

DISCUSSION PAPER SERIES:

Children's Rights and Business in a Digital World

FREEDOM OF EXPRESSION,
ASSOCIATION, ACCESS
TO INFORMATION AND
PARTICIPATION



DISCLAIMER

The views expressed in this publication do not necessarily represent the views of UNICEF, and UNICEF makes no representation concerning the source, originality, accuracy, completeness or reliability of any statement, information, data, finding, interpretation, advice or opinion contained herein.

©United Nations Children’s Fund (UNICEF) June 2017.

AUTHORS

A first draft of this discussion paper was prepared by Carly Nyst, independent consultant and expert on human rights in a digital world. The discussion paper series on children’s rights and business in a digital world is managed by Patrick Geary and Amaya Gorostiaga of the UNICEF Child Rights & Business Unit.

ABOUT THIS DISCUSSION PAPER SERIES

As more children around the world spend more time on the Internet in more ways, it becomes increasingly essential to appreciate what children’s rights mean in a digital world. While there is now a widely accepted public imperative to protect children from harm, abuse and violence online, there has been comparatively little consideration of how to empower children as active digital rights holders. At the same time, the rapidly expanding power and reach of the ICT sector have thrust communications and technology companies into key policy debates on the risks and opportunities children encounter online.

This series of discussion papers seeks to explore the relationship between children’s rights, business and the Internet in greater detail. The discussion papers address central themes, including children’s rights to privacy, freedom of expression, information, education and non-discrimination. While the issues presented are by no means exhaustive, it is hoped that these discussion papers will contribute to broadening the conversation on children’s rights and business in a digital world.

CONTENTS

INTRODUCTION	4
PART I: CHILDREN’S EXPRESSION AND INFORMATION RIGHTS UNDER INTERNATIONAL LAW.....	6
Why freedom of expression?	7
Children’s freedom of expression in international law	7
Striking a balance	8
PART II: RESTRICTIONS ON EXPRESSION AND INFORMATION	10
Illegal and harmful content	11
Promoting responsible conduct	14
Preventing violent extremism	15
PART III: THE RESPONSIBILITIES OF AND OPPORTUNITIES FOR THE ICT SECTOR.....	16
Human rights and the ICT sector	17
Integrating child rights considerations into all appropriate corporate policies and processes	17
Developing standard processes to handle child sexual abuse material.....	18
Creating a safe and age-appropriate online environment.....	18
Educating children, parents and teachers about children’s safety and their responsible use of ICTs	19
Promoting digital technology as a mode for increasing civic engagement.....	19
PART IV: THE ROLE OF STATES	20
Legislative measures.....	21
Enforcement measures	21
Policy measures	22
CONCLUSION.....	22

INTRODUCTION

There is a long-perceived tension between child protection advocates and freedom of expression defenders. A balanced approach to children's rights online has remained elusive, and early resistance to child online protection measures, grounded squarely in the discourse of Internet users' freedom of expression,¹ has now given way to a 'moral panic' regarding children's exposure to harmful online content.² As a result, current public policy is increasingly driven by overemphasized, albeit real, risks faced by children online, with little consideration for potential negative impacts on children's rights to freedom of expression and access to information. The ICT sector, meanwhile, is regularly called on to reduce these risks, yet given little direction on how to ensure that children remain able to participate fully and actively in the digital world.³

The risks children face online are not significantly different from the risks they face offline, and research suggests that a large majority of children does not have serious concerns about using the Internet.⁴ By the same token, concerns about children's freedom of expression and access to information are just as fraught in the offline world as in the online world. Regulators and companies have struggled with rating and classifying television, film, gaming and entertainment content for decades, and educators have long sought to adjust and restrict the availability of reading material in schools according to students' age and maturity.

Nevertheless, the Internet has fundamentally altered how information is accessed and imparted. It has displaced parents, guardians and educators as gatekeepers of children's media consumption, and likewise has displaced traditional media regulators as controllers of this content. Online material can be easily produced and viewed by anyone with a connection, and children now have direct lines of communication with Internet users all over the world. This clearly facilitates children's free expression and access to information, although it also introduces risks to children's safety and security by, for example, enabling contact with perpetrators of abuse and increasing exposure to harmful or inappropriate content.

Technology and policy have thus sought to replicate the traditional roles played by parents, regulators and business entities with respect to children online. Parental controls, content blocking and Internet filters have been developed to monitor and limit children's online activities, and laws have been advanced to regulate children's conduct in digital platforms, online games and social networks. Strict use policies mean that digital forums can be heavily policed, and children's browsing is tracked in the name of preventing violent extremism.

While the motivations behind these efforts are understandable, some measures taken in the name of child protection may disproportionately restrict children's participation in the digital world. Potential concerns might arise, for example, if parental controls restrict access to valuable and informative content; when children's Internet use is revoked or limited as a form of punishment; where children are penalized at school for sharing legal content online; or as network-wide blocking or filtering mechanisms are deployed. Businesses are often caught in the middle, striving to provide children with access to their services while responding to both parental demands for greater control and governmental demands to block and filter content.⁵

¹ Livingstone and O'Neil, 'Children's Rights Online: Challenges, Dilemmas and Emerging Directions', in S. van der Hof et al. (eds.), *Minding Minors Wandering the Web: Regulating Online Child Safety, Information Technology and Law Series 24*, 2014.

² Powell, Alison, Michael Hills and Victoria Nash, 'Child Protection and Free Expression', Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010, p. 3.

³ Notably, the United Nations Committee on the Rights of the Child has been unwilling or unable to flesh out the content of the rights and their relationship with the Internet. Article 19 has criticized the Committee's failings in this regard at length, in 'Kid's Talk: Freedom of expression and the UN Convention on the Rights of the Child', available at <www.article19.org/data/files/pdfs/publications/children-kid-s-talk.pdf>.

⁴ Powell, Alison, Michael Hills and Victoria Nash, 'Child Protection and Free Expression', Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010, p. 6; LSE Media Policy Project Blog, 'Should children's internet use be filtered? Multi-stakeholder prudishness impedes open deliberation', London School of Economics, 25 October 2012, available at <http://blogs.lse.ac.uk/mediapolicyproject/2012/10/25/should-childrens-internet-use-be-filtered-multi-stakeholder-prudishness-impedes-open-deliberation>.

⁵ Thierer, Adam, 'Parental Controls and Online Child Protection: A Survey of Tools and Methods', the Progress and Freedom Foundation, August 2010.

This paper explores the apparent tensions between children’s right to protection from violence and their rights to freedom of expression, association, access to information and participation. In so doing, it clarifies children’s expression and information rights from a holistic viewpoint (Part I), and identifies common restrictions placed on children’s participation in the digital world to protect against harmful content, contact and conduct (Part II). The paper then addresses the role and responsibilities of the ICT sector to respect and promote children’s expression and information rights (Part III), and concludes by highlighting legal and policy measures that governments might take to do the same (Part IV).

PART I

CHILDREN'S EXPRESSION AND INFORMATION RIGHTS UNDER INTERNATIONAL LAW

WHY FREEDOM OF EXPRESSION?

Freedom of expression is an essential foundation of democracy,⁶ and is enshrined around the world in international law, regional agreements and national constitutions.⁷ Broadly, this freedom aims to protect the communication of ideas and opinions for any purpose and in any form, from political writing and religious discourse to cultural exhibition and artistic performance. Importantly, it has come to encapsulate not only the right to impart information, but also the right to seek, receive and access information.⁸

Freedom of expression applies online just as it applies offline, and the Internet has dramatically expanded the volume, power and reach of information. This has not only recast the form, scope, market and impact of traditional media sources, but also empowered citizens to create, access, synthesize and share knowledge. As noted by the United Nations Special Rapporteur on freedom of expression, “individuals are no longer passive recipients, but also active publishers of information” contributing “to the discovery of the truth and progress of society as a whole”.⁹

CHILDREN’S FREEDOM OF EXPRESSION IN INTERNATIONAL LAW

The International Covenant on Civil and Political Rights (ICCPR) grants all individuals, including children, the right to freedom of expression.¹⁰ Children’s right to freedom of expression is further developed in the Convention on the Rights of the Child (CRC), firmly rooted in the Convention’s general principle that children have the right to participate in all aspects of their lives.¹¹ Building on this idea, Article 13 of the CRC states that children “shall have the right to freedom of expression ... includ[ing] freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child’s choice”. Article 15 further recognizes “the rights of the child to freedom of association and to peaceful assembly”.

The CRC also grants children a unique and explicit right to information, with Article 17 recognizing that children should have “access to information and material from a diversity of national and international sources, especially those aimed at the promotion of [their] social, spiritual and moral well-being and physical and mental health”. Article 17 calls for a number of supportive measures to promote children’s right to information, including mass dissemination of social and cultural content; prolific production of materials for children; greater awareness of minority linguistic needs; increased international cooperation; and the development of media guidelines to protect children from exposure to “information and material injurious to [their] well-being”.

This last point merits particular discussion, as much of the discourse on children’s access to information online is driven by the imperative to protect children from exposure to potentially harmful content. While this is a legitimate policy aim, it must be viewed in the context of the wider obligation to provide children with

⁶ *Handyside v. the United Kingdom*, no. 5493/72, para. 49, 7 December 1976.

⁷ See, e.g., Article 19 of the Universal Declaration on Human Rights, 1948; Article 19 of the International Covenant on Civil and Political Rights, 1966; Amendment I of the United States Constitution, 1791; and French Declaration of the Rights of the Man and the Citizen, 1789.

⁸ See United Nations Human Rights Committee, General Comment No. 34, adopted in July 2011, available at: <www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

⁹ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27 at [19], available at <www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>.

¹⁰ ICCPR, Article 19.

¹¹ CRC, Article 12 (“States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.”).

access to a wide range of beneficial content. Some organizations have highlighted this imbalance, calling for greater consideration of children’s right to receive and access material that could contribute positively to their development.¹²

STRIKING A BALANCE

To fully understand and appreciate children’s rights to freedom of expression and information, it is important to examine their scope, extent and relationship with other rights. The right to freedom of expression is not unbounded, and can be restricted either to protect the rights and reputations of other individuals or to protect national security, public order, or public health or morals. In some circumstances, constraints on children’s digital expression can be justified as an essential protection measure to combat online violence and exploitation. Notwithstanding, any such restrictions would need to be legitimate, predictable, transparent, necessary and proportionate,¹³ and the Special Rapporteur on freedom of opinion and expression has cautioned that “restrictions which may be deemed legitimate and proportionate for traditional media are often not so with regard to the Internet”.¹⁴

Interestingly, while Article 19 of the ICCPR emphasizes that the right to freedom of expression comes with “special duties and responsibilities”, Article 13 of the CRC lacks similar language. This leaves children’s rights to freedom of expression and information arguably less limited than that of adults, and conforms to the CRC’s recognition that children develop progressively as rights holders.¹⁵ Article 5 of the CRC further notes the role of parents to guide children in the exercise of their rights, and Article 3 ensures that the best interests of the child remain at the heart of all public actions concerning children.

Taken together with Article 17, these provisions suggest that parents, public authorities and media companies rightfully play a part in determining the content that children can create, access and disseminate. However, the role of parents must be conditioned on children’s growing autonomy. Any direction from public authorities must stem from a holistic understanding of children’s best interests, and businesses must meet their corporate responsibility to respect the full range of children’s rights.¹⁶

¹² ‘Kid’s Talk: Freedom of expression and the UN Convention on the Rights of the Child’, available at <www.article19.org/data/files/pdfs/publications/children-kid-s-talk.pdf>.

¹³ Report of the Special Rapporteur on the right to freedom of opinion and expression, A/HRC/17/27, 16 May 2011 at [24].

¹⁴ Report of the Special Rapporteur on the right to freedom of opinion and expression, A/HRC/17/27, 16 May 2011 at [27].

¹⁵ CRC, Article 5.

¹⁶ See United Nations Guiding Principles on Business and Human Rights, available at <www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

At present, there is little guidance on how to strike a balance between children’s rights to freedom of expression and access to information and children’s right to be protected from violence. This can be especially challenging in the digital world, which poses both vast opportunities for and tremendous risks to the enjoyment of children’s rights. While it may not be possible to give authoritative, detailed instructions on weighing children’s rights in a digital world that apply clearly and consistently in every circumstance, the CRC and ICCPR provide a strong, underlying set of interrelated rights and principles to consider, indicated in the table below.

Children’s Rights	
Participation	Children have the right to share their views about any decisions that affect them, and to participate in the digital world.
Expression	Children have the right to freely express themselves online, and to seek, receive and impart ideas and information through digital media.
Association	Children have the right to gather and communicate with one another, including through online forums and digital networks.
Enabling Factors	
Media	The mass media, including digital media, should support children’s right to information by providing varied, diverse and positive online content.
Parental Guidance	Parents play an important role in providing guidance to children, and can help children access and disseminate beneficial content online.
Restrictions	Any restrictions on children’s expression and information rights online must be legitimate, predictable, transparent, necessary and proportionate, and should consider the unique nature of the Internet.

PART II

RESTRICTIONS ON EXPRESSION AND INFORMATION

Traditionally, restrictions on children’s expression and information rights have been imposed to shield children from exposure to harmful or otherwise inappropriate content. Increasingly, however, such restrictions are being introduced for other purposes, including the promotion of responsible behaviour and the prevention of violent extremism. These motivations cast children in three markedly different roles: (i) online victims who need protection, (ii) digital citizens whose conduct must be regulated, and (iii) perpetrators who must be monitored and deterred. Each of these justifications presents complex implications for children’s rights, which are explored in further detail below.

ILLEGAL AND HARMFUL CONTENT

Efforts to restrict children’s access to potentially damaging information usually focus on two broad categories of content:

1. **Illegal content**, which includes child sexual abuse material, communications to groom children for sexual abuse, and illegal hate speech.
2. **Harmful content**, which has been defined as “content that is legal, but liable to harm minors by impairing their physical, mental or moral development”¹⁷ and can be understood to include:
 - **Content that is inappropriate for most children** and of little benefit, such as graphic violence or adult sexual imagery..
 - **Content that may be unpleasant for children** but is ordinary, such as stereotypical depictions of young people, women and minorities; pro-anorexia and eating disorder websites; or malicious criticisms.

Many restrictions designed to prevent children’s exposure to illegal content are well-considered and legitimate, and restrictions on obviously inappropriate content can be similarly justified. Restrictions on unpleasant but sufficiently ordinary content, however, are more difficult to ground in a rights-based framework. Additional concerns arise around overly broad definitions of ‘harmful’ that deny children access to content which is essential for their full development. For example, children may be restricted from accessing information about sexual health, sexuality and LGBTI issues in ways that impinge on their rights to health, education and non-discrimination.

Various mechanisms have been developed and deployed to protect children from harmful and illegal content, including network and device-level blocking and filtering, content restrictions, notice and takedown procedures, and restricted search engines. Even as protecting children’s rights is the stated intention behind these measures, the reality is far more complicated.

SERVICE PROVIDER-DEPLOYED BLOCKING AND FILTERING

Internet service providers can be mandated or encouraged to block or filter online content, denying all users or customers access to that content through their networks. Through network-level blocking, access to IP addresses hosting child sexual abuse material can be universally restricted. Law enforcement authorities and non-governmental organizations work to identify illegal websites, including through public hotlines and online reporting platforms. ‘Blacklists’ of IP addresses are compiled, which are then shared with Internet service providers and domain name registrars.¹⁸

¹⁷ Library of the European Parliament, ‘Protection of minors in the media environment in EU regulatory mechanisms’, Library Briefing, 18 March 2013, available at <[www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130462/LDM_BRI\(2013\)130462_REV1_EN.pdf](http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130462/LDM_BRI(2013)130462_REV1_EN.pdf)>.

¹⁸ <<http://domainincite.com/19431-xyz-to-put-global-block-on-domains-banned-in-china>>.

Network-level blocking can be an effective means to prevent the proliferation of and exposure to damaging material. Yet, at the same time, blocking can inadvertently restrict content that is neither illegal nor harmful, and the considered measures in place to identify child sexual abuse material are not typically employed to review other potentially problematic content. There is a notable lack of transparency in the development of blacklists; because blocking is generally done on a cooperative, voluntary basis, there is little independent verification, and Internet service providers may over-comply to avoid government regulation or negative publicity.¹⁹ Lists must be constantly updated to remain relevant, and blocking efforts may mistakenly restrict access to large numbers of websites.²⁰

Network-level filtering is more typically applied to restrict children's access to harmful but not illegal content, such as adult pornography. While such arrangements continue to differ widely across countries, they are increasingly common and often mandated by law. Depending on national requirements, Internet service providers might offer network-level filtering to customers on an opt-in or opt-out basis, and mandatory network-level filtering has also been introduced in public institutions frequented by children such as libraries and schools.²¹

Network-level filtering protocols can be troublingly opaque. As with blocking arrangements, filters can be based on lists of websites known to contain harmful content, and they may also employ keyword recognition and textual analysis to identify and assess content of potential concern. Network-level filters are problematic in that they are largely inscrutable, and may offer users no evidence to show where and when they have been deployed.²² As filtering software risks being over-inclusive in practice, restrictions can be placed on legitimate content without the knowledge or awareness of end-users.²³

Beyond these concerns, network-level blocking and filtering arrangements can be troublesome for many other reasons. Perhaps most importantly, child protection can be and has been used to legitimize the imposition of content restrictions that chill speech viewed unfavourably by authorities. This not only hinders all users' rights to freedom of expression, but also casts doubt over genuine efforts to combat the distribution of child sexual abuse material. Equally, the technical infrastructure that underlies network-level controls can be readily repurposed for state-sponsored censorship, and filtering can be used to further entrench societal prejudice and discrimination.

CONTENT RESTRICTIONS: NOTICE AND TAKEDOWN

Social media providers, search engines and other online platforms may all play a role in restricting access to harmful or illegal content. Social media companies may delete posts or suspend accounts; search engines may remove results; Internet platforms may cease to host websites. These decisions are generally managed through 'notice and takedown' procedures, whereby content is flagged and affected users are informed about the presence and intended removal of offending material.

Notice and takedown processes pose relatively little risk to freedom of expression as they are implemented transparently case by case, but there is mounting pressure to move beyond this approach. Content hosts are now being asked to more actively police platforms, and to prevent the upload of illegal content in the first instance. This has raised concerns about both the expanding liability for hosting user-generated content²⁴ and

¹⁹ EFF, in Powell, Alison, Michael Hills and Victoria Nash, 'Child Protection and Free Expression', Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010.

²⁰ For example, this may occur when IP addresses are spoofed. In one instance, a Pennsylvania law designed to combat child sexual abuse material online restricted access to more than 1.5 million unrelated and wholly lawful websites. Center for Democracy and Technology, submission, in Powell, Alison, Michael Hills and Victoria Nash, 'Child Protection and Free Expression', Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010.

²¹ For example, in the United States, the Children's Internet Protection Act requires that libraries and schools receiving certain kinds of government funding install technical protection measures to prevent children from accessing harmful content.

²² Some service providers display notifications when users attempt to access filtered content, but this is not always the case.

²³ Early versions of filtering software denied access to websites for a number of prominent human rights organizations, including Amnesty International, the American Kurdish Information Network, the International Gay and Lesbian Human Rights Commission, Dalitsan (an organization working to protect the rights of 'Untouchables' in India), the Milarepa Fund (an organization that raises awareness about human rights violations in Tibet) and Human Rights and Tamil People. Article 19, Background Paper on Freedom of Expression and Internet Regulation for the International Seminar on Promoting Freedom of Expression with the Three Specialised International Mandates, November 2001, available at <www.article19.org/data/files/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf>.

²⁴ A recent decision of the European Court of Human Rights found an Internet news portal liable for failing to remove unlawful remarks from unidentified sources in the comments section of the website. *Delfi v. Estonia*, App. no. 64569/09, 15 June 2015.

the practicality of pre-screening vast quantities of data, which could together threaten the very existence of many online platforms that facilitate children's expression and information rights.

There is also a growing debate about the ways in which Internet service companies can be expected to detect and delete illegal content. Private companies may be ill-equipped to make determinations about the legality of content, owing in part to potential resource constraints, poor oversight, lack of accountability, and conflicts of interest.²⁵ Even robust policies about the removal of illegal content face significant challenges in implementation,²⁶ meaning both that child sexual abuse material may remain online and that provocative speech may be wrongfully censored. For some, it is deeply concerning that private actors are being cast as arbiters of freedom of expression,²⁷ although the precise implications for children's rights remain to be seen.

USER-DEPLOYED BLOCKING AND FILTERING: PARENTAL CONTROLS

Parental controls block and filter Internet content through Internet routers and on individual devices. While these controls can provide young children with a safer online experience, they can also prevent children from seeking valuable information on politics, religion and sexuality as they develop greater senses of maturity and autonomy. Parental controls may also reinforce societal biases and discrimination, excluding content solely because it is seen as undesirable by the developers of device-level filtering protocols.²⁸

When parental controls are deployed without consideration for children's evolving capacity to exercise their rights, it can damage trust between children and parents and easily undermine children's rights to freedom of expression and access to information.²⁹ In the worst cases, filters may prevent children from seeking help about violence or abuse they face in the home. Parental controls may offer an appealing introduction for children to the digital world, but their mandatory, widespread or default use poses serious threats to children's expression and information rights and has not yet been consistently shown to reduce children's exposure to online risks.³⁰

CHILD-SPECIFIC SEARCH ENGINES

Search engines are a vital connection between Internet users and the information they seek, and how this content is indexed and presented plays a pivotal role in realizing users' freedom of expression.³¹ Unindexed websites are extraordinarily difficult to access, and the algorithms that underlie search engines can be manipulated to prioritize or restrict access to indexed websites. Such practices have recently come to the forefront in light of discussions around the emerging "right to be forgotten", which empowers individuals to request the delinking of certain information from named searches.

Children use search engines to access a tremendous variety of content, some of which is inevitably harmful or inappropriate. In an attempt to rectify this situation, search engines have now been developed to filter and restrict the range of query results with children in mind. Although child-specific search engines are still in the early stages of evolution, current user experience suggests that the overly broad restrictions imposed threaten to severely constrain children's ability to access beneficial information.³²

²⁵ EFF, in Powell, Alison, Michael Hills and Victoria Nash, 'Child Protection and Free Expression', Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010.

²⁶ <www.theguardian.com/technology/2017/mar/07/facebook-response-sexualised-child-images-bbc-extraordinary>.

²⁷ The Inter-American Commission on Human Rights has observed that "private actors who lack the ability to weigh rights and to interpret the law in accordance with freedom of speech and other human rights standards can seriously endanger the right to freedom of expression guaranteed by the Convention", pp. 47–48, <www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf>.

²⁸ EFF, in Powell, Alison, Michael Hills and Victoria Nash, 'Child Protection and Free Expression', Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010.

²⁹ LSE Media Policy Project Blog, 'Should children's internet use be filtered? Multi-stakeholder prudishness impedes open deliberation', London School of Economics, 25 October 2012, available at <<http://blogs.lse.ac.uk/mediapolicyproject/2012/10/25/should-childrens-internet-use-be-filtered-multi-stakeholder-prudishness-impedes-open-deliberation>>.

³⁰ Sonia Livingstone, *Children and the Internet: Great Expectations, Challenging Realities*, Cambridge: Polity, 2009.

³¹ 98, UNESCO Intermediaries.

³² For example, queries that include words like 'lesbian' and 'breasts' return zero results.

PROMOTING RESPONSIBLE CONDUCT

Over and above scanning, detecting and removing illegal content, online platforms may establish terms and conditions that regulate the dissemination of harmful content. Restrictions might be designed to combat cyberbullying, hate speech and other forms of online harassment, whether over social media networks or digital messaging applications.³³ Along these lines, many countries have in recent years introduced legislation to combat online abuse³⁴ with a particular focus on cyberbullying.³⁵ Some of these laws have empowered public authorities to order the removal of offending content, pushing businesses to develop and swiftly enforce protocols on responsible conduct lest they face hefty fines for non-compliance.³⁶

Despite the prominence of cyberbullying in public policy initiatives, the surrounding rhetoric is not necessarily borne out in evidence.³⁷ While there are some indications that a greater number of children experience sustained bullying online as opposed to offline,³⁸ comprehensive research reflects similar prevalence of bullying online and offline.³⁹ This apparent over-emphasis on cyberbullying can jeopardize children's expression and information rights, as evidenced in policies that seek to prevent children from expressing critical opinions about teachers, parents and friends. As such measures deny children the opportunity to share their legitimate views in a responsible manner, they risk unjustly chilling children's speech and can ultimately discourage children from learning to use the Internet freely and confidently as active digital citizens.

Nevertheless, the ICT industry faces rising expectations in the quest to fight online violence, and some companies have responded by more actively policing their platforms.⁴⁰ Other companies have launched public campaigns and taken steps to improve user complaint procedures.⁴¹ As with notice and takedown, responsive reporting mechanisms offer a suitable means to ensure that cyberbullying, hate speech and online harassment are addressed as and when they occur. The most effective mechanisms are likely to be visible, easily discoverable, recognizable, accessible and available at all times, with a clear infrastructure and established process to ensure speedy review and appropriate action.⁴²

³³ See, e.g., Child Helpline International, 'Briefing Paper on Bullying', October 2012, available at <www.childhelplineinternational.org/media/57468/chi_briefing_paper_bullying.pdf>.

³⁴ Recently adopted laws include the Nova Scotia Cyber Safety Act 2013 and the New Zealand Harmful Digital Communications Bill 2013, both of which address online bullying, harassment and intimidation.

³⁵ These measures may build on or supplant overall anti-bullying policies, many of which have been in place for over a decade. European Commission, 'Background paper for session 3: The role of child protection systems in protecting children from bullying and cyberbullying', 8th European Forum on the Rights of the Child, November 2013, available at <http://ec.europa.eu/justice/fundamental-rights/files/s3_forum_bullying_en.pdf>.

³⁶ In 2015, Australia adopted the Enhancing Online Safety for Children Act. The Act establishes an Office of an e-Safety Commissioner with the power to fine companies up to Aus\$17,000 a day for failing to remove cyberbullying material within 48 hours of receiving a complaint. Timson, Lia, 'Facebook, Twitter face \$17,000-a-day fines for cyber bullying posts as e-Safety Commissioner introduced', The Sydney Morning Herald, 3 December 2014, available at <www.smh.com.au/digital-life/digital-life-news/facebook-twitter-face-17000aday-fines-for-cyber-bullying-posts-as-esafety-commissioner-bill-introduced-20141203-11z2jz.html>; Paul Fletcher, MP, 'Senate passes Enhancing Online Safety for Children Bill with strong bipartisan support', 4 March 2015, available at <www.minister.communications.gov.au/paul_fletcher/news/senate_passes_enhancing_online_safety_for_children_bill_with_strong_bipartisan_support#VvGsqRKLsiw>.

³⁷ Powell, Alison, Michael Hills and Victoria Nash, 'Child Protection and Free Expression', Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010.

³⁸ Livingstone, S. and P. Smith, 'Research Review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age', 2013.

³⁹ European Commission, 'Background paper for session 3: The role of child protection systems in protecting children from bullying and cyberbullying', 8th European Forum on the Rights of the Child, November 2013, available at <http://ec.europa.eu/justice/fundamental-rights/files/s3_forum_bullying_en.pdf>.

⁴⁰ Hayes, Rob, 'Online Video Games May Expose Kids to Violent Language, Experts Warn', ABC Eyewitness News, 27 March 2012, available at <<http://abc7.com/archive/8596874>>.

⁴¹ 'Snapchat launches #BeStrong filter to stop bullying', BBC, 18 November 2015, available at <www.bbc.co.uk/newsbeat/article/34853591/snapchat-launches-bestrong-filter-to-help-stop-cyberbullying>.

⁴² European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Strategy for a Better Internet for Children', 2 May 2012, available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF>>.

PREVENTING VIOLENT EXTREMISM

With the growth in online recruitment for violent extremist organizations, concerns have proliferated around radicalization through social media networks, messaging applications and other digital platforms. As with other forms of harmful content, some governments have established systems to identify and request the removal of violent extremist material,⁴³ and efforts to preventively address radicalization have intensified. Children are understood to be at increased risk, and their online activities are often a critical focus of measures to combat violent extremism.⁴⁴

Initiatives to deter children from joining violent extremist groups abound. Many of these justifiably aspire to help children understand, identify and report concerning communications and material, but others have sought to police and restrict children's online and offline behaviour.⁴⁵ Schools have purchased software to track and report students' digital activities,⁴⁶ and filters have been developed to prevent children from accessing potentially extremist content.⁴⁷

Such measures clearly hamper children's freedom of expression and right to information. Strictly monitoring children's browsing behaviour does not facilitate their learning to use and explore the Internet, while overly broad filters block access to beneficial content. As noted by the United Nations Special Rapporteur on counterterrorism, any steps that curtail freedom of expression in this way must be narrowly tailored and rigorously justified.⁴⁸

⁴³ For example, the Europol Internet Referral Unit and UK Counter Terrorism Referral Unit are tasked with referring violent extremist content to online platforms for removal. See <www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda>; <www.npcc.police.uk/NPCCBusinessAreas/PREVENT/TheCounterTerrorismInternetReferralUnit.aspx>. The latter is specifically dedicated to removing online content of a "violent extremist or terrorist nature", including through methods that use websites' content flagging mechanisms to report content in violation of a site's terms of service. As a result of these efforts, 46,000 pieces of content were removed in 2014. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/31/65, 22 February 2016, at [40].

⁴⁴ <www.betterinternetforkids.eu/web/portal/news/detail?articleId=284946>.

⁴⁵ Khaleeli, Homa, 'You worry they could take your kids: Is the Prevent strategy demonising Muslim schoolchildren?' *The Guardian*, 24 September 2015, available at <www.theguardian.com/uk-news/2015/sep/23/prevent-counter-terrorism-strategy-schools-demonising-muslim-children>.

⁴⁶ See <www.imperosoftware.co.uk/classroom-management-software-fight-against-radicalisation>; <www.futuredigital.solutions/index.php/news/story/protecting-your-students-from-radicalisation-and-other-online-dangers-throu>.

⁴⁷ <www.manchesterscb.org.uk/docs/Safeguarding%20online.pdf>.

⁴⁸ Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/31/65, 22 February 2016, at [40].

PART III

THE
RESPONSIBILITIES
OF AND
OPPORTUNITIES
FOR THE ICT
SECTOR

HUMAN RIGHTS AND THE ICT SECTOR

While there has been much international attention on the ICT sector's responsibility to respect human rights⁴⁹, little of it pertains specifically to children. When children are mentioned, it has been almost exclusively in the context of sexual abuse, exploitation and harmful content without recognition of children's full range of rights. Given the many threats to these rights detailed above, the dialogue on digital rights must now be expanded to consider the ICT sector's impacts on children's rights to freedom of expression, association, access to information and participation. The Guidelines for Industry on Child Online Protection published by UNICEF and the International Telecommunications Union provide a useful framework to consider these rights, and highlight five key activities that ICT companies can undertake to respect and promote children's rights in a digital world:

1. Integrating child rights considerations into all appropriate corporate policies and management processes;
2. Developing standard processes to handle child sexual abuse material;
3. Creating a safe and age-appropriate online environment;
4. Educating children, parents and teachers about children's safety and their responsible use of ICTs;
5. Promoting digital technology as a mode for increasing civic engagement.⁵⁰

Notably, although the ICT sector can and should take many practical and technical steps to improve respect for children's rights to freedom of expression, association, access to information and participation online, full respect for these rights would require a paradigm shift in conceptions about children and the Internet. Children's safety, development, privacy and personal data must be protected, but this need not be at the expense of other rights and freedoms. So long as Internet governance remains driven by an overly protective approach, excessive blocking, filtering and content-policing will continue to threaten both children's and adults' expression and information rights. By empowering children and parents, supporting the development of rights-based legal frameworks, and engaging all relevant actors in a conversation about how human rights can best be respected and enjoyed online, businesses can help to bring about the fundamental change necessary to realize the entire spectrum of children's rights.

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND PROCESSES

By adopting a more holistic approach to children's rights, companies can move beyond a patchwork of ad hoc protection measures and accord greater respect to children's expression and information rights. Such an approach would allow companies to adopt measures that protect children from exposure to illegal and harmful content, and would also enable children to more confidently express themselves online and to freely seek, receive and impart information over the Internet. Industry could support the development of guiding principles

⁴⁹ See, for example, the work of the Global Network Initiative and Ranking Digital Rights, which publishes a corporate accountability index for companies in the ICT sector. See also the publication by Shift and the Institute of Business and Human Rights for the European Commission, 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', available at <http://shiftproject.org/sites/default/files/ECHRSG.ICT_.pdf>.

⁵⁰ <www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf>.

to further this approach, building on a proposed **Children's Internet Charter**:

- (1) Children should have online contents and services of high quality, which are made specifically for them, and which do not exploit them. In addition to entertaining them, these should allow children to develop physically, mentally, and socially to their fullest potential;
- (2) Children should hear, see, and express themselves, their culture, their languages, and their life experiences, through online contents and services that affirm their sense of self, community, and place;
- (3) Children's online contents and services should promote an awareness and appreciation of other cultures in parallel with the child's own cultural background;
- (4) Children's online contents and services should be wide-ranging in genre and content, but should not include gratuitous scenes of violence and sex;
- (5) Children's online contents and services should be accessible when and where children are available to engage, and/or distributed via other widely accessible media or technologies;
- (6) Sufficient funds must be made available to make these online contents and services to the highest possible standards;
- (7) Governments and production, distribution, and funding organizations should recognize both the importance and vulnerability of indigenous online contents and services, and take steps to support and protect it.⁵¹

DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL

ICT companies could work towards a more **considered, coordinated and transparent approach to the network-level blocking of illegal content**. While laws that would require blocking raise numerous concerns, voluntary processes must ensure sufficient accountability and oversight to be effective. In some countries, independent review boards have been appointed to monitor and assess Internet blacklists.⁵² Drawing from diverse expertise, **independent review boards** are well-placed to ensure that lists remain limited to websites hosting child sexual abuse material and allay worries about disproportionate restrictions on expression and information rights. Companies might advocate for, support the development of, or lend their experience and technical expertise to these boards as they fulfil their mandate.

CREATING A SAFE AND AGE-APPROPRIATE ONLINE ENVIRONMENT

Notice and takedown procedures provide an effective means to remove illegal content from online networks, and should be made comprehensible and accessible for children. Platforms that employ these procedures or other forms of network-level filtering should do so transparently, alerting users when and why access to content

⁵¹ The Children's Internet Charter, proposed by Professor Sonia Livingstone, would extend the internationally-endorsed 1995 Children's Television Charter adapted to the Internet. Livingstone, S., 'A rationale for positive online content for children', *Communication Research Trends*, vol. 28 (3) at 13, 2009, available at <http://eprints.lse.ac.uk/48922/1/Livingstone_Rationale_positive_online_2008.pdf>.

⁵² For example, South Korea and Germany have established independent review boards. Powell, Alison, Michael Hills and Victoria Nash, 'Child Protection and Freedom of Expression Online', Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010.

has been restricted. Network-level filters should strive to be both accurate and accountable, with systems in place to quickly address potential mistakes and challenge biases.

When implemented with due regard for children’s expression and information rights, device-level filters in the form of **parental controls** may help younger children learn to explore the Internet in a safe space. Companies might make parental controls available on an opt-in basis, empowering families to determine what is best suited to their situations. Importantly, any device-level filters offered should be easy to install and easy to disable, be clear in their reach and coverage, and provide varying levels of control to accommodate children’s evolving capacities. Filters should not entrench discrimination by restricting access to beneficial content, such as information about sexual orientation or gender identity, and should never track, log or report user behaviour to software providers.⁵³

Internet service companies may also take action to remove illegal and harmful content from their digital platforms. When terms and conditions appear to have been violated, companies can provide **clear, accessible, transparent and efficient complaint mechanisms** to report potentially offending material. Responses should aim to be constructive, noting that suspension and removal of children’s accounts can disproportionately interfere with their expression and information rights. Companies might also work to develop and publish straightforward guidelines to clarify when and how reports are shared with authorities, noting that information provided about suspected cyberbullying or the consensual sharing of sexual content between children may lead to overly punitive law enforcement action.

EDUCATING CHILDREN, PARENTS AND TEACHERS ABOUT CHILDREN’S SAFETY AND THEIR RESPONSIBLE USE OF ICTS

Companies can play a role in **educating children and families about responsible online conduct**, and contribute to a greater understanding of how the Internet functions as a conduit for expression. Internet service companies can explain how information is displayed and concealed, and support efforts to develop children’s critical reasoning skills. ICT companies, however, should refrain from promoting the idea that schools and families can ensure risk-free online experiences for children. Parents and teachers should appreciate the expansive complexity of the Internet, the growing challenges posed by user-generated content, and the potential negative impacts of an overly protective approach to children’s expression and information rights.

PROMOTING DIGITAL TECHNOLOGY AS A MODE FOR INCREASING CIVIC ENGAGEMENT

Companies can **encourage and empower children to participate in digital communities** and engage in democratic debate online. They can provide access to a diverse range of information and opinions, giving children the means to form and express their views. When enabling or supporting children’s access to online platforms for civic engagement, companies should make sure that children appreciate the full implications of their participation, including with respect to their right to privacy.

⁵³ Powell, Alison, Michael Hills and Victoria Nash, ‘Child Protection and Free Expression’, Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010.

PART IV

THE ROLE OF STATES

Governments have an obligation to ensure that businesses respect children's rights, and should take appropriate steps to prevent and redress abuses of children's rights to freedom of expression, association, access to information and participation online.⁵⁴ While these rights are often best realized in an absence of regulation, governments can take measures to empower and protect children online. For example, governments can support voluntary systems for blocking and filtering illegal content, establish independent review mechanisms for website blacklists, educate law enforcement authorities about children's expression and information rights, and develop guidelines for companies on children's rights online. At the same time, governments must respect children's rights in their own activities, and should bear children's expression and information rights in mind when considering measures that would monitor, track or restrict children's online behaviour.

LEGISLATIVE MEASURES

- **Support voluntary blocking and filtering of illegal content**

To facilitate the quick and effective removal of illegal content, governments should support the existence of voluntary frameworks. In most circumstances, formal regulation beyond the authorization of voluntary blocking and filtering of illegal content is unnecessary and would pose heightened risks of censorship and illegitimate content restriction.

- **Enable a free exchange of information and ideas**

Governments should scrutinize any measures that would mandate Internet service companies to police content on the websites and platforms they maintain or hold Internet intermediaries liable for third-party content. Where broadly applied, such measures could incentivize the removal of beneficial information and hinder the free exchange of information and ideas.

ENFORCEMENT MEASURES

- **Independent review of blacklists**

While mandatory blocking is not advisable in most circumstances, governments can be well placed to review and monitor the process by which website blacklists are developed and maintained. They might consider establishing or supporting the formation of an independent mechanism to approve and oversee the use of such blacklists in line with human rights obligations, incorporating viewpoints and expertise from a diverse array of knowledgeable professionals.

- **Training of judges, lawyers and police**

With the rapid expansion of the Internet and evolving nature of cybercrime, it has proved difficult for legal and judicial systems to keep pace. To ensure laws are enforced as effectively online as they are offline, governments should provide regular training for judges, lawyers and police on new developments in technology that incorporates an understanding of children's rights in a digital world.

⁵⁴ Committee on the Rights of the Child, General Comment 16, 17 April 2013.

POLICY MEASURES

- **Develop guidelines for business entities**

Governments can develop or support the development of guidelines to assist businesses in understanding their responsibilities with respect to children's rights to freedom of expression and access to information. These guidelines might provide general principles to clarify children's expression and information rights, and demonstrate how these can be balanced with children's protection rights.

- **Review child protection measures**

Children stand to benefit greatly from digital media, and government efforts to protect children online should be narrowly tailored to minimize negative impacts on children's expression and information rights. Mandatory Internet filtering in schools and public institutions should be re-examined; efforts to combat cyberbullying should be proportionate to the scale, scope and severity of the situation; and requirements that educators and guardians police children's online behaviour should be reconsidered. Measures that would interfere with children's rights to freedom of expression and access to information should only be introduced where this interference is both necessary and proportionate.

CONCLUSION

The Internet offers boundless opportunities for children to express themselves in new and meaningful ways, and gives children access to nearly limitless information at their fingertips. In an ever more connected world, digital technology is not only an enabler of children's rights, but also increasingly essential for their full realization. Public and private initiatives to protect children online, however well intentioned, can therefore have weighty impacts on children's expression and information rights.

Despite growing awareness, children's rights to freedom of expression and access to information are increasingly threatened with restriction. It is thus essential that all actors who operate in the ICT sector devote greater attention to these rights. This paper has presented a range of practical steps that can be taken to prevent unjustified interference with children's expression and information rights. In so doing, it is hoped that businesses and governments alike will adopt measures to better protect and empower children as full rights holders in a digital world.

