Childhood in the digital age: a socio-cultural and legal analysis of the UK’s proposed virtual legal duty of care

<table>
<thead>
<tr>
<th>Journal:</th>
<th>International Journal of Law and Information Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuscript ID</td>
<td>Draft</td>
</tr>
<tr>
<td>Manuscript Type:</td>
<td>Article</td>
</tr>
<tr>
<td>Keyword:</td>
<td>White Paper, duty of care, regulation, childhood, digital space, children, cyberspace, judicial review, human rights</td>
</tr>
</tbody>
</table>

http://mc.manuscriptcentral.com/ijlit
Childhood in the digital age: a socio-cultural and legal analysis of the UK’s proposed virtual legal duty of care

ABSTRACT

In 2019, the UK government issued an ambitious White Paper to regulate ‘online harms’. This article adopts a socio-cultural and legal approach to analyzing the proposed law in the context of children. How childhood is conceptualized influences public policy and legal interventions, including on the digital space. This remains contested terrain with different conclusions effects on the effects of the cyberspace. The biggest challenge with intermediary legal interventions on the digital realm is the need to achieve a balance between protection and participation rights of children. The dominant conception of childhood as a period of vulnerability has meant ‘protection’ often overrides participation rights. However, such focus is the subject of challenge, with some suggesting that regulation is the product of moral panic. A further strand is the potential of disproportionate punitive measures against internet companies against the backdrop of human rights obligations. The UK proposition is discussed within these socio-cultural and legal contexts with objective of highlighting challenges and legal pitfalls.

Key words: White Paper, duty of care, regulation, childhood, children, digital space

INTRODUCTION

Digital technology has transformed the world – and as an increasing number of children go online around the world, it is radically changing ‘childhood.’ 1 The pace with which networked and online media and information technologies have become embedded in children’s lives ‘has been overwhelming, triggering a revival of public hyperbole about media-related opportunities and risks, along with a burgeoning of argumentation and experimentation among social researchers keen to explore the significance of ‘the digital age’ for children and childhood’. 2 Young children growing up in the digital world of the twenty-first century have access to a wider range of information communication technologies (ICT) and engage with this technology at a younger age than ever before. 3 In fact, technology is becoming a normal part of young children’s daily existence. As such, in varying degrees, the digital space is reshaping the ‘traditional interests of childhood studies – identity, friendship, learning, family, play, disadvantage, risk and beyond’. 4

---

4 S Livingstone and A Blum-Ross, ‘Researching children and childhood in the digital age’. Available in LSE Research Online: January 2017, p.2

http://mc.manuscriptcentral.com/ijlit
ICT forms a valuable learning tool and gives children access to a world they have not previously experienced. However, a conflict now exists between the child’s right to access the opportunities it creates and the child’s right to be protected from harm. There is growing body of evidence on of harmful content and activity that people experience online. The UK government posits that online services can be used to spread terrorist propaganda and child abuse content, they can be a tool for abuse and bullying, and they can be used to undermine civil discourse. Despite the many benefits of the internet, more than one in four adult users in the UK have experienced some form of harm related either to content or interactions online.

As numerous cases over the years have demonstrated, severe harm can manifest itself as much in mental distress as in real physical injuries, including self-harm and suicide. Major areas of concern in terms of harm include pro-eating disorder and pro-suicide websites as well as cyberbullying and online child sexual abuse and exploitation.

In 2019, the UK government published White Paper (UK WP) which sets out a programme of action to tackle content or activity that harms individual users, particularly children, or threatens the way of life in the UK, either by undermining national security, or by undermining the shared rights, responsibilities and opportunities to foster integration. Increasing public concern about online harms has, according to the UK WP, prompted calls for further action from governments and tech companies. In particular, as the power and influence of large companies has grown, and privately-run platforms have become akin to public spaces, some of these companies now acknowledge their responsibility to be held to norms and rules developed by democratic societies. Critically, the government intends to impose a ‘duty of care’ on the companies. A virtual duty of care would appear to be a first in internet governance. There is currently a range of regulatory and voluntary initiatives aimed at addressing these problems, but these have not gone far or fast enough, or been consistent enough between different companies, to keep UK users safe online. The government noted that international partners were also developing new regulatory approaches to tackle online harms, but none had yet established a regulatory framework that tackled the range of online harms it seeks to tackle. The UK, the government claims, will this would be seminal. The range of harms it seeks to combat is indeed quite wide. It includes child sexual exploitation, terrorism and radicalisation, content illegally uploaded from prisons, serious violence online, gang violence, sale of opioids, online harms suffered by children and young people, cyberbullying, self-harms and suicide, underage sharing of sexual imagery.

8 UNICEF Report, Children in a Digital World, 2017
9 See ‘Online Harms White Paper’ Presented to Parliament by the Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department by Command of Her Majesty April 2019 (hereinafter ‘UK Online Harms White Paper 2019’)
10 UK Online Harms White Paper 2019, para 13
(sexting), ‘emerging challenge of screentime’; online disinformation (fake news) online manipulation and abuse of public figures.

The new statutory duty of care is intended to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services. Compliance with this duty of care will be overseen and enforced by an independent regulator. The government, nonetheless, acknowledges that this ‘novel’, ‘ambitious’ and a ‘complex’ area for public policy and it will consult further on the new regulatory framework and non-legislative package. The transnational nature of the internet poses problems in enforcing regulation, including conflicts of law, confusion about which jurisdiction applies and in seeking redress against foreign actors. The delicate balance between protection and observing human rights is delicate.

This paper discusses some the legal implications of the proposed law in particular the duty of care on internet companies. This paper adopts a socio-legal approach to analyzing the proposed law in the context of children. While the law proposes to protect different categories, it is evidently primarily concerned with the protection of ‘children’, a word mentioned 193 times in 102-page White Paper. How childhood is conceptualized influences public policy and legal interventions, including on the digital space. This remains contested terrain with different conclusions on the effects of the cyberspace. The biggest challenge with intermediary legal interventions is the need to achieve a balance between protection and participation rights of children. The hegemonic conception of childhood perceives it as a period of vulnerability. Resultantly, ‘protection’ often trumps participation rights. However, such focus is the subject of challenge. Others suggest the ‘media effects’ are not universal. Different children can have the similar experience online and yet experience very different outcomes. A further conundrum in internet governance is the potential of disproportionate punitive measures against internet companies against the backdrop of human rights obligations. The UK proposition is discussed within this context with objective of highlighting potential legal pitfalls.

The paper is organized as follows. The first section discusses the development of the relationship between children and the digital space. The second part explores the sociology of childhood in the digital age; it discusses how the cyberspace has changed the conception of childhood in the cyberspace and human rights era. The third section discusses the proposition of the ‘virtual legal duty of care’ and challenges in enforcement. The forth section deliberates on the potential challenges of the decisions of the regulator through judicial review. Lastly, the final part gives a sample of ECHR cases on the digital space and human rights.

---

11 UK Online Harms White Paper 2019, para 17
12 UK Online Harms White Paper 2019, para 49
13 UK Online Harms White Paper 2019, paras 10.2, 40
CHILDREN AND DIGITAL SPACE

Until recently, analysis of children’s experiences, social relations and lifeworlds implicitly prioritised face-to-face, physically collocated communication as the primary means through which their everyday lives are constituted and, therefore, the primary means through which research with children is to be conducted. Traditionallly, communication research had focused on parental efforts to mitigate deleterious effects of media on children. Findings suggested a limit to television viewing time, cautioned that television influenced children’s desires for commercial products. Parental role modeling was a significant component of a child’s socialisation into media use. Researchers used the concept of “parental mediation” as the indicator that parents take an active role in managing and regulating their children’s experiences with television.

Digital technology has transformed the world – and as an increasing children go online around the world, it is increasingly changing the notion of ‘childhood’. Thus, it has become necessary to rethink the role of media in family life. The parental mediation prism has been disrupted. Children and young people who have grown up with the technological innovations are popularly dubbed the ‘digital natives’ of a changed communication landscape that is still evolving and only partially understood. As children grow, the capacity of digitalisation to shape their life experiences grows with them, offering seemingly limitless opportunities to learn and to socialize, to be counted and to be heard. The offline/online binary has been transcended by the diversity of communicative modes and settings that now make up children’s daily lives.

22 L S Clark, ‘Parental Mediation Theory for the Digital Age’ Communication Theory (2011)21 (4)
24 UNICEF Report, Children in a Digital World, 2017
As children’s daily lives become ever more heavily mediated, and as the media themselves simultaneously converge and diversify, researchers along with policy-makers and the public are now debating whether ‘the digital age’ is enhancing or undermining children’s rights, with current controversies centring on children’s right to privacy online as offline, to information and freedom of expression, and to protection from sexual and aggressive threats variously mediated and amplified by the internet.  

Scholars in media and communication, like in the ‘TV era’, discuss these developments in the context of ‘media effects’, a contested terrain. Some of the impacts of digitalisation on children’s well-being are not universally agreed. There is a subject of growing public debate among policymakers and parents alike. There does seem to be a convergence of opinion, though, on the fact that, if leveraged appropriately and made universally accessible, digital technology can be a game changer for children being left behind – whether because of poverty, race, ethnicity, gender, disability, displacement or geographic isolation – connecting them to a world of opportunity and providing them with the skills they need to succeed in a digital world.  

The utility of the internet is aptly expressed in the UNICEF report *The State of the World’s Children — Children in a Digital World*:

> To be unconnected in a digital world is to be deprived of new opportunities to learn, communicate and develop skills for the twenty-first century workplace. Unless these gaps in access and skills are identified and closed, rather than being an equalizer of opportunity, connectivity may deepen inequity, reinforcing intergenerational cycles of deprivation.

For the so-called ‘digital natives’ – utilising social media for social activism is practically second nature. The internet can be a powerful force for good. It serves humanity, spreads ideas and enhances freedom and opportunity across the world. Online services facilitate the exchange of information, goods and services. They match supply and demand with great efficiency, increase consumer choice and lower distance between participants.  

Nonetheless, there seems to be some acceptance that digital technology and interactivity pose significant risks to children’s safety, privacy and well-being, magnifying threats and harms that many children already face offline and making already-vulnerable children even more vulnerable. Even as ICT has made it easier to share knowledge and collaborate, so, too, has it made it easier to produce, distribute and share ‘harmful material’, which exploits and abuses

---

28 UNICEF Report, Children in a Digital World, 2017,  
31 UK Online Harms White Paper 2019 para 1.2  
32 UNICEF Report, Children in a Digital World, 2017
children. Their whole private lives may be exposed to the marketing machine, which will not only watch and record what a child is doing but also reconstruct and manipulate the online social environment in ways that impact the child’s sense of self and security. Collecting personal data is now seen by companies as ‘business critical’. It has even been suggested that the most valuable resource for business today is not oil but data. Children are a highly marketed segment of the consumer population, and young people often serve as information brokers for their own personal information as well as data about their friends. The so-called ‘Big Data’ involves ways in which organizations, including government and businesses, combine diverse digital datasets and then use statistics and other datamining techniques to extract from them both hidden information and surprising correlations. For businesses, children can be important targets as sources of data because they influence their friends’ and families’ consumer decisions. Some may also be significant consumers themselves – both today and, crucially, in the future, when investment in securing their brand loyalty may really pay off. The gaze of cookies and Web bugs that are posted during online sessions facilitate collection, storage, and data matching. ‘Behavioural’ advertising, targeting online ads to specific behaviours, as well as other advertising techniques, can contribute to the growing commercialization of childhood.

These harms, which include Child Sexual Exploitation and Abuse (CSEA), have prompted regulatory measures to combat their abuse. However, others suggest the ‘media effects’ that have catalysed such action are not universal. The perception of vulnerability has held sway in childhood discourse. This position has been critiqued and supplemented by work which describes how children and young people use the internet in ways which reflects their agency. Different children can have the similar experience online and yet experience very different

---

33 UNICEF Report, Children in a Digital World, 2017
34 UNICEF Report, Children in a Digital World, 2017
35 Centre for Economics and Business Research, ‘The Value of Big Data and the Internet of Things to the UK Economy’ SAS:(2016); T Cooper & R LaSalle, ‘Guarding and Growing Personal Data Value’, Accenture Consulting Co
outcomes. What also remains contested is the action to be taken given the benefits and harms of the cyberspace, and if enacted, balancing the rights of parties involved.

It is against this backdrop that this article analyses White Paper published by the UK government in April 2019 proposing the regulation of the internet. Notably, the UK already has some regulation which covers the internet. Criminal and civil law generally applies to activity on the internet in the same way as elsewhere. For example, section 1 of the Malicious Communications Act 1988 prohibits the sending of messages which are threatening or grossly offensive; it applies whether the message is through the post or through any form of electronic communication. There is also legislation which specifically targets online behaviour, such as the Computer Misuse Act 1990. Several regulators have responsibilities for activities which are particularly relevant to the online environment. But no regulator has a remit for the internet in general and there are aspects of the digital environment, such as user-generated content, for which no specific regulator is responsible.

The government also has a ‘Digital Charter’, an ongoing programme of work aiming to make the UK the safest place in the world to be online. The UK WP notes that the current range of regulatory and voluntary initiatives aimed at addressing online problems, has not gone far or fast enough, or has it been consistent enough between different companies, to keep UK users safe online. In another report, the House of Lords Committee points out that in the long-term, regulatory fragmentation threatens the cohesiveness and interoperability of the internet, which has developed as a global and borderless medium.

The UK legal initiative is backed by an impressive weight of authority and data drawn from interest groups researchers and scholars as well as justificatory moral claims. Nearly nine in ten UK adults are online and adult users spend around one day a week on the internet. This is also true for children and young people, with 99% of 12-15-year-olds going online, spending an average of twenty and a half hours a week on the internet. The paper noted a growing threat presented by online CSEA. In 2018, there were over 18.4 million referrals of child sexual abuse material by US tech companies to the National Center for Missing and Exploited Children (NCMEC). Of those, there were 113, 948 UK-related referrals in 2018, up from 82,109 in 2017. In the third quarter of 2018, Facebook reported removing 8.7 million pieces of content globally for breaching policies on child nudity and sexual exploitation. Not only is the scale of

---

44 For detailed analysis, see L Edwards Law, Policy and the Internet, by Law, Policy and the Internet (Hart 2019)
50 NCMEC report. Available at: http://www.missingkids.com/footer/media/vnr/vnr2
this offending increasing, so is its severity. The internet Watch Foundation (IWF) estimates that 55% of the child sexual abuse material they find online contains children aged ten or under, and 33% of this imagery is in the most serious category of abuse.\textsuperscript{52} In 2017, the IWF assessed 80,319 confirmed reports of websites hosting or linking to images of child sexual abuse. A total of 43% of the children in the images were aged 11-15 years old, and 57% were ten years old or younger. Two per cent were aged two or younger.\textsuperscript{53}

It has become far much easier for bullies, sex offenders, traffickers and those who harm children to contact potential victims around the world, share images of their abuse and encourage each other to commit further crimes. The cyberspace has made children more accessible through unprotected social media profiles and online game forums. It also allows offenders to be anonymous – reducing their risk of identification and prosecution – expand their networks, increase profits and pursue many victims at once. Terrorist groups are finding new ways to spread propaganda and evade government and law enforcement efforts. These threats are not only restricted to the largest, best-known services, but are prevalent across the internet. Terrorist groups and their supporters constantly diversify their reliance on the online services they use to host their material online.\textsuperscript{54}

Rival gangs, the paper notes, utilise social media to glamourise weapons and gangsterism, as well as to directly depict or incite acts of violence. Apart from the illegal sale of weapons to young people online, online gangsterism is seen as a contributing factor to incidents of serious violence, including knife crime, in the UK. The latest police recorded crime figures, for the year ending September 2018, show an 8% increase in knife crime (to 39,818 offences) compared with the previous year. Homicide figures have risen by 14% (excluding terrorist attacks) over the same period.\textsuperscript{55} These misdemeanors have been linked to the cyberspace.

The UK government notes that many companies claim to hold a strong track record on online safety. However, in actuality, there is limited transparency about how they implement or enforce their policies. There is a persistent mismatch with users’ experiences: 70% of Britons believe that social media companies do not do enough to curtail illegal or unethical behaviours on their platforms.\textsuperscript{56} About 60% of respondents to the government’s Internet Safety Strategy Green Paper consultation claimed they had witnessed inappropriate or harmful behaviour online; only 41% thought their reported concerns were taken seriously by social media companies.\textsuperscript{57} The government thus found sound justification to intervene by stabiling a statutory duty of care to be enforced by an independent regulator.

\textsuperscript{52} See Internet Watch Foundation Annual Report 2017. Available at: https://annualreport.iwf.org.uk/
\textsuperscript{53} See Internet Watch Foundation Annual Report 2017. Available at: https://annualreport.iwf.org.uk/
\textsuperscript{54} UK Online Harms White Paper 2019, para 1.14.
\textsuperscript{57} See ‘HM Government Response to the Internet Safety Strategy Green Paper’ (May 2018)
While the new regulator would be reposed with authority to produce codes of practice, the government expected companies to take action immediately to tackle harmful content or activity on their services. For those harms where there is a risk to national security or to the physical safety of children, the government would publish interim codes of practice. The scope to use the regulator’s findings in any claim against a company in the courts on grounds of negligence or breach of contract. And, if the regulator has found a breach of the statutory duty of care, that decision and the evidence that has led to it will be available to the individual to use in any private legal action.

SOCIOMETRY OF CHILDHOOD IN DIGITAL AGE

The notion of ‘childhood’ is at the centre of the protective impulses. How childhood is conceptualised in a society shapes regulatory policies. On 193 occasions, the UK WP mentions ‘children’ undoubtedly revealing that they were at the centre of the policy formulation. The publication of the UK WP followed a report by the House of Lords committee on the subject. It stated that its earlier report, Growing up with the internet, had found that children were particularly vulnerable to online harms and that, although they were often early adopters of new technology, their welfare is very little considered by tech entrepreneurs. The House Lords argued that this should change to make the internet work better for children. Consideration of children should not just focus on protection. It was also necessary to consider how the internet could meet their needs and be accessible to them. Any principle-based approach to regulation had to recognise children’s rights, their legal status and the concept of childhood. However, childhood is not singular or linear conception. Socio-cultural approaches help in understanding the relationship between lad and culture.

Phillip Aries claimed in the medieval society, the idea of childhood did not exist. After seven year, the ‘child’ was recognized a mini-adult. By about the 15th and 17th century, a child began to be perceived as member of the family who deserved nurturing and protection. Over the last thirty years, researchers have demonstrated how ‘childhood’ is produced not only through the practices of family, schooling, medicine and law, but through the management of children’s participation in or exclusion from different spaces. Still, there are different conceptions of childhood. Different cultures construct childhood variously. Vygotsky theorized that children became enculturated into the social world as they interacted with their parents and with other significant people in their lives. Children’s potential for cognitive development depended upon

58 UK Online Harms White Paper 2019, para 7.3
64 D Archard, Children : rights and childhood (Routledge, London 1993)
65 L Vygotsky, Mind in society: The development of higher psychological processes (Cambridge, MA: Harvard University Press 1978)
access to what he termed the ‘zone of proximate development,’ or the opportunity for children to engage in experimentation beyond their current capabilities.  

A dominant feature of western ideas of childhood since the 19th century has been its association with private rather than public space and the construction of public and adult space as a site of threat to children. Adult perspectives focus on what children will be and not what they are. Children are viewed as passive consumers of a culture already established by adults through socialisation. Parental mediation theory posits that parents utilize different interpersonal communication strategies in their attempts to mediate and mitigate the negative effects of the media in their children’s lives. It also assumes that interpersonal interactions about media that take place between parents and their children play a role in socializing children into society.

The international legal imagination construes children as ‘faultless, passive victims’ lacking agency. This perception, in which the parent has a central role, has informed social policy perspectives at domestic level. The regulation of access to playgrounds or city streets, to bars or cinemas according to age, all served to construct different ideas of childhood and of adult-child relations. An authoritarian approach set out to compel and prohibit certain family behavior. On the other end of the scale is the laissez faire model which eschews state intervention and regards family life as private not warranting legal intervention. The ‘welfare model’ is where ‘the state intervenes, at least with coercive techniques, when clear dysfunctions are evident.’

The quarantining of children into specific spaces such as homes and schools is central to the production and maintenance of the ‘standard model’ of adult-child relations. This model produces specific identities for children, as dependent and vulnerable, and also specific identities for adults as protectors and as competent actors in public space. The welfarist model aims at protecting children who are seen as vulnerable members of society in need of guidance and control. The role of parents, schools, social services and the State is to protect, nurture and provide fulfilling opportunities for children’s development. At the heart of this idea of childhood is the construction of public space as potentially dangerous for children.

---


68 T. Buck International Child Law (Routledge 2014)

69 T. Buck International Child Law (Routledge 2014)

70 Lynn Schofield Clark Parental Mediation Theory for the Digital Age Communication Theory ISSN 1050-3293

71 M. Drumbil Reimagining Child Soldiers in International Law and Policy (Oxford University Press, 2012)


73 L Harding, Family, Sate and Social Policy (Macmillan 1996)

74 T. Buck International Child Law (Routledge 2014) 9

75 T. Buck International Child Law (Routledge 2014)

Throughout 1997, parents were being advised, through advertisements and enticed by special offers, on what computers to buy. The purchasing of computers was portrayed as a natural articulation between children and technology. Children were repeatedly presented as adept at using new technologies and at risk of being disadvantaged by not having access to the Internet. What began as a means of electronic information transmission—room-sized computer to room-sized computer—soon transformed into an omnipresent and endlessly multifaceted outlet for human energy and expression. New gadgets such as laptops and mobile phones were introduced through which they could explore the digital space without effective governance. As Schmidt put it ‘The Internet is the largest experiment involving anarchy in history’. Hundreds of millions of people are, each minute, creating and consuming an untold amount of digital content in an online world that is not truly bound by terrestrial laws.

The emergence of the ‘cyberspace’ dislocated the parent-child relationship even further. As an inevitable consequence of this, there was increasing public anxiety about how children’s participation in digital spaces might be managed. Given the dominant narrative in which children were seen as technologically competent, parents were seen as naïve, and in which the Internet was constructed as a distinctive adult space characterised by the right to complete ‘anything goes’ freedom of speech. This anxiety could be understood as the source of an explosion of discourse surrounding children and the Internet at the turn of the century as the news media identified a potential source of endless concerns with which they might attract and retain their readers. Digital technology is increasingly changing childhood. In varying degrees, the digital space is reconfiguring the traditional interests of childhood studies – identity, friendship, learning, family, play, disadvantage, risk and beyond.

Although there are increasingly more examples of child-centred initiatives that embed children’s insights and experiences at their core, current debates in many parts of the world continue to focus almost exclusively on the risks associated with children’s digital media engagements. Debate results in an overwhelmingly protection-oriented approach to children’s use of technology. However, the rights-based model is designed to support children’s own participation in decision-making and is based on a conception of children having distinct rights that can be asserted, both morally and legally. This approach resonates with the dominant sociological image of the child as a competent, autonomous and active social agent. The UNCRC
places emphasis on children’s agency and, therefore, their access to information, participation, freedom of thought and expression, and freedom of association. The emergence of the rights-based approach and the cyberspace have created a challenge to the traditional familial, welfarist model.

The UK government’s White Paper of 2019 attempts to achieve a delicate balance between the welfarist and human right-based approaches. It expresses recognition the benefits of the digital experience for young people\(^\text{86}\) and rights to free expression and privacy\(^\text{87}\) while justifying protection because of the hazards posed the digital space. The intended imposition of a ‘legal duty of care’ on internet companies is the confirmation of childhood as vulnerable protection. The UK WP posits that the government is considering ways of ensuring digital products and services were designed in a responsible way, with their users’ well-being in mind.\(^\text{88}\)

However, the presumed effects of digital media are sometimes conflicting, bringing into question the relevance of internet governance or the character of the regulatory measures. As children spend more and more time on digital devices, families, educators and children’s advocates are growing more concerned – if not more confused – by the lack of consensus among experts on the rewards and risks of connectivity.\(^\text{89}\) Parents struggle with conflicting messages on limiting screen time, on the one hand, or getting the latest device so their children can keep up, on the other.\(^\text{90}\) A recent research by internet Matters found that seven in ten parents thought screen time was essential for their children’s learning development while two thirds felt that devices gave their children another outlet for creativity, particularly so for children aged 6-10.\(^\text{91}\) Yet an Ofcom’s *Children and parents: Media use and attitudes* report 2018\(^\text{92}\) notes that parents and carers were increasingly concerned about the internet, and were finding controlling screen time harder. Fifty per cent of parents were concerned about the data companies are collecting on children and young people’s online activities. They were also worried about children damaging their reputations, the pressures of children to spend money and the possibility of children being radicalised online.\(^\text{93}\) The children’s commissioner for England accused social media companies of losing control of the content carried on their platforms, telling them that recent teen suicides should be a “moment of reflection’ for the way they operate.\(^\text{94}\)

---

\(^{86}\) UK Online Harms White Paper 2019, Box 7  
\(^{87}\) UK Online Harms White Paper 2019, Box 5  
\(^{88}\) UK Online Harms White Paper 2019 para 1,31  
\(^{93}\) UK Online Harms White Paper 2019, para 9.14  
However, some observers note that these articulatory practices, which seek to produce a new common sense about childhood in the face of rapidly changing technological environments, are in evidence both in the spectacular eruptions of the moral panic and in the day to day workings of the new media and policy spheres. Thus in public policy regarding children, the right to protection tends to take priority in theory, policy and practice, now online as, traditionally, offline. But online, once parents have provided access to the hardware and connectivity, protection tends to trump participation in their minds too, especially in risk-averse cultures where even children ‘have inherited a popular discourse that is characterized primarily by fear – if not moral panic [which] potentially inhibits their capacity to imagine and articulate the opportunities digital media affords them’.

While the government’s reaction might be regarded as a ‘moral panic’, the UK WP summons a great weight of evidence to justify the proposed intervention. These are not outlandish concerns. There are, indeed, very real and potentially serious risks associated with children’s use of digital media, particularly for those children who are most marginalised or vulnerable in their communities. Children have been radicalized online, notably the well-publicised case of Shamima Begun who travelled to join the Islamic State in Syria when she was 15. Breck Bednar, a 14-year-old boy who loved gaming, was groomed online and murdered in 2014. Fourteen-year-old Hannah Smith killed herself because of online bullying, according to her father. Molly Russell, 14, took her own life in 2017. When her family looked into her Instagram account they found distressing material about depression and suicide. Molly's father said he believed Instagram was partly responsible for his daughter's death. There a numerous other tragic incidents linked to the internet.

However, observers caution that a narrow focus on risk and safety can negatively impact children’s right to participation and undermine their ability to access the benefits of digital media. Accounts that focus unduly on the dangers posed by the internet frame children as passive, vulnerable consumers of digital culture endangered by the risks of the medium.

---

97 S Livingstone & A Third, ‘Children and young people’s rights in the digital age: an emerging agenda’. Available in LSE Research Online: January 2017
100 A Moore ‘I couldn’t save my child from being killed by an online predator’ The Guardian UK 23 January 2016
discourse portrays children as powerless victims rather resourceful participants\textsuperscript{104}, denying children agency and overlooking the ways in which children use the internet to establish their identities and participate in and extend their social worlds.\textsuperscript{105}

A common assumption is that time spent online will detract from other activities thought to be more valuable, such as face-to-face socializing, reading books or exercising. This is sometimes referred to as the ‘displacement theory\textsuperscript{106}’. The displacement theory offers the idea that online interaction supplants face-to-face interaction, resulting in children and young people having lower social capital and fewer personal acquaintances.\textsuperscript{107} While this hypothesis initially received some support, new evidence suggests that it may be simplistic or even inaccurate today. One reason for this shift is the growing recognition that digital technologies offer many opportunities for children to pursue developmentally valuable activities, and these opportunities are both increasing and improving. For example, some video games positively influence cognitive, motivational, emotional and social development.\textsuperscript{108}

Substantial research shows that risk does not equate with harm and, moreover, that some level of exposure to risk enables children to develop the digital literacy that is necessary to both minimise the potentially negative impacts of their online engagements, as well as unlock more of the benefits.\textsuperscript{109} A UNICEF Report summarized evidence on screen time and its impact on mental well-being, social relationships and physical activity, the debate over digital dependency and, finally, the effects digital experiences have on children’s brains.\textsuperscript{110} The report states:

As the debates continue, one thing is clear: unlimited — and especially unsupervised — connectivity has the potential to cause harm, just as access to the wealth of information, entertainment and social opportunity has the potential to benefit children around the world. So the task is to find ways to provide children with the support and guidance they need to make the most of their online experiences.\textsuperscript{111}

\textsuperscript{104} E Staksrud & S Livingstone, ‘Children and Online Risk: Powerless victims or resourceful participants?’ Information, Communication & Society (2009) 12 (3) pp. 364–387
\textsuperscript{109} L Green, D Brady, K Olafsson, J Hartley & C Lumby, ‘Risks and Safety for Australian Children on the Internet: Full Findings from the AU Kids Online Survey of 9-16 Year Olds and Their Parents. Melbourne’ ARC Centre for Creative Industries and Innovation (2011)
\textsuperscript{110}UNICEF Report, Children in a Digital World, 2017
While the evidence is mixed, recent research shows that children’s use of digital tech has a mostly positive effect. While parents and caregivers may think they are protecting their children by restricting the time spent on digital technology, this may not be the case. Common measures to restrict internet use – by governments, businesses, parents and others – usually take the form of parental controls, content blocking and internet filters. While well-meaning, restrictions may not always achieve their desired objective but may even create unintended negative effects. For example, such measures could cut adolescents, especially, off from their social circles, from access to information and from the relaxation and learning that come from play. Tension around these restrictions can also damage trust between parents and children. And extreme restrictions can hold children back from developing the digital literacy skills needed to critically evaluate information and communicate safely, responsibly and effectively through digital technology – skills they will need for their future.

A report by a government-appointed researcher, Tanya Byron, a psychologist, noted that as a society that adopted a risk-averse approach to childhood, she believed that there was a perception that most children and young people were going to encounter harm online. ‘This is not true. This skewed and unhelpful perception must continually be challenged so that we concentrate our efforts on both helping those who do encounter harm online and developing risk awareness and resilience in all children and young people.’

Equally, different children can have the same experience online and yet experience very different outcomes. One 2009 pan-European survey found a range of responses among children to pornographic content. Some children were not concerned about it, some thought it was funny and others wished they had never seen it. When faced with these types of risks, most children in the study responded with strategies that were either positive (seeking help from others) or neutral (ignoring the risk). Others seemed less able to diminish the risk and ended up, in turn, perpetrating other ‘conduct’ risks themselves.

It is evident the screen time of the TV era has been supplanted by screen time on modern gadgetry; so has the parental mediation approach. However, media and policy debate ‘shows how profoundly disturbing the unsettling of familiar roles remains, and how alluring the idea of the familiar, nostalgic role transposed to online public space continues to be.’ In the new era,

---

119 Ibid
the presumption is that parents who are frequent internet users are more likely to mediate their children’s use than are non-using parents.\textsuperscript{121}

The UNICEF report cautions that without consensus on screen time, it is important for parents, policymakers, researchers and the media not to jump to conclusions about what is healthy or unhealthy digital use.\textsuperscript{122} Considering the full context of a child’s life – together with an emphasis on content and experiences rather than screen time – may prove more useful for understanding the effects of digital connectivity on children’s well-being. Rather than utilising the dominant representation of children as naïve\textsuperscript{123} and assuming they need to be protected from the internet, policymakers need to understand that children have agency\textsuperscript{124} and that their use of the internet is purposeful and informed.

**VIRTUAL LEGAL DUTY OF CARE**

To be clear, internet governance and safeguarding children’s well-being is generally a noble agenda. The introduction of a ‘duty of care’ and making companies duty-holders on digital space is a novelty. Until 1932, there was no precedent that held businesses accountable for the well-being of the users of their products. This changed with the historic “Snail in the Bottle” case.\textsuperscript{125}

In 1928, May Donoghue was given a bottle of ginger beer by a friend. Unbeknownst to her, the bottle contained a dead snail. She drank most of the beverage before she found the snail, and consequently suffered gastroenteritis. Donoghue sued David Stevenson, the ginger beer’s manufacturer, for £500 damages.

This was an unprecedented case. Up to this point, plaintiffs were responsible for proving that negligence breached a contractual agreement. However, because Donoghue hadn’t purchased the beverage for herself, she technically hadn’t entered into an agreement with Stevenson. By ruling in favour of Donoghue, the House of Lords laid the groundwork for legal principles such as negligence and duty of care.

Nowadays, the duty of care manifests in different ways. In different spheres. For instance, employers have a duty of care for their employees; universities have a duty of care for students, health workers for patient and so on. Where children and young people are under the care and/or control of one or more adults, the adult(s) have a duty to take reasonable care to ensure their safety. In 1995, the Young Persons Safety Act 1995 made provision for the regulation of centres and providers of facilities where children and young persons under the age of 18 engage in adventure activities, including provision for the imposition of requirements relating to safety. In 1999 the Protection of Children Act was implemented with a view to increase the level of protection for children by screening those wishing to supervise children. Children Act 1989


\textsuperscript{122} UNICEF Report, Children in a Digital World, 2017


\textsuperscript{125} Donoghue v Stevenson [1932] AC 562
Section 47 places a duty on the local authority to make an investigation if they believe a child in their area is suffering or is likely to suffer from significant harm. The local authority must also decide whether to seek an order, provide services and/or review the case at a later date. Section 17 places a duty on local authorities to provide a range of services for children in need. This means all of the local authority services and includes the provision of daycare services for the under 8’s, as well as support for children who have suffered abuse.

Section 11 of the Children Act 2004 places responsibility on key agencies to safeguard all children and promote their welfare. The act encourages agencies to share early concerns about the safety and welfare of children and to ensure preventative action before a crisis develops. The Childcare Act 2006 provides a legal framework for inspection and regulation of childcare; this includes the Early Years Foundation Stage (EYFS) for early years and childcare provision from birth to 31 August following their fifth birthday and the Childcare Register for services provided for older children and young people. Working Together to Safeguard Children 2018 applies to all organisations and agencies who have functions relating to children. It should be read and followed by strategic and senior leaders and frontline practitioners of all organisations and agencies therein.

There is currently a range of regulatory and voluntary initiatives aimed at addressing these problems, but these have not gone far or fast enough, or been consistent enough between different companies, to keep UK users safe online. In 2019, the UK government published a White Paper which sets out a programme of action to tackle content or activity that harms individual users, particularly children, or threatens our way of life in the UK, either by undermining national security, or by undermining our shared rights, responsibilities and opportunities to foster integration.

A new statutory ‘duty of care’ is designed to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services. Imposing a virtual duty of care while groundbreaking is fraught with challenges. And the UK WP duly recognizes that the introduction of a duty of care for cyber activity is indeed nettlesome. The transnational nature of the internet poses problems in enforcing regulation, including conflicts of law, confusion about which jurisdiction applies and in seeking redress against foreign actors. The delicate balance between protection and observing human rights of both children and the companies is problematic. The potential for tortuous litigation by well-heeled internet companies is ever looming.

The UK WP insists that the private sector – especially in the technology and telecommunication industries – has a special responsibility and a unique ability to shape the impact of digital technology on children. Such power and influence should be leveraged to advance industry-wide ethical standards on data and privacy, as well as other practices that benefit and protect children online. Technology and internet companies were expected to take steps to prevent their networks

---

126 UK Online Harms White Paper 2019, para 49
and services from being used by offenders to collect and distribute child sexual abuse images or commit other violations against children.

As part of the new duty of care, companies will be expected, where appropriate, to have effective and easy-to-access user complaints functions. Companies will need to respond to users’ complaints within an appropriate timeframe and to take action consistent with the expectations set out in the regulatory framework. All companies in scope of the regulatory framework will be require to show that they are fulfilling their duty of care. The ‘ombudsman’ will assess how effectively these terms are enforced as part of any regulatory action. The regulator will have a suite of powers to take effective enforcement action against companies that have breached their statutory duty of care. This may include the powers to issue substantial fines and to impose liability on individual members of senior management. The regulator will set out how to do this in codes of practice. Compliance with this duty of care will be overseen and enforced by an independent regulator.

Enforcing virtual duty of care: possibilities and challenges

The introduction of a legal duty presupposes “negligence”: companies which fail to fulfil the duty of care would presumably be regarded as negligent. While the matters will be decided by a regulator, some principles can be drawn from well-established areas of law. In any case, the decisions will be subject to judicial review or, instead of a regulator, a tribunal could established instead. It is then possible that time-honoured legal principles will be applied to the regulator’s decisions. It is evident that the proposed law draws some of its precepts from other legislation, for example, on health and safety. The regulator will take a risk-based and proportionate approach across the broad range of business types on the internet. The regulator’s initial focus will be on those companies that pose the biggest and clearest risk of harm to users, either because of the scale of the platforms or because of known issues with serious harms. Under the current liability regime derived from the EU’s e-Commerce Directive, platforms are protected from legal liability for any illegal content they ‘host’ (rather than create) until they have either actual knowledge of it or are aware of facts or circumstances from which it would have been apparent that it was unlawful, and have failed to act ‘expeditiously’ to remove or disable access to it. In other words, they are not liable for a piece of user-generated illegal content until they have received a notification of its existence, or if their technology has identified such content, and have subsequently failed to remove it from their services in good time. Under the UK WP proposals, fail to fulfil the legal duty will construed as a dereliction of duty.

Where ‘harm’ or ‘injury’ is caused by such failure, it is possible to draw from the tort of negligence, again within the realm of health and safety. The tort of negligence could give some

---

128 UK Online Harms White Paper 2019, para 25
129 UK Online Harms White Paper 2019, para 18, 38
130 UK Online Harms White Paper 2019, para 20
131 UK Online Harms White Paper 2019, para 17
132 UK Online Harms White Paper 2019, para 6.13
133 UK Online Harms White Paper 2019, para 31
134 UK Online Harms White Paper 2019, para 2.6
guidance, or influence how the regulator would handle cases. For a plaintiff to succeed in a negligence case, the defendant must have owed a duty of care to the plaintiff. Secondly, the defendant must have breached that duty of care. Thirdly, the defendant must have caused the harm to occur, and fourthly, that causation must have resulted in damages. Liability for failing to meet the legal duty of care would only arise if an incident occurs and it can be proved that the risk was foreseeable but no action had been taken to avoid it.

The UK WP observes that under current arrangements, individuals can, in principle, obtain remedies in court against companies where they are negligent or breach their contract with the individual but such legal actions can face difficulties. For example, difficulties in establishing the company’s duty of care to the person bringing the claim, showing a causal link between their activities and harm caused, or obtaining factual evidence. The proposed regulatory model will provide evidence and set standards which may increase the effectiveness of individuals’ existing legal remedies.

If legal action is taken under the tort of negligence, the following criteria would be used to decide if an organisation or individual should be held responsible: injury is reasonably foreseeable and not too remote; and that it is fair, just and reasonable to impose a duty of care. The claimant would have to show: that they were owed a duty of care, that the defendant breached this duty and that they suffered damage as a result of the breach.

It has long been recognised that the imposition of a duty of care in respect of particular conduct depends upon whether it is just and reasonable to impose it. Over vast areas of conduct one can generalise about the circumstances in which it will be considered just and reasonable to impose a duty of care: that is a consequence of Donaghue v Stevenson [1932] AC 562. Across most grounds of liability, whether in tort, contract or by statute, it is possible to generalise about causal requirements. They represent what in ordinary life would normally be regarded as the reasonable limits for attributing blame or responsibility for harm: for example, that the defendant's conduct was a necessary condition for the occurrence of the harm (the "but for" test). The UK WP evinces that it is just and reasonable to impose the online duty of care.

However, ‘virtual causation’ presents a Herculean legal challenge. For instance, the UK WP suggests that all five terrorist attacks in the UK during 2017 had an online element. Under the proposed law, it would have been proven that “but for” the online content, the terrorist attacks would not have occurred. The evidential threshold for such litigation is extremely high. The evidential conundrums for causation extend to other harms identified in the UK WP.

The UK WP also proposes invoking a new form of vicarious liability, that is, where one person is held liable for the torts of another, even though that person did not commit the act itself. Under the proposals, this would mean individual senior managers would be held personally accountable in the event of a major breach of the statutory duty of care. This could involve

---

135 UK Online Harms White Paper 2019, para 3.29
136 Fairchild (suing on her own behalf) etc v. Glenhaven Funeral Services Ltd and others etc. [2002] UKHL 22
139 UK Online Harms White Paper 2019, para 1.9
personal liability for civil fines, or could even extend to criminal liability\textsuperscript{140}. The government, in justifying its feasibility, notes that the introduction of the Senior Managers & Certification Regime has driven a culture change in risk management in the sector. Another recent example of government action is establishing corporate offences of failure to prevent the criminal facilitation of tax evasion. With regard to this, the Government believes that relevant bodies should be criminally liable where they fail to prevent those who act for, or on their behalf from criminally facilitating tax evasion. The new offences will be committed where a relevant body fails to prevent an associated person \textit{criminally} facilitating the evasion of a tax, and this will be the case whether the tax evaded is owed in the UK or in a foreign country.\textsuperscript{141} Recent changes to the Privacy and Electronic Communications Regulations (PECR) also provide powers to assign liability to a specific person or position within an organisation.

However, it also observes that this is as yet largely untested. Difficulties with this include identifying which roles should be prescribed and whether this can be proportionate for small companies. Some managers and companies do not have a legal presence in the UK. On this, the government envisages close collaboration between government bodies, regulators and law enforcement overseas, in the EU and further afield, will be required. The government intends to design the regulator’s powers to ensure that it can take action against companies, including disrupting the business activities of a non-compliant company\textsuperscript{142} or blocking platforms from being accessible in the UK as a last resort.\textsuperscript{143}

JUDICIAL REVIEW: POTENTIAL CHALLENGES THROUGH ADMINISTRATIVE JUSTICE

The regulator will set out expectations for companies to do what is ‘reasonably practicable’ to counter harmful activity or content, depending on the nature of the harm, the risk of the harm occurring on their services, and the resources and technology available to them.\textsuperscript{144} This test that has underpinned the success of health and safety legislation.\textsuperscript{145} However, all companies within scope will be required to take reasonable and proportionate action to tackle harms on their services.\textsuperscript{146} Companies will have the ability to seek judicial review of the regulator’s actions and decisions through the High Court, ruling out the potential of an ‘ouster clause.’ The government will, however, seek views through the consultation about whether there should be another statutory mechanism of review, which would allow the use of a tribunal other than the High Court, and what bar should be set for appeals through this route.\textsuperscript{147} It has to be noted, nonetheless, that appeals and judicial review are different. Judicial review only focuses on the

\begin{footnotes}{
\footnotetext{140} UK Online Harms White Paper 2019, para 6.5
\footnotetext{141} Government guidance: Tackling tax evasion: Government guidance for the corporate offences of failure to prevent the criminal facilitation of tax evasion. 1st September 2017
\footnotetext{142} UK Online Harms White Paper 2019, para 40
\footnotetext{143} UK Online Harms White Paper 2019, para 6.9
\footnotetext{144} UK Online Harms White Paper 2019, para 35
\footnotetext{145} UK Online Harms White Paper 2019, para 5.7
\footnotetext{146} UK Online Harms White Paper 2019, para 5.7
\footnotetext{147} UK Online Harms White Paper 2019, para 6.13

http://mc.manuscriptcentral.com/ijlit
process by which the courts review the lawfulness of a decision (or lack of a decision) or action taken (or failure to act) by a public body whereas appeals will delve into the merits of a case.

In the UK, the grounds for judicial review are well-expounded. Decision-makers ought to comprehend the law that regulates them. Otherwise failure to follow the law properly, will result in their (non)decision, action or failure to act being declared ‘illegal’. Thus, an action or decision may be deemed illegal on the basis of public body acting beyond its powers or *ultra vires*. It is possible cases under the proposed law could be brought for judicial review under the rubric of “illegality” if the regulatory board transcends its powers.

Secondly, the courts may also intervene to quash a decision if they consider it to be so demonstrably unreasonable as to constitute ‘irrationality’ or ‘perversity’ on the part of the decision maker. The benchmark decision on this principle of judicial review was made in the Wednesbury case: ‘If a decision on a competent matter is so unreasonable that no reasonable authority could ever have come to it, then the courts can interfere... but to prove a case of that kind would require something overwhelming...’\(^{148}\) This threshold is extremely difficult to meet, which is why the Wednesbury ground is usually argued alongside other grounds, rather than on its own. The onus is also on the claimant to establish irrationality or perversity. Thirdly, complaints can also be made, not merely in respect of the decision taken, but the procedure by which the decision was made. These include: failure to give each party to a dispute an opportunity to be heard, bias, failure to conduct a consultation properly, failure to give adequate reasons and legitimate expectation.

Following the entry into force of the Human Rights Act (HRA), victims of unlawful acts by public authorities are able to raise Convention issues in the domestic courts. Section 6(1) of the Act provides that: It is unlawful for a public authority to act in a way which is incompatible with a Convention right. Section 3 of the HRA 1998, in effect, permits judicial review of Acts of Parliament.\(^{149}\) The use of the HRA has introduced different concepts like “proportionality” and the court has acknowledged that these might yield different results to traditional grounds of review.\(^{150}\) ‘Proportionality’ had previously been considered a facet of ‘irrationality’.\(^{151}\) In general terms, the concept of ‘proportionality’ requires a balancing exercise between, on the one hand, the general interests of the community and the legitimate aims of the state and, on the other, the

\(^{148}\) *Associated Provincial Picture Houses Ltd v Wednesbury Corporation* [1948] 1 KB 223, HL.

\(^{149}\) See for example Richard Gordon QC, “Principles for Judicial Deference”, [2006] JR 109 for a discussion of the Constitutional Status of the Human Rights Act and a consideration of “judicial supremicism”. In particular he indicates that Section 3 of the Act represents “a radical change to the conventional view of Parliamentary sovereignty [… representing] a significant change from the views expressed by Lord Reid in *Pickin v British Railway Board* [1974] AC 765

\(^{150}\) *R (on the application of Daly) v Secretary of State for the Home Department* [2001] UKHL 26, in which Lord Steyn indicated that “[T]he intensity of review in a public law case will depend on the subject matter in hand […] That is so even in cases involving Convention rights. In law context is everything”

\(^{151}\) For example, in the case of *R v Secretary of State for Transport ex p. Pegasus Holdings (London) Ltd* [1988] 1 WLR 990 Mr Justice Schiemann observed that “one aspect of reasonableness is proportionality: that is, that the means adopted should be reasonable, having regard to the aim to be achieved and the effects of any course adopted”
protection of the individual’s rights and interests. It has become ‘significantly more difficult to do so in the online world, especially considering that every action to restrict access to content is potentially in conflict with the right to freedom of expression and information as enshrined in Article 10 of the European Convention on Human Rights’ (ECHR). This fundamental right and freedom is a primary objective of the Council of Europe and its member states.

The Council recognizes that states also have a legitimate right, and even an obligation, to protect children from content which is unsuitable or inappropriate. Perhaps the most draconian proposition in the UK WP is that in the event of extremely serious breaches, such as a company failing to take action to stop terrorist use of their services, it may be appropriate to force third party companies to withdraw any service they provide that directly or indirectly facilitates access to the services of the first company, such as search results, app stores, or links on social media posts. The government notes however, that these measures would need to be compatible with the ECHR.

Under the ECHR, a restriction placed on a freedom guaranteed by the Convention has to be ‘proportionate to the legitimate aim pursued.’ If a Convention right is to be subject to a restriction, any measure will satisfy the proportionality test only if it meets three criteria: (a) the legislative objective must be sufficiently important to justify limiting a fundamental right; (b) the measures designed to meet the legislative objective must be rationally connected to that objective – they must not be arbitrary, unfair or based on irrational considerations and (c) the means used to impair the right or freedom must be no more than is necessary to accomplish the legitimate objective.

The dangers of censorship, when internet intermediaries are used to implement government policy, are well recognised; a ‘standard’ application of Article 10 of the ECHR (the right to freedom of expression and information) case law may ensure the proportionality of any such State requirements, bearing in mind the risk of collateral censorship. In Yildirim v Turkey, the European Court of Human Rights (ECtHR) held that Turkey violated Article 10 when it blocked access to all Google sites because of one Internet site facing criminal proceedings for insulting the memory of a former Turkish president. The court wrote that the right to freedom of expression is two-fold, encompassing not only the right to transmit but also to receive information, and that although Article 10 does not afford absolute protection against prior restraint, restrictions on freedom of expression do require strict judicial scrutiny.

152 Council of Europe Recommendation CM/Rec(2009)5 para I (7)
153 Council of Europe Recommendation CM/Rec(2009)5 para I (7)
154 UK Online Harms White Paper 2019, para 6.5
155 Handyside v United Kingdom (1976) 1 EHRR 737
157 See Information Law and Policy Centre, Institute for Advanced Legal Studies – written evidence (IRN0063) to the House of Lords Committee
158 Yildirim v Turkey – 3111/10 – HEJUD [2012] ECHR 2074
The task of balancing children’s digital participation with their protection is enormously complex.\(^{159}\) While the protection of children is paramount, it is critical that regulatory actions are legal. When considering situations where an individual is blocked from a particular service, the difference between implementation of State policy and the exercise of the service provider’s own rights must be recognised.\(^{160}\) The test for what is ‘reasonably practicable’ is potential ground for contestation. In other words, the law will not be absolute on the legal duty. Such expression provide duty holders with a defence against a duty. The definition set out by the Court of Appeal is:

Reasonably practicable’ is a narrower term than ‘physically possible’ … a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other.\(^{161}\)

The UK WP notes that the regulator’s decision will depend on the nature of the harm, the risk of the harm occurring on a company’s services, and the resources and technology available to them. It is not inconceivable that if the government’s intention to disrupt the business activities of a non-compliant company\(^{162}\) or block platforms from being accessible in the UK\(^{163}\) crystalise into statute, such measures could also be gauged against judicial review precept of “irrationality”. Given the contrasting evidence on the effects of the internet on children and their utility, such platform could be in lawful and beneficial use by others\(^{164}\). Such decisions could be regarded irrational and disproportionate.

**DIGITAL SPACE AND HUMAN RIGHTS: A SAMPLE OF CASES**

There is limited case law in this area, except decisions relating to different forms of publications, including the internet, by individuals.\(^{165}\) Rights claims, in general, are against the State not private actors. Even here, however, the State may have obligations to take any necessary measures to safeguard a right, including enacting legislation to protect rights based on the substantive rights and Article 1 of the ECHR (the states’ obligation to protect human rights).\(^{166}\)

---


\(^{161}\) *UK Online Harms White Paper* 2019, para 40.

\(^{162}\) *UK Online Harms White Paper* 2019, para 6.9.

\(^{163}\) See eg *Cengiz and Others v. Turkey* (applications nos. 48226/10 and 14027/11), the Ankara Criminal Court of First Instance ordered the blocking of access to YouTube on the ground that the website contained some ten videos which, under the legislation, were insulting to the memory of Atatürk. ECtHR ruled that the applicants, all academics in different universities, had been prevented from accessing YouTube for a lengthy period of time and that, as active users, and having regard to the circumstances of the case, they could legitimately claim that the blocking order in question had affected their right to receive and impart information and ideas.

\(^{164}\) See eg *Perrin v. the United Kingdom* (dec.) (no. 5446/03, ECtHR 2005-XI); *Akdas v. Turkey* no 41056/04; *Yildirim v Turkey* no 3111/10; Kharitonov v. Russia no 10795/14; Cengiz and Others v. Turkey nos. 48226/10 and 14027/11.

\(^{166}\) See Information Law and Policy Centre, Institute for Advanced Legal Studies – written evidence (IRN0063) to the House of Lords Committee.
While the court recognizes the protection of morals, interference with a right of freedom expression must be proportionate and the result of a social need and necessary in a democratic society, within the meaning of Article 10.\textsuperscript{167} In \textit{Perrin v UK}, the applicant complained under Article 10 of the Convention about his conviction and sentence for publishing an obscene article on an internet site. He argued that these constituted interferences with his right to freedom of expression which were not prescribed by law and/or were not necessary in a democratic society. Further, he contended he was exempt as the site was run by an external host. However, the Court was satisfied that the applicant's criminal conviction could be regarded as necessary in a democratic society in the interests of the protection of morals and/or the rights of others. It follows that this part of the application is manifestly ill-founded within the meaning of Article 35 § 3 of the Convention.\textsuperscript{168}

As regards the protection of minors, the ECtHR has explained that an individual of a young age is vulnerable. In \textit{K.U. v Finland}\textsuperscript{169}, applicant's father requested the police to identify a person who had placed the advertisement purporting his 12-year-old son was seeking a gay partner, in order to prefer charges against that person. The service provider, however, refused to divulge the identity of the holder of the so-called dynamic IP address in question, regarding itself bound by the confidentiality of telecommunications as defined by law.\textsuperscript{170} The applicant complained under Article 8 of the Convention that an invasion of his private life had taken place and that no effective remedy existed to reveal the identity of the person who had put a defamatory text on the Internet in his name, contrary to Article 13 of the Convention. The police then asked the Helsinki District Court to oblige the service provider to divulge the said information pursuant to section 28 of the Criminal Investigations Act (Act no. 449/1987). Both the District Court and Supreme Court declined the application.

The ECtHR, however, ruled that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case such protection was not afforded.\textsuperscript{171}

\begin{quote}
An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.\textsuperscript{172}
\end{quote}

In \textit{C.A.S. and C.S. v. Romania}, the ECtHR ruled that as a matter of principle, measures must exist at the national level to guarantee respect for human dignity and the protection of the best interests of the child.\textsuperscript{173} In that judgment the Court clearly acknowledges that the States have an

\begin{footnotesize}
\textsuperscript{167} See eg \textit{Akdas v. Turkey} no 41056/04
\textsuperscript{168} \textit{Perrin v. the United Kingdom} (dec.) no. 5446/03, ECHR 2005-XI
\textsuperscript{169} \textit{K.U. v. Finland} no. 2872/02
\textsuperscript{170} Para 35
\textsuperscript{171} Par 49
\textsuperscript{172} Par 49
\textsuperscript{173} \textit{C.A.S. and C.S. v. Romania}, no. 26692/05, § 82, 20 March 2012
\end{footnotesize}
obligation under Articles 3 and 8 to ensure that an effective criminal investigation is carried out in cases of violence against children. The Court also refers expressly to the international obligations of States and in particular the United Nations Convention on the Rights of the Child.

CONCLUSION

This article discussed the proposed UK law on online harms, highlighting some of the potential challenges and pitfalls with internet governance, with a focus on children. The proposition comes the backdrop of contested notions of childhood. A socio-cultural and legal approach is useful in shoring up the context of the regulatory environment. The digital space has ruptured conventional family dynamics. Unquestionably, the cyberspace has the potential for hazards for children while on the other hand, it is a useful space for young people for a variety of reasons discussed. This makes regulation a complicated, if not a contested affair. Clearly, there are potential challenges and pitfalls in introducing a new legal obligation to a virtual word. The proposed introduction of legal duty of care, while necessary, would come against a background of conflicting evidence on the media effects on children. It would appear legislation is necessary. However, it would require a balance between protecting children and regulating the internet. Draconian and disproportionate measures would be regarded as illegal, perverse and conflicting with the rights of all parties involved on the digital space.