Significant steps have already been taken to address this issue by, among others: the European Commission with initiatives such as the EU Internet Forum; the G20, and the G7, including work underway during France's G7 Presidency on combating the use of the internet for terrorist and violent extremist purposes; along with the Global Internet Forum to Counter Terrorism (GIFCT); the Global Counterterrorism Forum; Tech Against Terrorism; and the Aqaba Process established by the Hashemite Kingdom of Jordan.</p>
What does the future look like?	<p>Together with United Nations, members of the Call have agreed on an overhaul of the GIFCT to make it an independent body that will drive much of the tech sector's work on implementing the Call. The launch of a new crisis response protocol is intended to be used by governments and tech companies in the wake of terrorist and violent extremist attacks to coordinate and to manage the online impacts of the attack. A Christchurch Call Advisory Network has also been established to advise on the implementation of the Call.</p>



HERBERT
SMITH
FREEHILLS

Race to Regulate: Online Harms

 Global

Contact



Julian Lincoln
Partner
julian.lincoln@hsf.com
T +61 3 9288 1694



David Coulling
Partner
david.coulling@hsf.com
T +44 20 7466 2442



Alexandra Neri
Partner
alexandra.neri@hsf.com
T +33 1 53 57 78 30



Anna Jaffe
Senior Associate
anna.jaffe@hsf.com
T +61 3 9288 1152



Kaman Tsoi
Special Counsel
kaman.tsoi@hsf.com
T +61 3 9288 1336



Hayley Brady
Consultant
hayley.brady@hsf.com
T +44 20 7466 2079







Race to Regulate: Online Harms

Indonesia

Name	Electronic Information and Transactions (EIT Law) (Law No. 11 of 2008 as amended by Law No. 19 of 2016)
Type	Pornography Violence Hate speech Fake news Bullying & harassment
Status	Law
Sanctions	Maximum six year term of imprisonment and/or maximum fine of IDR1 billion. If the criminal act is committed by a corporation, the sentence will be increased by two-thirds.
What does it mean?	The EIT Law prohibits any person from intentionally or without rights distributing or creating electronic information that is violent, insulting, defamatory, threatening, false or misleading, hate speech that creates feuds amongst community groups or data that is modified to appear authentic.
What does the future look like?	The Ministry of Communication and Informatics (MOCIT) is in the process of preparing more specific regulation on online harmful content. While preparing the draft, MOCIT are also conducting a comparative study to learn how other countries in Asia and the EU regulate online harmful content. Currently, there is no public access to the draft regulation.



Name	The Provision of Applications Services and/or Content through The Internet (Over the Top (OTT) Circular Letter No.3/2016)
Type	 Pornography  Hate speech  Fake news  Bullying & harassment
Status	Law
Sanctions	No sanctions are regulated under OTT Circular Letter
What does it mean?	<p>The OTT Circular Letter is issued to alert businesses of the upcoming regulation to give sufficient time for them to be prepared to obey the provisions. Under the OTT Circular Letter, an OTT service provider has full responsibility in providing the OTT content services and is obliged to, among others:</p> <ul style="list-style-type: none"> • comply with laws and regulations on anti-monopoly, trading, consumer protection, intellectual property, broadcasting, movies, advertising, pornography, anti-terrorism, tax and any other prevailing laws and regulations; • conduct data protection, content filtering and censor mechanism in accordance with the prevailing laws and regulations; • ensure access to lawful tapping/interception of information and collection of evidence for criminal investigations conducted by the relevant authorities in accordance with the prevailing laws and regulations; • provide information and/or manuals on using the OTT services in the Indonesian language in accordance with the prevailing laws and regulations; • not provide services with contents which: <ul style="list-style-type: none"> - conflict with the Indonesian Constitution or prevailing laws and regulations or threatens the unity of the Republic of Indonesia; - give rise to conflict between groups, ethnicities, races and intergroup, insult, harass and/or desecrate religion (suku, agama, ras, dan antar golongan (SARA)); - encourage the public to engage in unlawful acts, violence, selling or consuming narcotics, psychotropics and other addictive substances or to degrade human dignity; - violate decency and pornography, gambling, humiliation, extortion or threats, defamation, hatespeech, or copyright infringement.



HERBERT
SMITH
FREEHILLS

Race to Regulate: Online Harms

 Indonesia


What does the future look like?

MOCIT is in the process of preparing more specific regulation on online harmful content. While preparing the draft, MOCIT are also conducting a comparative study to learn how other countries in Asia and the EU regulate online harmful content. Currently, there is no public access to the draft regulation.



Race to Regulate: Online Harms




Indonesia

Name	Controlling Internet Websites Containing Negative Content (Regulation of Minister of Communication No.19 of 2014)
Type	Pornography Hate speech Fake news Bullying & harassment
Status	Law
Sanctions	Internet service providers that fail to block websites on the TRUST+ Positive list are liable to criminal and administrative sanctions available under Law No. 36 of 1999 on Telecommunications, Law No. 11 of 2008 on Information and Electronic Transactions, and Law No. 44 of 2008 on Pornography.
What does it mean?	<p>This regulation sets out the procedure and basis for the government (through the MOCIT) to require Internet Service Providers to block online harmful content consisting of:</p> <ul style="list-style-type: none"> • pornography; and • other illegal activities based on prevailing laws and regulations. <p>Government institutions, law enforcers and the general public may submit reports to the Director General requesting websites with negative content be blocked. These websites are placed on a "TRUST+ Positive" list. Internet Providers must ensure they block access to these sites at least once per week.</p>
What does the future look like?	MOCIT is in the process of preparing more specific regulation on online harmful content. While preparing the draft, MOCIT are also conducting a comparative study to learn how other countries in Asia and the EU regulate online harmful content. Currently, there is no public access to the draft regulation.
Contact	 <p>Sakurayuki Partner (Hiswara Bunjamin & Tandjung, in association with Herbert Smith Freehills) sakurayuki@hbtlaw.com T +62 21 3973 8000</p>



Race to Regulate: Online Harms

↗ Mainland China

Name	Cyber Security Law of China (CSL)
Type	 Terrorism  Pornography  Political advertising
Status	Law
Sanctions	Maximum penalty up to RMB1,000,000 or ten times of the illegal incomes plus criminal and operational penalties (such as revocation of licenses)
What does it mean?	<p>The Cyberspace Administration of China (CAC) has been given the role of policing online content and coordinating the regulatory and enforcement efforts of various ministries in the cybersecurity sphere. Ever since the enactment of the CSL, the CAC and other ministries have intensified their action. Online content regulation is included in the CSL as an integral part of the cybersecurity landscape, which is of particular importance in China.</p> <p>Network operators are required to monitor the content being transmitted on their applications and platforms, and delete and report any violation of the law. The CAC has published regulations targeted at almost all the mainstream online speech forms, including the microblog, Wechat groups, public comments, online communicates and forums, and have requested all new applications capable of “mobilising the society” or influencing public opinion to go through a security assessment before being launched to the public. An array of rules have been published to focus on the online news service, which is subject to filing and approval of the CAC.</p> <p>The CSL proposes to build a cybersecurity protection regime centred around the multi-level protection scheme (MLPS), which classifies each network operator into different levels according to their importance to national security and public interest. The network operators will have to discharge their protection duties as specified by laws, regulations and standards. In addition, a small group of network operators that are most important will be considered critical information infrastructure (CII) operators and receive extra scrutiny on security protection.</p>
What does the future look like?	The CAC and other ministries have published a series of formal and draft regulations and national standards in an effort to fully implement the CSL and has accelerated its regulatory process in the past 12 months. As the core regulatory regime is being built up, it is expected that the authorities will step up their enforcement actions in the coming years. All the network operators must operate within the regulatory framework and strengthen their compliance efforts to avoid violations.



HERBERT
SMITH
FREEHILLS

Race to Regulate: Online Harms

 Mainland China

Contact



Karen Ip
Partner
karen.ip@hsf.com
T +86 10 6535 5135









James Gong
Senior Associate
james.gong@hsf.com
T +86 10 6535 5106



Race to Regulate: Online Harms



Name	Federal Law on Information, Information Technologies and Information Protection (The Information Law) Code of Administrative Offences of the Russian Federation Criminal Code of the Russian Federation
Type	 Terrorism  Pornography  Violence  Hate speech  Fake news  Bullying & harassment
Status	Law
Sanctions	<p>Individuals are subject to administrative liability such as fines or in certain cases, administrative arrest, if their actions do not amount to a crime. In the case of criminal liability, the Criminal Code provisions apply such as fines, imprisonment mandatory labour.</p> <p>Legal entities are subject to administrative liability only as Russian law is not familiar with a concept of criminal liability for corporates.</p>
What does it mean?	<p>The Information Law has historically provided for a list of information that is prohibited or limited for distribution in Russia where the imposition of any such limitations was the prerogative of the courts. The recent novelties in the regulatory framework are:</p> <ul style="list-style-type: none"> • Increase in the role of administrative authorities in imposing and enforcing the limitations on spread of certain categories of information (Restricted Information) in Russia and the instances where such limitations may be imposed out-of-court. In particular, administrative authorities include the office of the Attorney General of the Russian Federation and Federal Service for Supervision of Communications, Information Technology and Mass Media (RKN); • The introduction of new controversial categories of Restricted Information - Insults against Authorities and Fake News; • The introduction of a concept of an Undesirable Organisation - an international or foreign (governmental or non-governmental organisation) whose activities are deemed prejudicial to the security of the state and to the fundamentals of Russian Constitution by the office of the Attorney General of the Russian Federation. <p>The way the regulatory system works is that:</p> <ul style="list-style-type: none"> • It targets both the operators of the key online infrastructure (eg hosting providers, news aggregators, search engines and online media) (Infrastructure Operators) and individual internet users;



Race to Regulate: Online Harms



Russia

What does it mean?

- The Infrastructure Operators are expected to work closely with the RKN and other competent authorities to enforce the regulatory regime regarding access to Restricted Information. For instance:
 - RKN maintains the list of online resources containing information prohibited for distribution in Russia on the basis of a court decision or a decision of a competent governmental authority (child pornography, incitement of suicide or instructions to commit suicide, information on a minor – the victim of a crime, information on illicit drug production and distribution etc). RKN notifies hosting providers of the details of an online resource containing the relevant Restricted Information, which in turn informs the owner of the online resource. If the relevant Restricted Information is not removed, the resource is added to the block-list and hosting and communication service providers are liable to ensure that the access to it are blocked;
 - The Insults against Authorities and the Fake News or the spread of information about Undesirable Organisations is limited by the Infrastructure Operators on the basis of an instruction from RKN which is initiated by the office of the Attorney General. The RKN identifies the Infrastructure Operators for the websites, spreading the relevant categories of the Restricted Information and send an official notice to them. The Infrastructure Operators immediately notify the respective website owners that they must delete the Insulting Information in 24 hours. Failure to comply with the RKN's request results in blocking the website in the Russian Federation, until the relevant Restricted Information has been deleted.
 - Certain categories of the Infrastructure Operators (eg news aggregators or audio/video content aggregators) are required to ensure that their platforms are not used for the spread of certain specified categories of Restricted Information. Certain other categories of the Infrastructure Operators (eg the operators of instant messaging engines) are required to identify their users and store certain information and infrastructure in Russia on penalty of the access to their platforms being restricted in Russia.
- The cooperation of the Infrastructure Operators is ensured through their and their officer's administrative liability.
- The compliance of individual online users with the Restricted Information regime is ensured through the means of administrative and criminal liability against them personally.








What does the future look like?

The regulatory trends that we are seeing is the increased role of out-of-court enforcement mechanisms operated by RKN and the office of the Attorney General. The particular target is on the Infrastructure Operators whose cooperation is vital for the regulatory regime to work. Given the declared trend on the construction of a "sovereign" Russian Internet sector, it seems more likely than not that stricter obligations will be imposed on both the Infrastructure Operators and the online users, who shall be vigilant to limit their exposure for their online conduct (particularly, following a set of court cases based on the recent Fake News and Insults against Authorities additions to the regulatory framework, which showed that the authorities will not hesitate in enforcing the restrictions).




Race to Regulate: Online Harms



Name	<p>The right to oblivion</p> <p>Federal Law on Information, Information Technologies and Information Protection (The Information Law)</p> <p>Code of Administrative Offences of the Russian Federation</p>				
Type	<p> Fake news</p>				
Status	<p>Law</p>				
Sanctions	<p>Administrative liability and associated fines</p>				
What does it mean?	<p>An individual is entitled to request that an online search engine operator removes from the search results all resources containing illegal, outdated, misleading or inaccurate information about the applicant. The online search engine operator may comply with the request or decline to do so (giving reasons). The applicant then might apply to court.</p> <p>The applicant may not request that the search engine operator removes from the search results any information on potentially criminal actions of the applicant in relation to which the statute of limitation has not yet expired or information on the applicant having been convicted of a crime in relation to which the record of conviction has not yet been expunged.</p>				
What does the future look like?	<p>This initiative is aimed at protecting the privacy of individual online users although there is concern that the right might be abused by public officials or public figures to conceal information of public importance. The right was first introduced in 2015 and there are several precedents where it has been successfully implemented and there are no further initiatives at this stage.</p>				
Contact	<table border="0"> <tr> <td data-bbox="427 1166 573 1310"></td> <td data-bbox="600 1166 875 1278"> <p>Alexei Roudiak Partner alexei.roudiak@hsf.com T +7 495 363 6500</p> </td> <td data-bbox="1111 1166 1256 1310"></td> <td data-bbox="1283 1166 1570 1278"> <p>Danil Guryanov Senior Associate danil.guryanov@hsf.com T +7 495 783 6778</p> </td> </tr> </table>		<p>Alexei Roudiak Partner alexei.roudiak@hsf.com T +7 495 363 6500</p>		<p>Danil Guryanov Senior Associate danil.guryanov@hsf.com T +7 495 783 6778</p>
	<p>Alexei Roudiak Partner alexei.roudiak@hsf.com T +7 495 363 6500</p>		<p>Danil Guryanov Senior Associate danil.guryanov@hsf.com T +7 495 783 6778</p>		



Name	Protection from Online Falsehoods and Manipulation Act (POFMA) 2019
Type	 Fake news
Status	Law
Sanctions	<p>Individuals who communicate falsehoods will be liable to a fine up to S\$50,000 and/or a term of imprisonment up to five years. For non-individuals (eg online media platforms run by tech companies), a fine up to S\$500,000 will be imposed.</p> <p>Alternatively, where a fake online account or bot is used to spread such falsehoods, offenders who are individuals will be liable to a fine up to S\$100,000 and/or a term of imprisonment up to 10 years. For non-individuals, a fine up to S\$1 million will be imposed.</p> <p>Additionally, if a falsehood has been communicated, the Minister can issue Directions found in Part 3 of the POFMA (Part 3 Direction) if it is in the public interest to do so.</p> <p>Non-compliance with a Part 3 Direction is an offence that individuals can be fined up to S\$20,000 and/or imprisoned for up to 12 months. For non-individuals, they may be liable to a fine up to S\$500,000.</p>
What does it mean?	<p>POFMA was passed in May 2019 by the Parliament gazette in June 2019 and came into effect on 2 October 2019. POFMA primarily aims to protect society from the damage caused by deliberate online falsehoods and fake accounts used to spread such falsehoods.</p> <p>It also intends to protect against malicious actors who knowingly spread harmful falsehoods, or offer disinformation tools and services, by implementing criminal sanctions. Statements communicated to one or more end-users in Singapore, through the internet and on social media platforms such as Facebook and Twitter, as well as MMS and SMS, will fall under the POFMA's purview. POFMA will also cover closed platforms, such as private chat groups and social media groups. However, POFMA does not cover opinions, criticism, satire or parody.</p> <p>POFMA also grants the powers to the competent authority to issue binding Codes of Practices for technology companies as a more proactive step to prevent abuse of their platforms, and keep their platforms safe and secure.</p> <p>A new POFMA office has been established within the Info-communications Media Development Authority (IMDA) to act as the administering body.</p> <p>Note that the POFMA is mainly intended for "public interest" purposes, while individuals and victims should rely on recourses under the Protection from Harassment (Amendment) Act, discussed below.</p>



What does it mean?

In order for any legal action to be taken under POFMA, two criteria must be met:

- there must be a false statement of fact which has been or is being communicated in Singapore, and
- it must be in the public interest to do something. It is in the public interest to do anything, if the doing of such thing is necessary or expedient:
 - in the interest of the security of Singapore or any part of Singapore;
 - to protect public health or public finances, or to secure public safety or public tranquillity;
 - in the interest of friendly relations of Singapore with other countries;
 - to prevent any influence of the outcome of an election to the office of President, a general election of Members of Parliament, a by-election of a Member of Parliament, or a referendum;
 - to prevent incitement of feelings of enmity, hatred or ill-will between different groups of persons; or;
 - to prevent a diminution of public confidence in the performance of any duty or function of, or in the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board.

POFMA also sets out the actions and orders which may be made against internet intermediaries and providers of mass media services. These include directions which may be made to an internet intermediary that provided the service by means of which the relevant material was communicated in Singapore, such as:

- **Targeted Correction Direction:** to communicate by means of that services to all end users in Singapore, a correction notice.
- **Disabling Direction:** to disable access by end-users in Singapore.
- A **General Correction Direction** may also be issued to licence holders under the newspaper and Printing Presses Act (Cap. 206), Broadcasting Act (Cap. 28), Telecommunications Act and other prescribed internet intermediaries or persons to communicate, publish, broadcast or transmit such correction notices.

In certain circumstances, the Minister may also declare an online location as a declared location (if it publishes at least three different falsehoods against public interest first communicated in Singapore in the preceding six months), and the internet access service provider may be ordered to take reasonable steps to disable access by end-users in Singapore to the declared online location.



What does it mean?

In addition, service providers and digital advertising intermediaries must take reasonable steps (both in and outside Singapore) to ensure that any paid content that it includes or causes to be included on a declared online location is not communicated in Singapore on the declared online location (thereby cutting off its profits).

POFMA (and the wider recommendations made by the Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures (Select Committee)) reflect the Government's growing attitude that technology companies need to contribute to a clean internet ecosystem. Technology companies are also encouraged to increase their transparency and improve accountability by looking at how they can prevent the spread of false information and ensure their digital advertising tools are not used by suspicious actors.

The competent authorities may, also pursuant to the POFMA, issue code of practices:

- to prescribed digital advertising intermediaries and prescribed internet intermediaries for the purposes of enhancing transparency in communication in Singapore of paid content that is directed to a political end; and
- to prescribed internet intermediaries for the purposes of detecting, controlling and safeguarding against misuse of online accounts, and giving prominence to credible sources of information and not giving prominence to declared online location or any location that consists of or contains a statement or material that is the subject of Directions made under the POFMA.

What does the future look like?

The new law has been seen to be controversial and three nominated members of Parliament abstained, while members of the opposition Workers' Party voted against the bill.

POFMA is part of a multi-pronged, nation-wide response to tackle online falsehoods. POFMA also includes criminal sanctions as the Government looks to further tackle against malicious acts making use of digital tools for misinformation campaigns that have national security implications.

The view from many technological companies is that self-regulation by online platforms was adequate to deal with the problems posed by online falsehoods and additional regulation was not required. Social media giants such as Facebook, Google and Twitter have voiced that they are not in a position to be 'arbiters of truth' and are unlikely to adopt internal policies to ensure everything posted on its platform must be 'true, verified and accurate'. They are however, prepared to respect court orders requiring it to take down any online falsehoods. Additionally, these technology giants have also expressed concerns about the anticipated high compliance costs in relation to POFMA requirements.



Race to Regulate: Online Harms

 Singapore

What does the future look like?

These legislative reforms culminate to a broader, and growing, sense of public awareness of intangible yet harmful content in the age of internet and technology, and demonstrate the Government's pressing attitude towards tackling such content that have the potential to negatively impact on both personal and national security and privacy.

The introduction of POFMA will increase compliance obligations of various technological intermediaries, and the challenge would be to come up with a viable compliance framework to satisfy, in particular, the requirement of "reasonable care" defence in certain cases against civil and criminal liabilities. We expect that more detailed implementation mechanisms will be introduced via subsequent subsidiary legislations and codes or practices which will give further guidance to parties involved.



Race to Regulate: Online Harms



Name	Protection from Harassment Act (POHA) Amendment Bill 2019
Type	Fake news Bullying & harassment
Status	Draft Law
Sanctions	A perpetrator who breaches any order or direction in a protection order can be fined up to S\$5,000 and/or jailed up to six months. The May 2019 amendments to the POHA put in place tougher penalties for repeated breaches of protection orders (POs). In the future, repeat breaches of POs will command a fine of up to S\$10,000 and/or a jail term of up to 12 months.
What does it mean?	Enacted in 2014, POHA intends to protect victims of harassment by giving them a range of criminal and civil remedies against harassment, and civil remedies for false statements of facts. The Amendment Bill was passed by Parliament in May 2019 and gazetted in June 2019, but the changes are not yet in effect. The amendments include proposed changes to online falsehoods affecting private persons (both individuals and entities), doxxing and the creation of the Protection from Harassment Court (PHC) to simplify the process for persons seeking a court order.
What does it mean?	The amendments also bring the POHA in line with various provisions in the Women’s Charter (Cap. 353) with a view that the Women’s Charter similar deals with harassment through the issuance of personal protection orders. The amendments recognise that an entity’s reputation may be ruined if online falsehoods are allowed to continue. Therefore, it will enhance protection for such entities by allowing them to obtain remedies as victims of falsehood. The scope of orders in relation to falsehoods also expanded, allowing relevant interim orders for victims requiring urgent relief. As for the newly established PHC, it will aim to hear applications for expedited protection orders within 48 to 72 hours of the application. Where there is a risk of actual violence, the PHC will aim to hear the application within 24 hours. Individuals and companies who cannot get their harassers to take down false or damaging statements about them online can turn to the PHC for corrections to be posted and for interim orders to be made in order to stop the spread of false statements. Additionally, under section 499 of the Penal Code, defamation at its broadest is a criminal offence and is also a wrongful act that can give rise to civil action under the tort of defamation and the Defamation Act.
What does the future look like?	The May 2019 amendments have been introduced to keep pace with changes in technology and the POHA is likely to continue to evolve in line with technology and the abuses which may arise.



Name	Criminal Law Reform Act (CLRA) 2019
Type	Pornography
Status	Law
Sanctions	<p>A person who takes an upskirt photo or video faces a possible sentence of up to two years' jail, along with a fine and caning.</p> <p>Knowingly possessing and distributing content of the relevant offence is punishable by imprisonment of up to five years', a fine, and/or caning.</p> <p>Dissemination or threat to disseminate intimate images (ie revenge pornography) is punishable by imprisonment of up to five years', a fine, and/or caning.</p>
What does it mean?	<p>The CLRA passed in Parliament on 6 May 2019, and provides an overhaul of the Penal Code. In addition to codifying cross-border fraud and strengthening protection for minors, in order to keep the Penal Code relevant in the age of internet, the overhaul includes tackling new technology-related sexual offences such as "voyeurism" and the dissemination or distribution of intimate images (revenge pornography).</p> <p>Originally, such offences were dealt with under "Insult of Modesty" in the Penal Code and the Films Act. However, the Government recognised that those areas did not adequately address the range of offences which could potentially cause great harm to the victim.</p> <p>In the Penal Code Review Committee Report (2018), it was specifically recognised that due to the proliferation of the Internet and smart phones, it is extremely easy for intimate images to be uploaded and shared on various platforms, and very difficult for these images to be removed completely. The introduction of the new offence of "distributing or threatening to distribute an intimate image" will provide a stronger and more consistent response to these actions.</p> <p>While offences introduced under CLRA are primarily aimed at perpetrators engaging in voyeurism and revenge porn, the CLRA will also criminalise the possession and distribution of voyeuristic images or recordings by a person who knows or has reason to believe that the image or recording was obtained through the commission of the relevant offence.</p> <p>Platform providers and content providers must remain vigilant of such digital content being distributed across its platforms and take actions to remove, limit or report such acts.</p>
What does the future look like?	This is the most extensive overhaul of the Penal Code in recent history and addresses many offences which were not directly dealt with under the Penal Code. It is likely that additional changes will only take place should new developments in technology warrant such changes.



Race to Regulate: Online Harms

Singapore

Name	Broadcasting (Class Licence) Notification (Notification) and Internet Code of Practice (Code)
Type	Pornography Violence Hate speech
Status	Law
Sanctions	Under the Broadcasting Act, the IMDA has the power to impose sanctions, including fines, on licensees who contravene the Notification and Code.
What does it mean?	<p>Internet Service Providers (ISPs) and Internet Content Providers (ICPs) are regulated through the Notification and Code, both of which are authorised under the Broadcasting Act 1994, to ensure content offered are compliant with the laws. The Government’s key focus is on content such as those relating to public interest, race, religion, pornography and other content harmful to children.</p> <p>Internet Access Service Providers (IASPs) are required under the Internet Class Licence to offer optional internet filtering services to their subscribers either at the point of subscription or renewal of their fixed residential internet access and mobile internet access. One of the aims of this service is to act as a security tool to assist individuals (eg parents) in blocking online harmful content.</p> <p>ISPs and ICPs must ensure, for legal compliance and as a symbolic statement of societal values, that it restricts public access to a limited number of mass impact websites which contain harmful or offensive content. This is of particular importance as the Government does not monitor or restrict individual’s access to online content, nor does it regulate webpages operated by individuals and personal communications such as email and instant messaging.</p> <p>The internet industry is also encouraged to self-regulate and be socially responsible for their content. While not mandatory, IMDA encourages content providers to develop industry costs of practice that can be used to promote greater industry self-regulation and complement existing internet content regulations.</p>



Race to Regulate: Online Harms

 Singapore

What does the future look like?

IMDA recognises the need to educate the public on both the advantages as well as the downsides of the information superhighway. In view of this, IMDA initiates programmes to promote media literacy and the discerning use of the media including the promotion of cyber wellness.

To take such efforts further, the Media Literacy Council (MLC) was formed in August 2012 to spearhead public education programmes and initiatives on media literacy and cyber wellness. As its Secretariat, IMDA supports the Council's programmes to build awareness of media and digital literacy issues and promote responsible online participation.

Contact



Mark Robinson
Partner
mark.robinson@hsf.com
T +65 6868 9808




Sandra Tsao
Director (Prolegis LLC, in Formal Law Alliance with Herbert Smith Freehills)
sandra.tsao@pro-legis.com
T +65 6812 1353



Race to Regulate: Online Harms

 South Africa

Name	Films and Publications Act 1996 (Act) Films and Publications Amendment Bill 2015 (Bill) FPB Online Regulation Policy 2016 (Policy)
Type	 Pornography  Violence  Hate speech  Bullying & harassment
Status	Law
Sanctions	<p>The Act contains sanctions for various types of offences, ranging from the relatively minor offence of distributing certain films or games without registering with the Films and Publications Board (Board) to distributing pornography without it having first been classified by the Board, the distribution of such material to persons under 18 years of age, to the possession, distribution and consumption of child pornography.</p> <p>The most minor offences carry maximum fines of ZAR150,000 (about US\$10,000) or imprisonment for up to eight months. The most serious offences in connection with child pornography carry fines of ZAR2,000,000 (about US\$135,000) or 10 years imprisonment or both.</p>
What does it mean?	<p>The Act requires distributors of films, games and certain publications to register with the Films and Publications Board (Board), and submit each film, game or publication to the Board for examination and classification. The Bill was introduced to deal with the regulation of online publications, including user generated content, as the Act did not specifically address online content.</p> <p>Given the large volume and nature of online content, the Board published the Policy which provides guidance on the self-classification of online content and regulatory compliance. The Policy also deals with user generated content and how that would be dealt with by the Board.</p> <p>Where companies publish or distribute online publications, films or games, they should apply for accreditation and a permit from the Board (in the form of an agreement between the Board and the companies) so they are able to self-classify their content. Although not obliged to monitor user generated content, companies should investigate and take down any content that is prohibited in the Act when they receive complaints or concerns.</p>



HERBERT
SMITH
FREEHILLS



Race to Regulate: Online Harms

South Africa

What does the future look like?

The draft Bill was heavily amended and the subsequent versions, presented for public comment, have been heavily criticised on the basis that the Bill enforces censorship as it is broad-reaching due to vague definitions and an increase in the powers and reach of the Board. Nevertheless, Parliament has passed the Bill and it was signed by the President on 2 October 2019. The only remaining step before it becomes law is the administrative step of the proclamation of a commencement date. Given the extent of public criticism, once it becomes law, it is not impossible that the enacted Bill will face a constitutional challenge from one or more public interest groups.





Name	Cybercrimes Bill B6B-2017 (Bill)
Type	 Pornography  Violence
Status	Draft law
Sanctions	<p>Sanctions for offences committed under the Bill vary from imprisonment for up to five years to imprisonment for up to 15 years or to unspecified fines or both. In some cases, courts can impose a sentence that the court believes is appropriate.</p> <p>In sentencing perpetrators for thefts committed by electronic means, the Bill requires courts to consider the fact that the offence was committed by electronic means to be an aggravating factor. The extent of financial gain from the theft, if the offence was committed in concert with others and the loss suffered by the victim are other aggravating factors that courts are required to take account of.</p> <p>For offences related to hacking activities, the sentence imposed by a court may not be suspended.</p>
What does it mean?	<p>The Bill creates a framework within which cybercrimes can be dealt with and expands upon the existing cybercrimes by providing further detail on those crimes and creating new offences in response to developments in technology generally. New structures are also created by the Bill to assist with the investigation and enforcement of cybercrimes.</p> <p>The Bill criminalises hacking activities, the making available, broadcasting and distribution of data messages which incite damage to property or violence, threatens people with damage to property or violence, or include intimate images. These are termed “malicious communications” in the Bill.</p> <p>Technology companies must ensure that any content published on their online sites, by themselves or by users, does not include any malicious communication.</p>
What does the future look like?	The legislation has not yet been passed into law but is generally being well received as it addresses current technologies and related cybercrimes.



Race to Regulate: Online Harms

 South Africa

Name	Promotion of Equality and Prevention of Unfair Discrimination Act 2000 (PEPUDA)
Type	 Hate speech  Bullying & harassment
Status	Law
Sanctions	PEPUDA establishes equality courts which have jurisdiction to hear matters relating to contraventions. It's powers are civil rather than criminal but equality courts can hand down a wide range of orders including payment of compensation, the making of apologies and restraining orders in respect of unfair or discriminatory conduct.
What does it mean?	<p>PEPUDA was passed, amongst other things, to give effect to the constitutional prohibition of unfair discrimination and its requirements for equality.</p> <p>Technology companies must ensure that content published on their online sites, by themselves or by users, does not include communication or publication relating to hate speech and does not unfairly discriminate against any person. The obligation relating to unfair discrimination is particularly important as the prohibition is broader and extends to the dissemination or broadcasting of this content and the publication or displaying of any advertisement or notice that unfairly discriminates.</p> <p>This places an obligation on technology companies who provide platforms on which users generate their own content and on which advertisements are placed directly by users, to investigate and take down any content that is prohibited by PEPUDA where they receive complaints or concerns about content or where they are aware of this content.</p> <p>A quarter century after the abolition of apartheid, race remains a particularly sensitive topic in South Africa. Publications which discriminate, or promote hatred, based on race are especially concerning to the public. There are a number of examples of reputations and even businesses having been destroyed as a result of the publication of racially derogatory comments. Any company doing business in South Africa should be aware of these sensitivities.</p>



Race to Regulate: Online Harms

South Africa

What does the future look like?

PEPUDA has generally been well received. The prohibition relating to unfair discrimination mirrors the prohibition in the Constitution of the Republic of South Africa, 1996 (Constitution).

The Constitution grants a broad right of freedom of expression but lists certain categories of expression to which the right does not extend. One such category is where speech advocates hatred based on race, ethnicity, gender or religion. PEPUDA goes further than the Constitution by prohibiting the advocacy of hatred based on a number of additional grounds such as sexual orientation, pregnancy and marital status. The legislation could be challenged on this basis, resulting in amendments.

Contact



Rohan Isaacs
Consultant
rohan.isaacs@hsf.com
T +27 10 500 2667










Tatum Govender
Associate
tatum.govender@hsf.com
T +44 20 7466 2374



Race to Regulate: Online Harms

United Kingdom

Name	Online Harms White Paper
Type	 Terrorism  Pornography  Violence  Hate speech  Political advertising  Fake news  Bullying & harassment
Status	Research
Sanctions	The white paper sets out a new system of accountability and oversight for technology companies, with those within scope potentially facing substantial fines (and individual liability for members of senior management) where the duty is breached, among other sanctions.
What does it mean?	<p>On 8 April 2019 the government launched a consultation putting forward plans for a comprehensive “world leading” package of ambitious new online safety measures to help keep UK users, particularly children and vulnerable users, safer online, as well as “support innovation and a thriving digital economy”.</p> <p>The main areas of concern/key issues the UK Government seeks to address include:</p> <ul style="list-style-type: none"> • Protection of individual users from online harmful content, for example: <ul style="list-style-type: none"> - illegal content and activities (eg terrorist content) which threatens national security as well as physical safety of users; - abuse with the impact being particularly damaging for vulnerable people, including children, as well as the potential impact on their mental health and wellbeing; - terrorist groups using online platforms to spread propaganda designed to radicalise vulnerable people and distribute material aimed to aid or abet terrorist attacks; - child sex offenders viewing and sharing inappropriate material, including regarding the sexual abuse of children; - disinformation and fake news undermining democratic value and debate. • Develop rules and norms for the internet, including protecting personal data, supporting competition in digital markets and promoting ethical and responsible digital design.



What does it mean?

- End self-regulation and provide clearer and consistent standards for organisations and oversight for regulating online content, reinforced by appropriate potential enforcement action.
- Harmonise legislative framework and role of the regulator in a disaggregated environment where many regulators are looking at similar / overlapping issues.
- Consolidation of existing legislative initiatives to form part of the online harms framework once established, such as:
 - implementing new measures in national legislation to regulate measures placed on video sharing platforms under the EU Audio Visual Media Services Directive; and
 - age verification legislation for online pornography is expected to come into force January 2020 (originally July 2019) with the UK being the first country to do so, as well as execution of recommendations in respect of disinformation and ‘fake news’.
- Help to shape an internet that is free, open and secure but also protects its users from harms.
- Create an environment to support innovation and to help ensure that innovation and safety online are not mutually exclusive. It is proposed that the regulator will also have a legal duty to pay due regard to innovation and to protect users’ rights online, being mindful not to infringe privacy and freedom of expression.
- Use of emerging technologies and innovative regulation to boost tech-safety.
- Enable the UK to lead the way for new, global approaches to online safety and to make “Britain the safest place in the world to be online”.

What does the future look like?

The consultation closed on 1 July 2019. The government is currently considering stakeholder responses to the consultation and will then publish its response, summarising the feedback received and setting out the action it will take to develop final proposals for legislation. In parallel the government will continue to draw on advice from legal, regulatory, technical, online safety and law enforcement experts to further develop the proposals.

Whilst the UK Government appears to be the first to attempt to address a comprehensive range of online harms in one coherent framework, the regulatory scrutiny of online platforms / social media aligns with wider trends beyond just the UK and we expect other jurisdictions to follow suit. In particular, these include international calls for:

- Government intervention – particularly in the wake of recent high profile co-ordinated cross-platform efforts to generate maximum reach of harmful content such as terrorist attacks; and



Race to Regulate: Online Harms

United Kingdom

What does the future look like?

- introducing tighter regulation of online content to place it on more of an even keel with “offline” content, as well as a universal push towards online platform providers (as well as other providers in the digital ecosystem) being required to take on more responsibility for the user-generated content on online platforms.

Whilst the large technology companies have acknowledged the need for clearer and consistent standards and measures to tackle online harmful content, it remains to be seen whether the proposed regulatory framework adequately strikes the balance between ensuring sufficient accountability and oversight of online platforms, whilst also supporting the growth of digital business and ensuring freedom of speech. Much of the detail will be set out in the codes of practice which are still to be developed by the proposed independent regulator (with stakeholder input).

Contact



Hayley Brady
Consultant
hayley.brady@hsf.com
T +44 20 7466 2079



James Balfour
Associate
james.balfour@hsf.com
T +44 20 7466 7582



Anna McGowan
Professional Support Lawyer
anna.mcgowan@hsf.com
T +44 20 7466 2228



Additional reading

Please access our [Horizon Scanning: Digital Regulation](#) tool to read further about, and track the progress of, digital regulation across the UK and EU (including developments relating to the Digital Single Market).



Race to Regulate: Online Harms


 United States

Name	Honest Ads Act (H.R.2592/S.1356)
Type	 Political advertising  Fake news
Status	Draft Law
Sanctions	Online platforms, and persons requesting to purchase a qualified political advertisement on online platforms, must comply with the disclosure requirements of the Federal Election Campaign Act of 1971 which outlines penalties for failure to comply in section 309. Enforcement provides for monetary civil penalties for violations with higher levels for knowing and wilful violations, with possibility of referring matter to US Attorney General or instituting a civil action.
What does it mean?	<p>The purpose of the bill is “to enhance transparency and accountability for online political advertisements by requiring those who purchase and publish such ads to disclose information about the advertisements to the public, and for other purposes.”</p> <p>By improving the disclosure requirements for online political advertisements, this bill aims to enhance the integrity of American democracy and national security in order to uphold the United States Supreme Court’s well-established standard that the electorate bears the right to be fully informed.</p>
What does the future look like?	<p>The bills have bipartisan support.</p> <p>On 7 May 2019, S.1356 was introduced in the Senate and Referred to the Committee on Rules and Administration, where it remains. H.R.2592 was introduced in the House and Referred to the House Committee on House Administration on 8 May 2019, where it remains.</p>



Race to Regulate: Online Harms


 United States

Name	Federal stalking statute: cyberstalking – stalking that occurs using internet (Section 2261A(2) – Title 18 of the United States Code)
Type	 Bullying & harassment
Status	Law
Sanctions	The penalties available for violating section 2261A, contained in section 2261(b), range from a maximum of five years to a maximum of life where stalking results in death of the victim.
What does it mean?	<p>Cyberstalking refers to a “pattern of malicious or threatening behaviours” involving a “credible threat to harm” through the use of the internet, email or other electronic communications. The law includes any course of conduct that:</p> <ul style="list-style-type: none">• places that person in reasonable fear of the death of or serious bodily injury to “that person, an immediate family member, a spouse or an intimate partner of that person”; or• causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to “that person, an immediate family member, a spouse or an intimate partner of that person”.
What does the future look like?	Federal authorities will continue to prosecute cyberstalking.



Race to Regulate: Online Harms

 United States

Name	Combat Online Predators Act (H.R.570/S.134)
Type	 Bullying & harassment
Status	Draft Law
Sanctions	The maximum imprisonment for the offence is five years greater than the maximum term of imprisonment otherwise provided for that offence in section 2261 (refer to “Federal stalking statute: cyberstalking”).
What does it mean?	This bill adds a new section (2261B – “Enhanced penalty for stalkers of children”) to Title 18 of the United States Code which increases the maximum prison term for a stalking offense, if the victim is under 18 years of age.
What does the future look like?	<p>The bills have bipartisan support. If enacted into law, they will provide greater deterrence and punishment.</p> <p>On 15 January 2019, the S.134 was introduced in the Senate. It passed with an amendment by unanimous consent on 28 October 2019 and was sent to the House, where it was referred to the House Committee on the Judiciary, where it remains.</p> <p>H.R.570 was also introduced in the House on 15 January 2019, and referred to the House Committee on the Judiciary. On 25 February 2019, it was referred to the Subcommittee on Crime, Terrorism, and Homeland Security, where it remains.</p>



Race to Regulate: Online Harms

United States

Name	DEEP FAKES Accountability Act of 2019 (Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act - H.R.3230)
Type	 Pornography  Fake news  Bullying & harassment
Status	Draft Law
Sanctions	<p>Criminal penalties for failure to disclose, or for altering disclosures, is fine and/or imprisonment up to five years.</p> <p>Civil penalties for failure to disclose, or for altering disclosures, is up to US\$150,000 per record or alteration, as well as appropriate injunctive relief.</p> <p>The bill also provides a private right of action with potential damages being the greater of:</p> <ul style="list-style-type: none"> • actual damages suffered by the living person or the affiliated corporation or entity, and any additional substantially derivative profits of the defendant; and • US\$50,000-US\$150,000 per record depending on the facts.
What does it mean?	<p>The Act proposes to add a new section (1041 - “Advanced technological false personation record”) to Title 18 of the United States Code. It is designed to combat the spread of disinformation through restrictions on deep-fake video alteration technology.</p> <p>With exceptions, it provides that “any person who, using any means or facility of interstate or foreign commerce, produces an advanced technological false personation record with the intent to distribute such record over the internet or knowledge that such record shall be so distributed, shall ensure such record, complies with:</p> <ul style="list-style-type: none"> • the watermark requirement under subsection (b); and <p>Digital watermark: any advanced technological false personation record which contains a moving visual element shall contain an embedded digital watermark clearly identifying such record as containing altered audio or visual elements.</p> <ul style="list-style-type: none"> • a. in the case of an audiovisual record, the disclosure requirements under subsection (c); <p>Audiovisual disclosure: any advanced technological false personation records containing both an audio and a visual element shall include:</p> <ul style="list-style-type: none"> - not less than 1 clearly articulated verbal statement that identifies the record as containing altered audio and visual elements, and a concise description of the extent of such alteration; and



Race to Regulate: Online Harms

United States

What does it mean?

- an unobscured written statement in clearly readable text appearing at the bottom of the image throughout the duration of the visual element that identifies the record as containing altered audio and visual elements, and a concise description of the extent of such alteration.

b. in the case of a visual record, the disclosure requirements under subsection (d); or

Visual disclosure: any advanced technological false personation records exclusively containing a visual element shall include an unobscured written statement in clearly readable text appearing at the bottom of the image throughout the duration of the visual element that identifies the record as containing altered visual elements, and a concise description of the extent of such alteration.

c. in the case of an audio record, the disclosure requirements under subsection (e).

Audio disclosure: any advanced technological false personation records exclusively containing an audio element shall include, at the beginning of such record, a clearly articulated verbal statement that identifies the record as containing altered audio elements and a concise description of the extent of such alteration, and in the event such record exceeds two minutes in length, not less than 1 additional clearly articulated verbal statement and additional concise description at some interval during each two-minute period thereafter.”

What does the future look like?




On 12 June 2019, the bill was introduced in the House and referred to the Committee on the Judiciary, and in addition to the Committees on Energy and Commerce, and Homeland Security. The bill was then referred to the Committee on Homeland Security’s Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation on 24 June 2019.

On 28 June 2019, it was referred to the Committee on the Judiciary’s Subcommittee on Crime, Terrorism, and Homeland Security where it remains.



Race to Regulate: Online Harms

United States

Name	Deepfakes Report Act of 2019 (H.R.3600/S.2065)
Type	 Pornography  Fake news  Bullying & harassment
Status	Draft Law
Sanctions	N/A
What does it mean?	<p>The Act requires the Secretary of Homeland Security to publish an annual report on the use of, and state of, digital content forgery technology including artificial intelligence and machine learning techniques, which are able to fabricate or manipulate audio, visual, or text content with the intent to mislead. Acting through the Under Secretary for Science and Technology, the Secretary, must produce the initial report no later than 200 days after the date of enactment of the Act and every 18 months thereafter.</p> <p>Each report shall include, inter alia:</p> <ul style="list-style-type: none"> • an assessment of the underlying technologies used to create or propagate digital content forgeries, including the evolution of such technologies; • a description of the types of digital content forgeries, including use: <ul style="list-style-type: none"> - by foreign or domestic sources; and - in cyber attacks, pornography, and media. • an assessment of how foreign governments, and the proxies and networks thereof, use, or could use, digital content forgeries to harm national security; • an assessment of how non-governmental entities in the United States, use, or could use, digital content forgeries; • an assessment of the uses, applications, dangers, and benefits of deep learning technologies used to generate high fidelity artificial content of events that did not occur;



Race to Regulate: Online Harms

United States

What does it mean?

- an analysis of the methods used to determine whether content is genuinely created by a human or through digital content forgery technology, including an assessment of any effective heuristics used to make such a determination;
- a description of the technological counter-measures that are, or could be, used to address concerns with digital content forgery technology; and
- recommendations regarding whether additional legal authorities are needed to address the findings of the report.

What does the future look like?

The bills have bipartisan support and any future generated reports may prompt further legislative measures.

On 28 June 2019, H.R.3600 was introduced in the House, and referred to the House Committee on Energy and Commerce, where it remains.

On 9 July 2019, S.2065 was introduced in the Senate and referred to the Committee on Homeland Security and Governmental Affairs. It passed the Senate with an amendment by Unanimous Consent on 24 October 2019 and was referred to the House Committee on Energy and Commerce on 28 October 2019, where it remains.

Contact



Joseph Falcone
Partner
joseph.falcone@hsf.com
T +1 917 542 7805



Lawrence Savell
Counsel
lawrence.savell@hsf.com
T +1 917 542 7816