Free speech and internet regulation

Frederick Mostert *

Free speech has always required public forums to flourish, but shaping these forums to the challenging contours of today's online world presents unique challenges. Social media forums serve as the prime source of knowledge and human thought for many users and have taken on the identity of 'the modern public square', as noted by the US Federal Supreme Court.[1]

The ebb and flow of public discourse is at present being controlled and curated in particular by the large social media platforms—the modern-day public forums. As the power and influence of large internet companies have grown, 'privately-run platforms have become akin to public spaces . . . ' as noted in a recent White Paper in the UK.[2] The major players such as Facebook, YouTube and Twitter exercise near omnipotent reach and influence on public discourse to monitor and moderate our speech. In this context, Professor Keller accurately points out: 'Never before have so many of our communications shared a common infrastructure, and hence a common point of control—and never before have so many of us convened in the same virtual "public square" to share our creativity, our political opinions, our cat pictures, and all of the other speech we value. We have barely begun to grapple with what this shift means for our communications ecosystem or our constitutional rights.'[3] As traditional public forums have moved to virtual platforms, the demands of free speech and anti-trust considerations raise the question of whether adequate alternate channels for speech and access to information exist. The private ownership of the public forum in today's world is an issue.[4]

The author

- Frederick Mostert is Founder, Digilabs, Professor of Practice at the Dickson Poon School of Law, King's College, London, Research Fellow at the Oxford Intellectual Property Research Centre, University of Oxford, and a Research Fellow at the Research Centre for Intellectual Property at of Tsinghua University School of Law, Beijing.

This article

- The article analyses free speech and internet regulation.
- Governments have come up with new regulatory proposals for privately-controlled platforms virtually overnight in contrast to their traditional hands-off approach to platform regulation. The Internet Safety Report in the UK, the EU Directive on Copyright in the Digital Single Market and the US President's Memorandum on Combating Trafficking in Counterfeit and Pirated Goods, and a slew of other regulatory proposals, were produced within an extraordinarily short space of time.
- In particular, free speech has always required public forums to flourish, but shaping these forums to the challenging contours of today's online world presents unique challenges. Social media forums serve as the prime source of knowledge and human thought for many users and have taken on the identity of 'the modern public square', as noted by the US Federal Supreme Court.

* Email: frederick.mostert@kcl.ac.uk.

1 *Packingham v North Carolina*, 137 S Ct 1730, 1737 (2017) (deciding that North Carolina could not prohibit sex offenders from using Facebook and other platforms) Justice Kennedy eloquently described this phenomenon even further: 'Minds are not changed in streets and parks as they once were. To an increasing degree, the more significant interchanges of ideas and shaping of public consciousness occur in mass and electronic media.' in *Denver Area Educ Telecommunications Consortium, Inc v FCC*, 518 US 727 (1996) at 802-3.

2 UK Government, DCMS Online Harms White Paper, 8 April 2019, at 6 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>. See also UK House of Lords, Select Committee on Communications, Regulating in a Digital World, 9 March 2019, at 3 and 8 : 'The digital world has become dominated by a small number of very large companies . . . " and "A small number of companies have great power in society and act as gatekeepers to the internet' at 4 (and 34) - <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>.

3 Daphne Keller, 'Who do You Sue, State and Platform Hybrid Power Over Online Speech, A Hoover Institute Essay', at 27, <https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf>.

4 Keller, ibid-. As she aptly noted: ' . . . the economic success of a handful of platforms and the resulting concentration of users . . . effectively creates new bottlenecks and scarcity of communication channels'.

Some may argue that the concentration of the private ownership of the public forum is the defining central issue/shift of our time. The shift is quantitatively and qualitatively different from previous eras. We have seen similar issues raised before, for example, when privately owned

doi:10.1093/jiplp/jpz074
Advance Access Publication 25 June 2019

A unique case in the context of the off-line world, demonstrating remarkable insight into public forums and free speech in private spaces is *PruneYard v Robins*.[5] The US Supreme Court affirmed plaintiffs' rights, as activists, under the California constitution, to enter a Silicon Valley shopping mall to distribute leaflets. A privately controlled space, therefore, was recognized as a public forum for free speech purposes because of its social and community function. It may well be argued that in today's world platforms provide the same compelling social and community function, if not more so.

Of interest is the fact that the original real-world public 'Forums' promoted speech in Roman law times. Although constitutional rights of freedom of speech were obviously not recognized, public 'Fora' in Rome were considered to be public spaces where speech must be encouraged during the Republican period. The great traditions of public speech and oratory in public forums, a cornerstone of Western liberal democracy, may very well have some of their origins during this Roman law period. As a Roman law scholar, Professor Diaz de Valdes,[6] notes: 'The Forum ... was for all the citizens of Rome. It was open, wide and popular. It was also the main stage of the influential Roman oratory tradition ... the main functions of the Forum were the political education of the people, providing information on public affairs, and oratory contests. All of the above consolidated the Forum as a privileged place for the exercise of freedom of speech ... '[7]. There are obvious similarities between ancient Roman 'Forums' as places where people would congregate for commercial and social activities in open markets, and the shopping malls and social media platforms of the present day. Whether a real-world forum of 50 BC or the Twitterverse, they share the same compelling social and community functions of informing the public, encouraging speech and the airing of the different sides to issues of public importance.

Against this background, it is counter-intuitive to observe that there is little scope for legal and even constitutional grounds for asserting free speech claims against platforms by users who generate content on those platforms in the US. The reason is that platforms and our modern public forums are in private ownership and control. Free speech claims are traditionally brought against government in public forum settings—not in the context of privately-owned spaces. Consequently, to date, most of the legal challenges by content-generating users against privately controlled platforms have been unsuccessful in the US[8]. Many users who generate content online (such as criticisms or parodies), have in some instances had their works taken down by platforms as offensive speech or as infringing copyright material. These users have mostly failed to compel the platforms to re-instate such content on the grounds of free or artistic expression. The users have argued that the platforms essentially act as public forums and therefore 'must carry' their works or content.[9]

The argument, which the platforms have wielded against such 'must carry' claims by users, is a First Amendment defence. The defence is predicated on the premise that platforms, as private content curators, will lose the right to express their editorial judgment through their removal choices.[10] The counter-arguments from 'must carry' claimants are that the Big Tech platforms, with significant market presence, have in reality become the gatekeepers of today's public

newspapers and television networks (for example the three major US networks) became significantly influential. The network and reach effects driving today's social media are quite different, though. For instance, in the past local newspapers could compete with national papers and access independent revenue, hence allowing different viewpoints. Simple regulations could prevent reach. However, Facebook and Google directly compete in local markets for news and revenue, and have driven local reporting to endangered status. Newspaper content is driven by contracted journalists whose work, on the whole, is meticulously fact-checked. Social Media Content is usually independently user-generated and typically not fact-checked.

This leads to the obvious next question around the disruption of the news industry. Are Facebook or YouTube publishers, or a neutral tech platform from a legal perspective? Even Facebook has given different answers to this question depending upon the circumstances—see 'Is Facebook a publisher? In public it says no, but in court it says yes'. The Guardian, 'https://www.theguardian.com/technology/2018/jul/02/facebook-mark-zuckerberg-platform-publisher-lawsuit'.

This is a subject on its own - worthy of a separate law review article.

5 *Pruneyard Shopping Ctrs v Robins* 447 US 74 (1980). 447 US 74 (1980). See contra - *Hudgens v NLRB*, 424 US 507, 521 (1976) (federal First Amendment 'has no part to play' in a case against privately owned shopping centre).

6 Jose Manuel Diaz de Valdes, 'Freedom of Speech in Rome' <https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S0716-54552009000100004&lng=en&nrm=iso>, see also in a related, but more narrow context, Laura Robinson, '*Freedom of Speech in the Roman Republic* xiv+93. Baltimore: J H Furst Company, 1940. Paper.

It should also be noted that the ancient Greeks had two concepts of freedom of expression: one called *isegoria*, which described the equal right of citizens to participate in public discourse in, and the other *parrhesia*, the license to say what one pleased – no matter how distasteful it was or whether it would cause offence. The internet was envisaged from the beginning to be an open platform that had the potential to uphold both *isegoria* and *parrhesia*, See "The Two Calshing Meanings of 'Free Speech' by Teresa M. Bejan, The Atlantic, December 2, 2017.

7 Needless to say, large sections of the population were not Roman citizens and speech was severely censored after the Republican golden era —during the reign of the Emperors. Nonetheless, the oratory and speech traditions epitomised by Cicero, and other public figures may just possibly have been some of the first seeds for encouraging speech in society.

8 Keller (n 3).

9 Keller refers to such cases as 'must carry' claims, see Keller (n 3).

10 Keller (n 3).

forums. The platforms should, therefore, have special obligations or a duty of care towards users who generate speech and content on their platforms. Moreover, it has been pointed out that major platforms are akin to monopoly utility providers which provide the essential infrastructure for speech to be enabled online.[11] Some also argue that platforms, which act as public forums, effectively stand in the shoes of the State and accordingly have to assume the State's duties towards its citizens.[12] These are persuasive and compelling arguments on both sides of the divide.

Setting legal niceties aside, even though platforms are privately controlled spaces, they *de facto* set new norms in society. Platforms have assumed essential social and community functions—they have become today's public forums. Whether President Trump's Twitter feed, or Assange's Wikileaks disclosures, or Private Eye, Trevor Noah's and Bill Maher's satirical platform presence or Taylor Swift's posts, all demonstrate how platforms have transformed into the primary public forums for information, free speech and artistic expression.

Governments have come up with new regulatory proposals for privately controlled platforms virtually overnight in contrast to their traditional hands-off approach to platform regulation. The Internet Safety Report in the UK,[13] the EU Directive on Copyright in the Digital Single Market[14] the US President's Memorandum on Combating Trafficking in Counterfeit and Pirated Goods,[15] The Protection from Online Falsehoods and Manipulation Act in Singapore[16] and a slew of other regulatory proposals, were produced within an extraordinarily short space of time. Some of these regulatory proposals were driven by public demand and concern about the proliferation of unregulated 'harms' for which social media platforms have acted as windows to the world.[17]

Such public concerns are present and clear. Bad Actors are exploiting technology in multiple ways: posting child pornography; exchanging terrorist messages; texting hate speech; spreading fake news; interfering in elections; promoting hate crimes, or by harnessing and misusing private data of unsuspecting consumers. Ironically, Bad Actors engage in their nefarious activities while wrapping themselves in the protective cloak of free speech. They are also masters at weaponising technology and use it smarter and more efficiently than Good Actors. A case in point is the ruthlessly efficient way in which Bad Actors flood online marketplaces and platforms with pirated works and counterfeit goods. Their success in churning out perfect copies at unprecedented volume and speed stands in stark contrast to the slow and faltering efforts of Good Actors attempting to use technology to authenticate their product through supply chains and online distribution platforms.

These concerns and challenges raise the thorny issue of whether regulation may be an effective response to the smart use of technology by Bad Actors in the digital world. Regulation intuitively goes against the very grain of the prime directive of the original dreamers of the digital age who built the internet. Digital pioneers John Postel, Sir Tim Berners-Lee, and Vinton Cerf postulated a free and unfettered cyberworld—a glorious environment where information flows freely, where the right to know is a given, where scientific collaboration is easy, where you can express your opinions without censure, and where innovation and free competition allow you to set up an online business that knows no boundaries or borders.[18] So how then to reconcile that which is potion, with that which is poison? It is indeed dispiriting

11 UK House of Lords, Select Committee on Communications, Regulating in a Digital World, 9 March 2019, at 44 paras 169 and 171, also noting that Mark Zuckerberg has spoken of Facebook as a 'social utility'. <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>. See also Keller (n 3 at 16).

12 Keller (n 3 at 15).

13 <https://www.gov.uk/government/consultations/online-harms-white-paper>.

14 <http://www.europarl.europa.eu/doceo/document/TA-8-2019-0231_EN.html?redirect>.

15 <https://www.whitehouse.gov/presidential-actions/memorandum-combating-trafficking-counterfeit-pirated-goods/.

16 Passed into law on 8 May 2019. The law prohibits false statements against the public interest and can be applied to websites, platforms including social media. It should also be noted that an eSafety Commissioner has been in operation in Australia since 2015 to deal with cyberbullying, image-based abuse and illegal content to protect Australians but in particular children.

17 As observed by the UK House of Lords report (Select Committee on Communications, Regulating in a Digital World, 9 March 2019, at 5): 'Public opinion is growing increasingly intolerant of the abuses which big tech companies have failed to eliminate'. <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>

Beyond clearly illegal content and activity, online 'harms' - which have been enumerated in recent UK Government reports - include: 'cyberbullying against children, women, minorities, the LGBT community, and disabled individuals, misogynistic abuse online, bullying, trolling, online harassment of those in public life, online disinformation on public health issues such as anti-vaccination, messaging on self-harm and suicide involving teenagers, generating fake content "deepfakes" and personal data being abused in digital political campaigning.' See UK Government, DCMS Online Harms White Paper, 8 April 2019,

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>, UK House of Lords, Select Committee on Communications, Regulating in a Digital World, 9 March 2019, <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>.

18 Communication with Maria Fredenslund, Executive Director, RettighhedsAlliancen, on 1 April 2019: 'Maybe part of the explanation of why the internet is so unregulated is that we had decades where regulators did not want to regulate the internet because they were so afraid to

that the boundless freedom of a utopian internet has brought forth some primeval human instincts of dark and dystopian virtual spaces where there is no rule of law. A borderless *laissez-faire*, free-for-all cyberspace only served to virtually showcase, in some instances, the worst in human behaviour. Also, we have to contend with the Dr Jekyll and Mr Hyde phenomenon. Some users, because of the-anything-goes culture on the internet, have ventured into faceless activities online which they would never have contemplated engaging in the offline world. Aberrant behaviour of this nature flies in the face of the principle of parity—that the fundamental rule of law principles should equally apply in the real world and in cyberspace.[19]

There can, of course, be no doubt that digital technology is arguably humankind's greatest achievement since the invention of the printing press. Thanks to Big Tech and the advent of platforms such as Facebook, Twitter, WeChat, Amazon and Google, the way we live, search for things, shop, communicate, and even woo each other have changed fundamentally.[20] Digital technology has freed up our time from manual tasks; it enables us to keep in touch globally and to be informed on a scale never experienced in history. But as we open our houses to ever more interconnected technology, as governments ponder the idea of 'smart cities', and as the hunger for convenience and speed push caution to one side and increase our attack surface, the same technology we are embracing is being turned against us.

How then does one reconcile these seemingly irreconcilable universal issues in our new world? The underlying issues are all of fundamental and equal importance and form the cornerstone of democracy. On the one hand are the demands of freedom of speech, innovation and competition and, on the other are the protection of victims and society against child pornography, safeguarding national security, preventing hate crimes, and stopping the abuse and harvesting of private data. Bright-line demarcations may well be apparent in many cases between clear illegal activities on platforms by Bad Actors versus creative, free speech expressions by Good Actors. But, in many other situations, a careful, proportionate and appropriate balancing of fundamental interests will be required. An absolutist starting point on either side of this equation is unreasonable and unrealistic.

An even more significant and more pressing issue within the digital environment is the unprecedented volume and frequency of online criminal activity. Courts and legislatures around the world have become woefully inadequate in attempting to contain the full flow of online actions by Bad Actors. The law has traditionally lagged behind commercial and technological development and the courts are playing catch-up as they try to deal with the explosively rapid pace of technological development, as foreseen by Moore's Law.[21] It makes no sense, for example, for a content holder to run to court—at great expense—to stop the single sale of pirated content on a digital platform as the actual listing typically appears online for only a few hours. Moreover, such court action does nothing to address the multitude of other fake listings or pirated live streamings set up by other Bad Actors on platforms. The same holds for the avalanche of hate speech, child abuse and fake news listings going viral on platforms and made even more challenging by ephemeral apps such as Snapchat.

Setting aside the obvious benefit of anonymity for online free speech activists living under repressive regimes, anonymity is the root cause of nefarious activity on the internet. The mask of anonymity allows Bad Actors to evade detection. Only if the wrongdoing is systematically tracked and traced to the source—from the digital world to a physical location in the real world—can enforcement make any substantive headway. Although it seems logical to stop the toxic flow of harmful postings at the distribution point of the gatekeepers—the platforms—this is as successful as trying to make a river reverse its flow at the estuary.

The volume and velocity of the toxic flow of illegal content contribute to the size of the problem. How does one police the endless flow of illegal detritus in the virtual world without boundaries between countries? The digital age has changed the very nature of the threat of illegal activity. Issues specific to nefarious online activities means that illegal content can be accessed at the click of a button. Unlike the off-line distribution of criminal spoils which requires physical activity, digital technology allows an internet user to access/download/stream illegal

harm innovation. The idea was that internet should be this free flow of data with no restrictions. . . this ideology formed our idea of the internet and maybe therefore it took a while before we realised that freedom lies in regulation – also online.'

19 See also UK House of Lords, Select Committee on Communications, Regulating in Digital World, 9 March 2019, at 3, 8 and 15: ' . . . a large volume of activity occurs online which would not normally be tolerated offline'. <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>.

20 The Global Digital Enforcement of Intellectual Property, WIPO Magazine, September 2018, <https://www.wipo.int/wipo_magazine/en/2018/si/article_0005.html>.

21 By which the number of transistors per square inch on integrated circuits has doubled every year since they were invented although this exceptional pace is coming to an end - <https://www.sciencefocus.com/future-technology/when-the-chips-are-down/>, but see: <https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/ for a more optimistic view>.

content instantly. Once viewed, the illegal material can be processed, stored and disseminated globally.

Existing solutions in the digital environment are often subject to intractable challenges. First, the identity of the illegal content up-loader is often unknown to the victim or authorities; second, the anonymity problem exacerbates the 'whack a mole' phenomenon—where one online listing is taken down and another one pops up under a different URL almost instantly as the Bad Actors themselves evade identification; third, the sheer volume and velocity of postings of illegal content make online listings very time sensitive—they are typically posted for a few hours or days only, making timely online tracking and tracing of illegal listings extremely difficult; fourth, Bad Actors typically use more than one server in different countries. This raises questions of international jurisdiction; and fifth, there is no uniform, international mechanism for delisting and redlisting online Bad Actor identities.[22]

Therefore, if we are to address the great digital challenges of our time, a global, holistic solution, not unlike the universal collaboration around climate change, is required.[23] The internet by its nature is global and requires a worldwide solution engaging all of humankind. Examples of productive global cooperation are the calling into life of the WePROTECT Global Alliance (established to tackle Child Sexual Exploitation and Abuse at a global level), the Global Internet Forum to Counter Terrorism (on global counter-measures), and the Code of Practice for Consumer IoT Security (creating the first globally-applicable security industry standard for the Internet of Things)[24]. What makes the first initiative noteworthy is that various stakeholders were involved by bringing together government, law enforcement, industry and civil society in a transparent way.[25] Consistent with local law, there may well be instances where government may feel obliged to set some rules for online action to protect its citizens. The chances are though that many of these rules will be shared as natural law outflows - common to all humankind in cyberspace. At the end of this spectrum, purely regional efforts (although well-intentioned) tackling only local fragments of the internet, may very well be counter-productive[26] as such efforts pull into different directions and weaken initiatives. Cyber-crime police units and others who grapple daily with enforcement activities can point to the vast volume of cross-border, international follow-throughs they have to constantly pursue. Moreover, without a shadow of a doubt, the most effective and cost-efficient technological solutions across borders are uniform codes and not fragmented local fixes.

It is therefore clear that the key to solving this global problem will be achieved through a universal, collaborative effort on the part of all stakeholders which should include private platforms, governments, rights holders, users and other experts and interested groups in the relevant sectors.[27] The stakeholders will need to develop uniform guidance at international Summits with full transparency. Experience dictates that for this to work, a clear and consistent set of global rules need to be established—a type of *ius gentium*, natural law or Law Merchant in the form of a universal body of customary rules.[28] Business requires certainty and bright line demarcations. Clear guidelines promote certainty—and certainty, it is submitted, is one of the cornerstones of online justice. The pronouncement of Justice Peterson aptly applies in this context: 'I've always believed that certainty is the most important factor in the law … Most people like to know what the law is, so that they can now

22 See WIPO Study on IP Enforcement Measures, Especially Anti-Piracy Measures in the Digital Environment, Frederick Mostert and Jane Lambert, in press, September 2019.

23 The global solution approach was emphasized in the vision statement of the recent UK Government's White Paper, UK Government, DCMS Online Harms White Paper, 8 April 2019, at 6 : 'A global coalition of countries all taking coordinated steps to keep their citizens safe online' and " the threat posed by harmful and illegal content and activity online is a global one . . . ' at 38 and also at 39: ' The approach proposed in this White Paper is the first attempt globally to tackle this range of harms in a coherent, single regulatory framework.' <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>

As noted, in the House of Lords Report on Regulating in a Digital World: ' Regulation of the digital environment is fragmented with overlaps and gaps . . . We recommend the development of a comprehensive and holistic strategy for regulation.' UK House of Lords, Select Committee on Communications,, 9 March 2019, at 3.

24 See UK Government, DCMS Online Harms White Paper, 8 April 2019, at 84 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf >.

25 It may well be argued that ACTA (Anti-Counterfeiting Trade Agreement), PIPA (Protect IP Act) and SOPA (Stop Online Piracy Act) failed significantly due to a lack of transparency among other reasons.

26 As pointed out in the House of Lords Report on Regulating in a Digital World: 'In the long-term regulatory fragmentation threatens the cohesiveness and interoperability of the internet, which has developed as a global and borderless medium . . . Global action also makes domestic measures more effective.' UK House of Lords, Select Committee on Communications, 9 March 2019, at 10.

27 This crucial point was emphasized in the UK Government's White Paper on Online Harms, 8 April 2019, at 95 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>.

28 Akin to the *ius gentium* during the Roman Law period as a universal set of customary rules (known as natural law - *ius naturale* - 'what reason has established among all people' as per the jurist, Gaius, Digest 1.1.9). Also see the Law Merchant or Lex Mercatoria operating in the same way during the medieval period. The Lex Mercatoria evolved as a system of custom and best practice and functioned as the *de facto* rules for the international law of commerce. Some argue that a modern manifestation of the lex mercatoria can be seen in the dispute resolution procedure used in cyberspace to resolve domain name disputes. On this point, see the text at n 33 below.

know what they can and cannot do.'[29] Consequently, global guidance needs to focus on uniform digital tools and administrative measures inclusive of due process and proportionality to combat the volume and velocity of illegal content on private platforms. As a starting point, the primary focus should be aimed at the hard-core areas of clear-cut cases of illegal online content (with no or little free speech issues) such as child pornography, fake pharmaceuticals, pirated works and terrorist recruitment. Such clear-cut areas of fundamental universal human values among nations could be the obvious touchstone for developing universal digital tools[30] in conjunction with administrative measures.[31] Examples of potential universal digital tools and administrative measures include blocking, filtering, domain name tracing, Bad Actor listings, digital authentication via Blockchain, Big Data Analytics on criminal content and measures such as notice and takedown, notice and staydown and online public awareness initiatives.[32] The effective use of administrative measures in the digital era is exemplified by the speedy and cost-effective procedures specifically set up on a global basis to deal with the volume of cybersquatting by a United Nations Agency, the World Intellectual Property Organisation (WIPO). The Uniform Dispute Resolution Policy (UDRP) was developed by WIPO through an independent panel to represent different stakeholders around the world. Although the arbitration process of the UDRP has been updated at times to deal with issues, the system as a whole has functioned well internationally. This UDRP has been referred to as an example of the Law Merchant in operation in cyberspace.[33]

Free speech defences are more nuanced but this inherent challenge must not impact the vigour with which this fundamental human freedom should be safeguarded on the internet.[34] Guidelines are urgently needed to ensure that digital tools in conjunction with administrative measures are employed with discretion and proportionately by platforms. A genuine concern is the significant chilling effect some digital tools may have on free speech—such as over-blocking and excessive filtering by platforms.[35] Over-blocking and excessive filtering could too easily lead to censorship.[36] Platforms may at times be tempted to err on the side of caution and resort to over blocking or filtering to avoid possible liability from content holders.[37] Free expression and artistic creations and user generated content such as news commentary, criticism, informative and educational works, parody and other transformative works require protection online. Stakeholders should with equal commitment develop uniform guidance at international Summits.

As Sir Tim Berners-Lee points out, a Magna Carta of the online world requires development.[38]

29 Justice Edwin J Peterson of the Oregon Supreme Court—see Paul E Loving, The Justice of Certainty, 73 OreLRev 743 (1994).

30 See in this context the World Intellectual Property Organisation's Study on IP Enforcement Measures, Especially Anti-Piracy Measures in the Digital Environment, Frederick Mostert and Jane Lambert, (in-press September 2019) and the proposed 'RESIST' toolkit to enable organisations to develop a strategic counter-disinformation capability - announced by the UK Cabinet Office on 8 April 2019, see <https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws> . Technology is specifically earmarked as part of the solution in by the UK Government in its recent White Paper: UK Government, DCMS Online Harms White Paper, 8 April 2019, at 6 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>.

31 A step in this direction can be found in the 'Budapest Convention on Cybercrime', Budapest, 23 November 2001, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185C>. Codes of practice, overseen by a regulator, is also foreseen UK Government, DCMS Online Harms White Paper, 8 April 2019, at 9 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>.

32 See WIPO Study on IP Enforcement Measures, Especially Anti-Piracy Measures in the Digital Environment, Frederick Mostert and Jane Lambert, in press, September 2019.

33 See: <https://en.wikipedia.org/wiki/Lex_mercatoria>.

34 See also UK House of Lords, Select Committee on Communications, Regulating in a Digital World, 9 March 2019, at 18 <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>.

35 See for example UK House of Lords, Select Committee on Communications, Regulating in a Digital World, 9 March 2019, at 51 at para 192 <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>.

36 As noted in the UK House of Lords' report: 'Many legal experts felt that too much power had been delegated to private companies to act in effect as censors.' (UK House of Lords, Select Committee on Communications, Regulating in a Digital World, 9 March 2019, at 57 at para 216).<https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>.

37 A possible solution to provide a balanced approach may lie in the new proposed art 17 of the EU Directive on Digital Single Market. Art 17(9) in particular, provides users with rights to enforce against platforms which unduly block or filter their speech in relation to parody, criticism, quotation, pastiche and other transformative, creative speech content. There is also an analogy to be found with the 'unjustified threats action' provisions of the UK Intellectual Property (Unjustified Threats) Act 2017 which essentially prevents overreaching 'cease and desist' letters to be directed by holders of patent, trade mark or design rights to potential infringers.

38 See Sir Tim Berners-Lee's statement to this effect: <https://webfoundation.org/2015/11/consumers-international-and-web-foundation-team-up-to-advance-rights-of-internet-users/>. The Magna Carta in cyberspace is based on 9 principles. The 'Principles of the Contract for the Web' include – 'Governments will: ensure everyone can connect to the internet, keep all of the internet available, all of the time, respect people's fundamental right to privacy; Companies will: make the internet affordable and accessible to everyone, respect consumers' privacy and personal data, develop technologies that support the best in humanity and challenge the worst; Citizens will: be creators and collaborators on the web, build strong communities that respect civil discourse and human dignity, fight for the web'.