Towards an Internet Safety Strategy

5Rights Foundation

January 2019

5Rights

5Rights Foundation
Towards an Internet Safety Strategy

Table of Contents

Preface

This excellent report from 5Rights Foundation sets out a 360 degree framework to prevent harm to children from digital products and services. The report is a world-leading piece of public policy in this area.

The seven pillars of a safety strategy set out by Beeban Kidron and her team - **parity of protection**, **design standards**, **accountability**, **enforcement**, **leadership**, **education** and **evidence-based interventions** - are universally applicable and could serve as a model for not just the forthcoming UK Government strategy and ICO Code on Age Appropriate Design, but almost any other government or regulator in the world.

The universality of the 5Rights approach sits well alongside the work on a duty of care for online services that Professor Lorna Woods and I have carried out for Carnegie UK Trust. The breadth and complexity of issues faced in reducing harm from digital technologies are best met with overarching principles rather than detailed individual laws. Knowing that principles will be applied, creates more certainty for companies as they innovate, rather than having to wait for laws to catch up. 5Rights' 'seven pillars' set out such principles and encompass a duty of care.

The 5Rights framework is an optimistic one, harnessing the benefits of digital goods and services for society, as well as the shareholders of the companies that produce them. The report suggests that regulation is necessary to make the market work properly by allocating costs where they belong – with the companies that create them. The history of economic development shows us that we can't rely on company boards to see much beyond the shareholder interest. Governments must act on behalf of society to make companies factor external costs into their production decisions, particularly where child safety is at stake.

The report reminds us that 5Rights is supporting leading academics to work with the United Nations Committee on the Rights of the Child to formally clarify how the UN Convention on the Rights of the Child applies in the digital space.

I hope that this report is a precursor of what we can expect from the United Nations. Governments, regulators and technology companies across the world should pay close attention to it.

William Perrin, Trustee, Carnegie UK Trust

About 5Rights Foundation

The inventors of the digital world imagined an environment in which all users would be equal, but in fact, 1/3rd of users globally and 1/5th in the UK, are children.[1] Children are growing up in an environment that systematically fails to recognise their age, meet their needs or uphold their rights.

The 5Rights Foundation works toward a digital environment that anticipates the presence, meets the needs and respects the rights of children. Our interdisciplinary network includes; child development experts, online protection experts, lawyers, technologists, NGOs, campaigners, academics, policy makers and many from the commercial sector.

Together we imagine a digital environment that delivers on the promise of its founders to be "a public good that puts people first" and fulfils "the goal of helping humanity promote truth and democracy".[2] An environment that allows all children to access it creatively, knowledgeably and fearlessly; an environment that offers support by default; one that operates to agreed, universal, ethical and enforceable standards. It is to this end that we work, and in the pursuit of this vision that we consider the need for a safety strategy.

Introduction

In this paper, 5Rights Foundation considers the risks and harms that the digital environment poses for children[3] and proposes seven pillars upon which a safety strategy should be built: **parity of protection**, **design standards**, **accountability**, **enforcement**, **leadership**, **education** and **evidence-based interventions.**

Many of the risks and harms that children face mirror concerns Government has for other user groups, indeed all user groups. But children have particular vulnerabilities associated with age and benefit from particular privileges, including those set out in the United Nations Convention on the Rights of the Child (UNCRC).[4] Meeting children's needs and ensuring they are adequately protected online requires specific actions and should be articulated as a clear priority, uncluttered by the interests of others.

Mitigating risk and harm must not be the extent of Government's ambition. Technological progress should be harnessed for societal good, to promote individual and collective rights, and to meet the needs of vulnerable users, particularly children. It should also reflect the values embodied in our culture, laws and international agreements in all areas of a child's life. In short, it should be the Government's policy to create a digital environment in which children's needs are prioritised and their rights routinely upheld.

Family, peers and school have long been recognised as the three environments of a child's socialisation. Experts now understand that the digital environment has become the fourth.[5]

[1] One in Three: Internet Governance and Children's Rights, S. Livingstone, et al, Unicef, January 2016
[2] Tim Berners-Lee Launches Campaign to Save the Web From Abuse, The Guardian, 5 November 2018
[3] A child means every human being below the age of 18. Article 1, Convention on the Rights of the Child, 1990
[4] Convention on the Rights of the Child, 1990
[5] Nurture Network Launch Event: Promoting Mental Health for Young People in a Digital World, 30 November 2018

This is why we must urgently take steps to make the digital environment one that recognises the privileges, needs and rights of childhood.

Most businesses and organisations, including those run by Government, are fully or partially technology businesses. To be effective, a safety strategy must apply to all online services and all in the digital value chain, and respond to the full impact of digital interactions on a child's experience.

Background

Government published its Internet Safety Strategy Green Paper in October 2017. In it, Government made a commitment to the principle that what is unacceptable offline should be unacceptable online. Following a public consultation on the Green Paper, the Government response was published in May 2018. A White Paper is expected.[6]

The purpose of the Safety Strategy is widely understood to be; to identify the risks and harms associated with the digital environment; to require companies to take action to militate against them; and to enforce non-compliance where necessary.

Risks

There are many individual and combinations of risk, but they can be categorised into four broad categories:

Content risks: a child or young person is exposed to harmful material (e.g. indecent images of children, pornography, age-inappropriate content, extreme and real-life violence, discriminatory or hateful content, fake news, disinformation, hostile public discourse, echo chambers, polarisation, machine reinforcement of polarised views, dissemination, content that endorses risky or unhealthy behaviours such as anorexia, self-harm, suicide).

Contact risks: a child or young person participates in activity with a malign actor, often, but not always, an adult (e.g. child sexual exploitation, discriminatory abuse and hate speech, grooming, harassment, stalking, blackmail, catfishing, unwanted sexual advances, location sharing, cybercrime, fraud, scams, phishing, surveillance by state, public and commercial institutions).

Conduct risks: a child or young person is involved in an exchange, often, but not always, peer-to-peer, as either a perpetrator or victim, sometimes both (e.g. bullying, sexting, revenge porn, trolling, threats and intimidation, baiting, dog-piling, privacy breaches, impersonation, social humiliation, loss of control of personal data, loss of control of digital legacy/footprint)**.**

Contract risks (also referred to as commercial risks): a child or young person is exposed to inappropriate commercial contractual relationships or pressures (e.g. compulsive use,

[6] Internet Safety Strategy, HM Government, October 2017-2019

gambling, targeted advertising, aggressive marketing schemes or hidden costs, misuse and misappropriation of intellectual property, unfair terms and conditions, weighted search rankings, undisclosed and/or opaque marketing and advertising, inaccurate or discriminatory socio-economic profiling, unfair automated/semi-automated decision-making and data set training, misuse of personal data).

Contract risk includes commercial drivers that create design norms that children are not developmentally able to manage or absorb without harm.

Harms

A harm is anything that negatively impacts on the health, wellbeing and/or safety of a child. Risks may cause one or a series of harms. They include:

- Loss of confidence
- Isolation
- Sleeplessness
- Over-exposure and over-sharing
- Stress
- Anxiety
- Depression
- Family conflict
- Diminished empathy
- Poor fine motor skills
- Aggression
- Opportunity cost
- Diminished memory, concentration and ability to focus/engage
- Obesity
- Self-harm
- Violent extremism
- Suicide/suicidal ideation
- Misogyny
- Reputational damage
- Loss of autonomy
- Sexual exploitation
- Violence/fear of violence
- Sexual assault
- Addiction/compulsion
- Emotional difficulties/distress
- Behavioural difficulties/distress
- Financial loss
- Permissive and unrealistic sexual attitudes
- Gender-stereotypical sexual attitudes
- Maladaptive attitudes to relationships
- Susceptibility to advertising
- Self-exclusion/self-editing
- Unrealistic body image/pressure to conform to narrow body image
- Discrimination

Primary Sources:

Growing Up With The Internet, Select Committee on Communications [HL], 2017
Mental Health of Children and Young People in England, NHS, 2018
Girls Attitude Survey 2018, Girl Guiding, 2018
Safety Net: Cyberbullying's Impact on Young People's Mental Health, The Children's Society, 2018
Children and Parents: Media Use and Attitudes Report, Ofcom, 2017
Impact of Marketing Through Social Media, Online Games and Mobile Applications on Children's Behaviour, European Commission, 2016
The Datafied Child: The Dataveillance of Children and Implications for Their Rights, New Media and Society, 2017
Young People's Experiences of Online Sexual Harassment, Project deSHAME, 2017
How Technology Hijacks People's Minds, Tristan Harris, 2016
Growing Up Digital Alberta, Harvard Medical School, 2016
Association Between Portable Screen-Based Media Device Access and Sleep Outcomes, JAMA Pediatrics, 2016
Smartphone and Tablet Use: Associations with Sugary Drinks, Sleep, Physical Activity and Obesity, Harvard School of Public Health, 2017

Issue Paper on Youth Radicalisation, Radicalisation Awareness Network, 2018

Using the Internet to Access Information Inflates Future Use of the Internet to Access Other Information, Memory, 2017
Mobile and Interactive Media Use on Young Children, Pediatrics Journal, 2015
The Influence of the Internet on Self-Harm and Suicide, PLOS One, 2013
Increase in Depressive Symptoms, Suicide-Related Outcomes and Suicide Rates… and Links to Increased New Media Screen Time, Association for Psychological Science, 2017

Conflict, Friendships and Technology, PEW Research Center, 2015

The Selfie Generation: Examining the Relationship Between Social Media Use and Early Adolescent Body Image, The Journal of Early Adolescence, 2018
Social Media Use and Perceived Social Isolation, American Journal of Preventive Medicine, 2017
Girls' Experience of Harassment and Bullying Online, Plan International UK, 2017
Managing Expectations: Technology Tensions Among Parents and Teens, University of Michigan, 2016
Surgery Students Are Losing Dexterity, BBC News, 2018

Most approaches to militate against harm are constructed as if harm is an individual harm created by an individual service experienced by an individual user. However, it is also important to consider cumulative harms to an individual, harm(s) to specific communities and harm(s) to society as a whole. For example; a child may be overwhelmed by several services aggressively competing for their attention; algorithmic bias may discriminate against a specific user group (e.g. girls, BAME); technology that distributes fake news may polarise public debate or undermine democracy. Policy must reflect the full gamut of ways in which harm manifests.

Often, when defining harm, the expression 'extreme harm' is used to separate harms that must be tackled, from those (lesser) harms that must be tolerated. This analysis fails to account for interactions that "prime" children's brains, teaching habits that may harm them in the future nor the impact of cumulative harms, nor does it allow for the different tolerances of children, who respond differently when confronted with the same circumstances, including responding in an extreme and sometimes tragic manner to what appears to be an inconsequential event.

Children's rights are deliberately conceived as non-hierarchical so that a child is protected against *all* negative impacts on their wellbeing. A successful safety strategy must seek to deal with extreme harms and everyday (quotidian) harms by minimising risk, upholding rights and putting the 'best interest of the child' above any other consideration.

Seven Pillars of Safety

No environment can be made entirely risk free. However, in a rapidly evolving digital-first world, government, business and civil society can and should do much more to support children in the digital environment. A failure to do so is a failure to uphold the privileges, protections and undeniable rights that define childhood.

A policy response based on the following seven pillars of safety would transform the relationship between children and the technology they use, and would fulfil Government's promise to "make Britain the safest place in the world to be online",[7] whilst respecting the benefits and creativity of digital technologies. Each of the seven pillars cut across all the risks and harms identified above.

First Pillar: Parity of Protection

Parity of standards between online and offline[8] should require the norms and expectations of society to apply in online settings. To differentiate societal expectations and values in online and offline settings is to misunderstand the way in which technology impacts on society. We live not on and offline, but in a reality that is organised, interrupted and augmented by technology. Therefore, to deliver on any societal contract (e.g. democracy, rights, rule of law, childhood), standards and expectations have to apply seamlessly on and offline, even if the practical implementation of agreed standards differ according to setting.

Harmonisation and clarification of existing regulation are required to address the disparity of standards. For example, Ofcom (2018) highlighted "significant disparities in whether and how online content is regulated".[9] As a result, a wide range of popular online content is subject to no UK regulation at all, and in other cases the same piece of content is subject (or not) to regulation based only on its delivery format. This 'different screen, different rules' approach provides no clear level of protection for viewers and fails to meet consumer expectations (as reported by the BBFC) that protections offline should be replicated online.[10]

The Law Commission for England and Wales' Scoping Report on Abusive and Offensive Online Communications called for reform and consolidation of existing criminal laws to achieve parity of protection.[11] In answer to a Parliamentary question, Government confirmed that Section 6 of the Health and Safety at Work Act 1974 (which places duties on any person who designs, manufactures, imports or supplies any article for use at work to ensure that it will be safe and without risks to health) "applies to artificial intelligence and machine learning software".[12] Thereby confirming the application of existing regulation to online scenarios. Government has yet to respond to similar questions as to the relevance of the Equality Act 2010 and the Consumer Rights Act 2015.[13]

[7] Page 77, Forward Together: Our Plan for a Stronger Britain and a Prosperous Future, The Conservative and Unionist Party Manifesto 2017
[8] Page 4, Government Response to the Internet Safety Strategy Green Paper, May 2018
[9] Page 3, Addressing Harmful Online Content, Ofcom, September 2018
[10] BBFC, The Internet: To Regulate or Not To Regulate, House of Lords Select Committee on Communications, 8 June 2018
[11] Scoping Report on Abusive and Offensive Online Communications, Law Commission, 1 November 2018
[12] Industrial Health and Safety: Artificial Intelligence: Written Question – HL8200, 5 June 2018
[13] Hansard, Volume 794, Column 34, Artificial Intelligence (Select Committee Report) [HL], 19 November 2018,

At an international level, 5Rights Foundation is supporting the United Nations Committee on the Rights of the Child in writing a General Comment that will formally outline the relevance of the Conventions' articles for the digital environment.[14]

A strategy of clarification, harmonisation, consolidation and enhancement of existing agreements, laws and regulations would underpin the parity principle and deliver offline norms and expectations in online settings. Parity could also be supported by:

Publishing guidance on a sector-by-sector basis to confirm where existing law is applicable in online settings and filling gaps where there is a lack of clarity. Guidance should have particular regard to criminal, health and safety, equality and consumer legislation, as well as unfair business practices and children's rights.

Bringing forward an overarching harmonisation bill to require all legislation to be interpreted in a manner that creates parity of protection and of redress for unlawful acts, irrespective of whether they occur on or offline. Such legislation would operate in a similar way to Section 3 of the Human Rights Act 1998, which creates an obligation to interpret existing law in a way that is compatible with human rights, to the extent that it is possible to do so.

Creating a duty of care for the digital environment. William Perrin and Professor Lorna Woods have pointed to the well-established concept of duty of care in "the physical world".[15] The argument that this duty would drive a precautionary approach which would result in better safety by design and default, is well-founded. Such a duty could usefully cover the digital ecosystem and should extend beyond a handful of major online services.[16]

Working internationally to share definitions and protocols across borders to improve global coordination. The Child Dignity Alliance's Technical Working Group report on preventing Child Sexual Abuse Material (CSAM) outlines the way in which variations in the classification of CSAM hampers detection and take down; the report makes powerful recommendations to adopt international approaches and definitions.[17] In another context, the Select Committee on Artificial Intelligence report, AI in the UK: Ready, Willing and Able? outlined the problems inherent in the UK's definition of autonomous weapons.[18] These are just two of many areas that would benefit from a commitment to agreed international wording and definitions.

Parity of enforcement on and offline (see Fourth Pillar: Enforcement).

[14] General Comment on the Digital Environment, 5Rights Foundation

[15] The Internet: To Regulate or Not To Regulate? Professor Lorna Woods and William Perrin, House of Lords Select Committee of Communications, 30 May 2018

[16] Baroness Kidron, Hansard, Volume 793, Column 1766 - 1768, Social Media Services [HL], 12 November 2018

[17] Technical Working Group Report, Child Dignity Alliance, 16 November 2018

[18] Paragraphs 334-346, AI in the UK: Ready, Willing and Able? House of Lords Select Committee on Artificial Intelligence, Report of Session 2017-2019, 16 April 2018

Second Pillar: Design Standards

Safety, privacy, security and rights by design and by default. The argument for services and devices to be 'better by design and by default' is very advanced and has a broad set of advocates (see Box A). Better by design and by default follows methodology widely used in many other settings, for example, building regulations,[19] drivers' hours,[20] food safety standards[21] and offshore diving.[22] In the digital environment the universal adoption of Content Accessibility Standards transformed the online experience of those with disabilities.[23]

Designing the digital environment to meet the needs of children is sometimes characterised as a hazard to free speech.[24] However, a child's right to freedom of expression is not a standalone right. It sits alongside a broad spectrum of rights, including; privacy, the right to be shielded from inappropriate content in accordance with their development stage, protection from all forms of physical and mental violence, the right to rest, leisure and play, the highest attainable standard of health and development, and protection from economic exploitation. [25]

5Rights fully supports a child's right to freedom of expression, however it does not have automatic priority over other rights, nor is it unlimited. For example, Article 10(1) of the European Convention on Human Rights (ECHR) expressly envisages the regulating of certain forms of mass media. Freedom of expression allows the state to consider it against other societal interests, and in some instances requires it; provided the intrusion is proportionate to the need; and for it to be balanced against other rights.[26] In the context of mass media, the ECHR has held that the state must be the ultimate guarantor of pluralism and where necessary, regulate to ensure that some voices/world views are heard.

The interpretation often put forward by the technology sector that all views are equal, unlike the ECHR judgement, fails to recognise the inequalities of power between users. Specifically, it does not allow for the vulnerabilities and immaturities associated with childhood. The vast majority of the content online is created by adults for adults which has resulted in a sexualised, polarised and commercialised digital environment. Realising children's right to express themselves whilst simultaneously upholding their right to be protected from inappropriate content[27] requires the technology sector to first recognise the presence of children as a user group, then to respond to differences in capacity between children of different ages - only then can it be an environment in which all children can enact their right to express themselves. For example, the digital environment has been proven hostile to girls, particularly in their teens,[28] which means that the most important place of public discourse is a place where girls and young women feel uncomfortable or prevented

[19] Building Regulations 2010
[20] Driver's Hours Regulations 2014
[21] Food Standards Agency Guidance
[22] IMCA Code of Practice for Offshore Diving 2014
[23] Web Content Accessibility Guidelines (WCAG 2.0), HM Government, 3 October 2017
[24] Google, Responses to the Call for Evidence on the Age Appropriate Design Code, Information Commissioner's Office, 2018
[25] Articles 13, 16, 17(e), 19, 31, 24, 27 and 32. Convention on the Rights of the Child, 1990
[26] Campbell v MGN Ltd [2004] 2 WLR 1232; Paragraph 17, Re S (FC) [2004] UKHL 47
[27] Articles 13 and 17, Convention on the Rights of the Child, 1990
[28] Girls Attitude Survey 2018, Girl Guiding, 2018

from expressing their views.[29]

Design standards must not be restricted to content. System design that pushes behaviour (e.g. endless feeds, aggressive pushes and notifications[30]); device security (e.g. smart toys that stream[31]) or default privacy settings (e.g. system changes at operating system or device level that could promote privacy[32]) are all areas that get less policy and media attention than content standards, but arguably have a greater impact on the safety, security, rights and wellbeing of children.

BOX A: Better by design and by default

- The Department for Digital, Culture, Media and Sport's report Secure by Design (2018)[33] found that privacy concerns are given low priority in the design process and that manufacturers and suppliers have few incentives to prioritise built-in security.
- Australia's eSafety Commissioner, Julie Inman-Grant, in the Child Dignity report (2018), stated that industry's role is not limited to simply developing tools, they should be "expected – and possibly mandated by government – to ensure they take proactive steps to combat CSAM" and other harms.[34] The report recommends that technical data relating to CSAM should be treated as 'global assets', i.e. be shared and placed at the disposal of all parties involved in fighting, regardless of sector.[35]
- Center for Humane Technology shows how system design "follows norms that bias towards collecting data rather than protecting privacy" with profound societal and individual damage, and argue for systemic change in design norms.[36]
- The Information Commissioner, Elizabeth Denham, said in explaining the potential of the Age Appropriate Design Code to design rights into the system, "people should have the same rights online as they have offline."[37] Giving voice - on behalf of children - to the principle in the General Data Protection Regulation (GDPR) that requires safety and security by design as a matter of law.[38]
- The same principles used by the Government's Behavioural Insights Team to encourage people to make better choices for themselves and society could be harnessed by government and tech companies to design better/safer services.[39]
- 83% of 11-12 year olds are in favour of platforms removing offensive or abusive content or direct messages automatically, without the need for a user complaint to be made first and for this to be the default setting.[40]

[29] Dink v Turkey (Application Numbers: 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09), Judgment 14 September 2010
[30] Chapter Three, Disrupted Childhood: The Cost of Persuasive Design, B. Kidron, et al, 5Rights, June 2018
[31] #WatchOut: Analysis of Smartwatches for Children, Norwegian Consumer Council, October 2017
[32] Snap Response to the Information Commissioner's Call for Evidence on the Age Appropriate Design Code, September 2018
[33] Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report, Department for Digital, Culture, Media and Sport, 2018
[34] Technical Working Group Report, Child Dignity Alliance, 16 November 2018
[35] Recommendations 3 and 8, Technical Working Group Report, Child Dignity Alliance, 16 November 2018
[36] Center for Humane Technology's Response to the Information Commissioner's Call for Evidence, 21 September 2018
[37] Question 116, Oral Evidence, Elizabeth Denham to the House of Lords Select Committee on Communications, The Internet: To Regulate or Not To Regulate? 11 September 2018
[38] Articles 25 and 32, Recital 78, Regulation (EU) 2016/679 (General Data Protection Regulation)
[39] Our Work, Behavioural Insights Team
[40] Children's Views on Internet Safety, British Computer Society, February 2018

Security, safety and privacy by design and default can be achieved by the introduction of a number of well-established approaches:

- A duty of care imposed upon providers of digital services in respect of their users, enforced by a regulator from which would flow a regime that includes;[41]
- Impact assessments to identify and mitigate against risk, especially for vulnerable or young users, as part of the design process.
- Ethical standards on Autonomous and Intelligent Systems (A/IS)[42] such as those being created by 5Rights/IEEE's programme of Universal Standards for Children and Adolescents, or by the European Commission.[43]
- Tools that support user autonomy through settings that respect children's need for time off, time on uninterrupted and privacy time e.g. apps with automatic time-out, less pervasive notifications and nudges.[44]
- Rating and labelling aspects of online environments e.g. privacy standards, sharing policies, age-ratings, violent content, etc., to give clearer indication of the environment that a user is entering.
- Standardised reporting and resolution procedures including: visibility, response times, penalties, oversight and appeal.
- Certification[45] offers a speedy way for users to make an informed decision about a service, offers online services a way of ensuring that they have met the required bar, and will engender trust in service.
- Enforcement (see Fourth Pillar).
- Universal standards (see Minimum Universal Design Standards below).

Tools that require additional or complex user decisions and actions do not contribute to a safety by design and by default model.[46]

Addressing the design of each player/stakeholder/technological layer in the value chain would identify and allocate responsibilities for safety to each party, based on where changes to their specific design features would have the most impact.

In their submission to the ICO's call for evidence on the Age Appropriate Design Code, Snap Inc. identified four layers of technology that users are required to pass before reaching the app itself; the mobile operator, the hardware, the operating system and the app store, saying:

"Children, by and large, do not buy their own phones. At the point of purchase, the purchaser (usually the parent or carer) should be guided through the options to configure, in an age-appropriate manner, the phone's safety parameters using the operating system tools provided, including linking to a family account controlled by a parent/carer for young children.

[41] Professor Lorna Woods and William Perrin, The Internet: To Regulate or Not To Regulate? House of Lords Select Committee of Communications, 30 May 2018
[42] IEEE Standards Association and MIT Media Lab Form Council on Extended Intelligence, 17 September 2018
[43] High-Level Expert Group on Artificial Intelligence, European Commission
[44] Nudge: Improving Decisions About Health, Wealth and Happiness, R. Thaler, C. Sunstein, Penguin Random House, 24 February 2008; The Power of Nudges, for Good and Bad, R. Thaler, New York Times, 31 October 2015
[45] Generation AI: What Happens When Your Child's Friend is an AI Toy that Talks Back? World Economic Forum, May 2018
[46] Deceived By Design, Norwegian Consumer Council, June 2018

"Similarly, children, by and large, do not sign up for mobile data subscriptions. At the point of purchase, small changes to the purchase flow could be designed so that the purchaser would be guided through the options to configure, in an age-appropriate manner, both the phone's safety parameters using the operating system tools, as well as the mobile network operators' own tools, such as age gates, white/black lists and parental filters.

"A user's first interaction with an app store is another key pinch point through which all users must pass before they can install apps on their phones. There are only two app stores, run by the two operating system providers - Apple and Android. Introducing the two companies' comprehensive family suites of safety and wellbeing tools - age gates, screen time limiters, downtime setting, monitoring app downloads and in app purchases, white/black lists, etc - when signing up to the app stores would catch any new users who somehow fell through the first two points-of-purchase gates."[47]

Whilst 5Rights believes that the measures as set out by Snap Inc. rely too much on parental supervision rather than greater corporate responsibility by default, they usefully point to a much-needed intervention at each layer of the system. When speaking to Snap's leadership in November 2018, Young Scot 5Rights Youth Leaders explained that such measures would only work in concert with better design of all online information services. A point recognised in the recent revision of the Audiovisual Media Services Directive, that (partially) extends regulation of 'video-sharing platforms' – including the requirement for "transparent and user-friendly mechanisms" in relation to the flagging of videos as inappropriate.[48]

5Rights urges government to consider a system in which each technology layer is required to provide ***age appropriate design by default***, and not miss out any technological layer.

Minimum universal design standards have been called for by many safety campaigners, including NSPCC[49] and the Child Dignity Alliance Technical Working Group.[50] Creating standards that encompass safety and security is the norm in almost every other sector (e.g. oil, airline, food, nuclear). Common standards are especially important in the global digital environment where companies trade across borders.

The Age Appropriate Design Code introduced into the Data Protection Act 2018 requires online services to offer the highest bar of data protection, in a way that reflects the best interests of the child to meet their changing development needs and to uphold their rights under the UNCRC. [51] Data is the driver behind most commercial (and increasingly public sector) design decisions, and therefore data protection regimes can transform the design culture. For example by:

- Introducing high privacy by default

[47] Snap Inc, Response to the Information Commissioner's Call for Evidence on the Age Appropriate Design Code, 18 September 2018

[48] Article 28b(d), Directive (EU) 2018/1808, [2018] OJ L303/69

[49] How Safe Are Our Children? NSPCC, 2018

[50] Technical Working Group Report, Child Dignity Alliance, 16 November 2018

[51] Articles 3 and 5, Convention on the Rights of the Child, 1990

- Defining data minimisation to mean that data is collected only for the child's primary/first and intentional use
- Preventing visible, real-time GPS tracking of children
- Mandating automatic time-outs
- Prohibiting commercial profiling of a child
- Age rating games and services adult-only where the game uses aggressive data collection loops that make them compulsive.

The Information Commissioner's Office has published the responses to its call for evidence. With the exception of the major digital platforms and their industry representatives, there was broad support for the Code. Respondents echoed 5Rights' concern about the widespread deployment of personalised persuasive design strategies that undermine a child's exercise of free will by designing services to be compulsive in order to maximise opportunities for data collection. Respondents cited research that highlighted negative impacts upon children, including; interrupting their activities, sleeplessness and lowered self-esteem. We hope that the Information Commissioner will take the evidence of harm as a strong mandate for setting robust standards.

The Government's response to the Internet Safety Strategy Consultation acknowledges the contribution of the Age Appropriate Design Code to protecting children. Adopting it's systemic and pre-emptive approach, and its ability to tackle a number of interrelated risks, offers a precedent that could be applied more broadly to safety issues.

Innovation and investment need not be stifled by safe digital service design. On the contrary, Sir Tim Berners-Lee,[52] Tristan Harris,[53] Senator Mark Warner,[54] US Financial Conduct Authority (FCA),[55] Farhad Manjoo,[56] House of Lords Communications Committee,[57] George Soros,[58] Foursquare co-founder, Naveen Selvadurai and former Facebook employee, Josh Lee,[59] believe that innovation is fettered by having a few dominant players.

The number of investments in internet and mobile social companies has been steadily declining since 2014; global investments in 2017 in this sector were just $693 million - less than half of 2014's $1.4 billion.[60] Innovation relies upon a well-functioning market and markets do not work well when the cost of a company's product is not borne by them. In much digital safety work we see costs of the impact of products and services on children being left to society to pick up. Internalising these external costs will help the market function better and support innovation.

[52] World Wide Web Foundation
[53] Tristan Harris Essays
[54] Potential Policy Proposals for Regulation of Social Media and Technology Firms, U.S. Senator Mark Warner, 30 July 2018
[55] The Big Tech Competition Dilemma, Financial Conduct Authority, 1 November 2018
[56] How the Frightful Five Put Start-Ups in a Lose-Lose Situation, New York Times, 18 October 2017
[57] UK Advertising in a Digital Age, House of Lords Select Committee on Communications, 11 April 2018
[58] Remarks Delivered at the World Economic Forum, 25 January 2018
[59] Will Facebook Kill All Future Facebooks? WIRED, 25 October 2017
[60] Ibid

It is crucial that the Internet Safety Strategy does not characterise online safety and innovation as two mutually exclusive concepts that must be balanced, but rather harness the understanding that safety, rights and ethics - by design and default - *reinforces* innovation and investment. Introducing ethical standards would necessitate different business models and different values to emerge to create a more diverse, and therefore more competitive, sector. On occasions where there is a genuine conflict between innovation and online safety, it is government's role to find in favour of the best interests of the child.[61]

Consideration should also be given to whether an innovation is an innovative service or technology, or simply an innovative business model that is avoiding local laws and regulations.

Third Pillar: Accountability

Accountability is sometimes proffered as a principle. In the context of this paper it is construed as an obligation backed up by enforcement (Fourth Pillar).

Accountability as an obligation. Because the technology sector benefits from its historic protections from liability, it has been able to operate without being accountable for the consequences of its impacts,[62] or as the sector calls it, "negative externalities".[63] In the absence of a regulatory environment in which platforms have liability for their actions, a number of obligations could usefully be put on the sector to improve accountability. The GDPR, in Article 5(1) sets out principles and then in paragraph 2 requires that "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1" (i.e. accountability). This principle should be articulated in each specific area of activity, design and service, and, in doing so, incentivise equitable, proactive and safe design by default.

A regulatory backstop for community guidelines. Companies rely on community guidelines, terms and conditions and privacy notices to set standards of content, conduct, contact and contract. These vary greatly from site to site, service to service, and among different players in the value chain; but invariably they do not give users any indication of how successfully the published standards are delivered. For example, Facebook's published guidelines prohibit hate speech and disinformation,[64] yet these guidelines aren't adequately enforced. A Channel 4 investigation, *Inside Facebook: Secrets of the Social Network,*[65] found graphic video footage of child abuse being shared thousands of times, and racist content and hate speech that received special protection when posted on popular accounts and pages - including those of Britain First and Tommy Robinson.[66] The investigation also found clips of people eating live animals, school bullies beating up victims and images of self-harm and eating disorders - all of which contravened Facebook's community guidelines.[67]

[61] Article 3, Convention on the Rights of the Child, 1990
[62] Electronic Commerce Directive 2000/31/EC
[63] What Is To Be Done? Safeguarding Democratic Governance in the Age of Network Platforms, Hoover Institution, 13 November 2018
[64] Facebook, Community Standards; Objectional Content
[65] Inside Facebook: Secrets of a Social Network, Firecrest Films, 17 July 2018
[66] Britain First's Facebook page had almost 2 million likes. Facebook Bans Britain First and Its Leaders, The Guardian, 14 March 2018. Tommy Robinson's Facebook page has almost 1 million likes and over 1 million followers.
[67] Channel 4: Inside Facebook's Social Network Revealed Disturbing Posts, The Telegraph, 17 July 2018

Also in contravention of the minimum joining ages of 13 or 16 years old,[68] 46% of UK children have a social media profile by the age of 11 and by 12 it is 51%.[69]

A regulatory backstop for community rules would offer a powerful way of changing the culture of the online world. This would allow companies the freedom to set their own rules as they wish, but ***routine failure*** to adhere to their own published rules (including content or conduct standards, terms and conditions, age restrictions and privacy notices) would be subject to enforcement notices and penalties. Under this regime, terms that they cannot adequately define would be disallowed and age-rating encouraged.

Mandated transparency reporting against predetermined measures would foster cultural change. For example, research by sociologists at Washington University found that salary transparency raised wages, in part because "being cognizant of gender pay disparity" helped change norms.[70] Reporting standards must cover specific groups, specific harms, and harms to communities and groups of people, as well as set expectations on time limits for reporting, response and outcomes. It must make clear the numbers of complaints, characterise where they have come from, how they have been addressed, to what level of satisfaction of the complainant, and the level of human moderation both before and after the complaint.

Transparency reporting is not a substitute for design standards, impact assessments, certification or any of the other pillars of safety: it is a limited, after-the-event provision.

Regulator powers to demand information where it is necessary to come to judgements in relation to promises made in published community guidelines, terms and conditions, privacy notices, age restrictions, company advertising or published information about services. For example, proprietary safety provisions provided by the technology sector are not subject to independent evaluation or oversight.[71]

Health warnings should be mandated by government (against harms as laid out in Harms) in a similar manner as the drug, food and tobacco sectors are mandated to publish known side-effects, allergies and known harms.

Research access to commercial data would reverse the lack of data currently provided by platforms. Creating a public interest data access law would allow independent, public interest researchers to be licensed to access activity data on platforms.[72] This would ensure that problems on the platforms were identified and evaluated by researchers and academics. Implementation of currently private solutions would also be subject to independent oversight. Data and analysis generated could inform policy and regulatory priorities.[73]

[68] Children and Parents: Media Use and Attitudes Report, Ofcom, 29 November 2017
[69] Page 102, Children and Parents: Media Use and Attitudes Report, Ofcom, 29 November 2017
[70] The Power of Transparency, J. Rosenfeld, P. Denice, American Sociological Review, 1 September 2015
[71] The Corporate Accountability Index 2018, Ranking Digital Rights 2018
[72] Approved Researcher Scheme, Office for National Statistics,
[73] Potential Policy Proposals for Regulation of Social Media and Technology Firms, U.S. Senator Mark Warner, 30 July 2018

A public data regime with regulatory oversight. Government has a particular duty of safety and accountability relating to public service information data. There is considerable disquiet about uses of pupil and health data and the lack of joined up provision for children across health and social care. For example, the Department for Education suspended access to the National Pupil Database in June 2018[74] after thousands of children's identifiable personal data (including ethnicity, SEN status and eligibility for free school meals) was collected and provided to commercial companies, journalists and academics.[75] Data was also provided to the Home Office for immigration enforcement.[76] Similar concerns have also been raised about public health data most notably in the case of DeepMind and The Royal Free Hospital Trust.[77]

Outlining a public information regime with clarity over the rules and regulatory oversight would restore trust and confidence in government's own responsibilities for online safety and children's rights.

Fourth Pillar: Enforcement

Whilst some companies have taken steps to improve the safety of their services, they have largely done so in response to public outrage at a particular incident. Over many years, online service providers have failed to offer a proactive, comprehensive or measurable safety regime. When challenged on the failure of self-regulation, online services routinely say they "respect the laws of the jurisdictions in which [they] operate".[78] This indicates the need for an enforceable regulatory response. A credible regulatory regime is based upon enforcement that is respected and considered effective by those who are regulated. Enforcement combines a regulator with adequate resources and expertise and a robust tool kit of regulatory penalties. The technology sector can look to other regulatory regimes with penalties designed to bite on large corporations, such as the criminal penalties on companies failing to prevent financial crime[79] and in health and safety law where offences can apply personally to the Directors of the company.[80]

Many organisations and stakeholders have put forward views on how to structure regulatory oversight,[81] any enforcement regime must:

- Be based on the seven pillars as outlined.
- Tackle each of the categories: content, conduct, contact and contract; with risks identified and defined by Parliament or a regulator, not private companies.
- Ensure that vulnerable users benefit from a higher-than-standard level of protection.
- Introduce significant penalties for services that fail to meet the required standard.

[74] Sharing of School Pupils' Data Put On Hold, BBC, 15 May 2018
[75] State of Data 2018: Report for Policy Makers with a View to GDPR in Education, Defenddigitalme, 13 May 2018
[76] School Census Data, October 2016
[77] NHS: Healthcare Data, Hansard [HL], Volume 792, 6 September 2018; Artificial Intelligence (Select Committee Report), Hansard [HL], Volume 794, 19 November 2018
[78] Sundar Pichai Response to Senators Regarding China, 31 August 2018
[79] Bribery Act 2010; Corporate Criminal Offences in the Criminal Finances Act 2017
[80] Health and Safety at Work Act 1974 Section 37
[81] The Internet: To Regulate or Not to Regulate? House of Lords Select Committee on Communications, 2018

- Reflect the fact that complex companies with interrelated services must be considered both in relation to their individual services and cumulative control and power.
- Recognise that trust in the system is dependent upon upholding/creating societal norms and expectations, therefore it is the intention of the user/citizen that must be privileged, rather than the desires of service provider - and it must be fair and equitable in its impact.

Parity of enforcement. While UK cybercrime represents around half of the total crimes that happen to people in the UK,[82] police report only being able to investigate 4% of the cases they receive, and only 57 cybercrimes have been prosecuted.[83] A commitment to police training and investment in enforcement for cybercrime would serve to make clear that online behaviour has consequences. The Law Commission's report states that "criminal law has an important role to play in setting standards and deterring and punishing unacceptable online conduct" and, most importantly, that society will change when prosecutions are brought.[84]

'Levelling up' regulation can create a commercial advantage for those subject to it, and it also serves to spread best practice elsewhere. For example, rather than isolate the EU, the introduction of the GDPR has spread good practice internationally, upgrading data protection and impacting on service design around the world. It is likely that the introduction of safety regulation will act in a similar manner and create a market for new, safety-conscious digital offers.

Resourcing regulation. Well-funded regulators are essential to effective regulation. Since the 1970s, the 'Polluter Pays' principle[85] has met with widespread acceptance as the most efficient method of mitigating external costs created by corporate activity.[86] Regulators should be able to recover costs of regulating from those that they regulate, and Parliament should create mechanisms to support any new regulation in this manner. Tax revenue should come via the anticipated international tax reforms for internet companies, and should support central government more generally.[87] A certification scheme would also usefully provide a flow of funds to support regulation.[88]

Law enforcement and Child Online Protection

Whilst what is illegal sits outside the terms of reference of the Government's Safety Strategy, it is worth noting that a definition of terms, mitigating risks, safety by design, the introduction of universal standards, robust data protection, access to commercial data, effective reporting monitoring and take down, ubiquitous support services for children and better public awareness are routinely cited by the enforcement community as essential to in the fight

[82] British Police Are On The Brink Of A Totally Avoidable Cybercrime Crisis, WIRED, 22 August 2018
[83] Oral Evidence: Policing For The Future, Home Affairs Committee, 19 June 2018
[84] Abusive and Offensive Online Communications, Law Commission, September 2018
[85] Recommendation of the Council on the Implementation of the Polluter Pays Principle, OECD, 14 November 1974
[86] What Is The Polluter Pays Principle? London School of Economics, 11 May 2018
[87] Digital Services Tax: Consultation, HM Treasury, 7 November 2018; Hammond Targets US Tech Giants With 'Digital Services Tax', The Guardian, 29 October 2018; Big Tech's Next European Nightmare: A Tax on Revenues, CNN, 31 October 2018
[88] Professor Lorna Woods and William Perrin, The Internet: To Regulate or Not to Regulate? 30 May 2018

against CSA, CSAM, radicalisation, hacking, blackmail, financial scams, and other illegal online activities that effect children.

Fifth Pillar: Leadership

Leadership in government is required to respond to the digital-related challenges and impacts in society. Several government departments have a role to play, for example, the Department for Digital, Culture, Media and Sport; the Home Office; the Ministry of Justice; the Department of Health; and the Department for Education. Clarity about who is responsible for delivery and accountable for impact within each department, including named leads, is critical. How these knit together and where the final authority lies is necessary to ensure that government's response is coherent and coordinated.

Critical oversight is urgently needed. A child-focused body is required, resourced with staff and funds, to carry out research and make policy recommendations against predetermined, long-term objectives and to support the work of all departments to develop and implement evidence-based, consistent policy across government. Such a body would put the views and experiences of users (under 18s) at the heart of its work and it would work closely with, but not be directed by, industry. This work should be backed by statutory powers, including the power to require disclosure of information and people to appear before it. Such a body would provide critical leadership and ensure that all stakeholders (including government and industry) were held accountable for progress.

We note the number of different initiatives and taskforces announced by Government. The way these finally inform and change public policy should be joined up, incorporate diverse voices including those of children and be subject to scrutiny.[89]

Clarity on regulatory responsibility. There is an ongoing discussion about whether a new dedicated internet regulator is needed or whether existing regulators should be required to take on new responsibilities.[90] However responsibilities are allocated, it is critical that there is clarity so that the public knows who to turn to, and all in the digital ecosystem know to whom they are accountable.[91]

Global leadership and governance structure. 5Rights supports Government's commitment to advocate for a more robust international response to online safety. But we note that even global initiatives have become fragmented. Probably the most effective body in tackling tech's overarching power is the EU. Post-Brexit, the UK should seek the closest possible ties with Europe in this policy area whilst still working toward a global response.

[89] Lord Stevenson of Balmacara at Column 57, Artificial Intelligence (Select Committee Report) [HL], Volume 794, 19 November 2018

[90] The Internet: To Regulate or Not to Regulate, House of Lords Select Committee on Communications, 2018

[91] Ibid; Keeping Consumers Safe Online: Legislating for Platform Accountability for Online Content, M. Bunting, July 2018

Sixth Pillar: Education

Education is a key component of any safety strategy. However, it is frequently used to demand that users, particularly children, be resilient to a system that does not respect or protect their safety and security. For example, the then Secretary of State, Rt Hon Karen Bradley MP, supported Facebook's provision of £1 million to train Digital Safety Ambassadors to "enable young people to look after themselves and their peers" as part of the media campaign to announce the Internet Safety Strategy Green Paper.[92] The donation came as Facebook faced criticism from MPs for failing to combat online abuse[93] and from both the BBC and NSPCC for failing to remove clearly abusive content.[94] Currently, there is concern about Google's suite of educational programmes deployed widely in UK and US schools.[95] The programme "presents Google as impartial and trustworthy"[96] yet the programme emphasis the risks to children from milling actors and does not adequately address the risks associated with the sector norm, such as profiling, compulsion, the impacts of data collection, or sharing GPS location.

A comprehensive school curriculum would address concerns about the quality, depth and consistency of education provision. A review of digital literacy programmes (including those offered in the curriculum in England, Scotland, Wales and Northern Ireland) by BT and 5Rights (2017)[97] found the overwhelming majority, 50 of the 73, covered e-safety; 17 looked at the impacts on personal wellbeing; nine considered digital rights and only one considered commercial drivers/design which are broadly understood to be at the core of many of the issues that children face online. There is considerable evidence that children want a very different approach to education; focused on the purposes of technology, and offering social and critical skills.[98] Education must not be used as 'tech wash' or as a substitute for robustly enforced design standards.

Tertiary education must introduce ethics and safety and rights by design modules to computer science and related disciplines at all levels, including degrees and professional qualifications.[99]

Professional training (for example, teachers, social workers, health and legal professionals) must include a broad understanding of the full range of opportunities and risks in the digital environment, including compulsive use. Training should be included as part of degree accreditation, professional standards and continued professional development (CPD).[100] This would be a fast and effective strategy to upgrade the understanding of adults with responsibilities for children and children's services.

[92] Internet Safety Strategy Green Paper, Department for Digital, Culture, Media and Sport, 11 October 2017
[93] Facebook, For Every UK Secondary School, The Drum, 16 October 2017
[94] Facebook, Anti-Bullying Training in Schools, BBC, 16 October 2017; Facebook, Cyber Bullying, The Telegraph, 16 October 2018
[95] Google, Bringing Online Safety Education Programmes to UK Schools, 27 February 2018
[96] Google, Teaching Children How to Act Online, New York Times, 23 October 2018
[97] The Right to Tech Literacy – A Framework for 8-13 Year Olds, BT, EdComs, October 2017
[98] Our ~~Digital~~ Rights, 5Rights Young Scot, May 2017; The Internet on our Own Terms, University of Leeds, University of Nottingham, 5Rights, January 2017
[99] Column 34, Artificial Intelligence (Select Committee Report) [HL], Hansard, Volume 794, 19 November 2018
[100] Disrupted Childhood: The Cost of Persuasive Design, B. Kidron, et al, 5Rights, June 2018

Information for parents contains conflicting messages about their child's interaction with the digital environment. On one hand, they are told that their child's future prospects depend on their ability to harness technology, on the other, headlines make extreme harms loom disproportionately large. Neither properly reflects the full spectrum of risk and opportunity online. Parents ask for quality and consistent messages and guidance on internet safety,[101] and more information and advice about technology, social media and how to discuss online activity with children.[102] They also express the view that companies make it hard to parent: "We set boundaries and when he is at home we can enforce them - not easily but eventually. When he is out of our sight it is a whole other issue and I resent having to 'police' him all the time. That isn't the sort of trusting parent I want to be."[103] It is important to note that some of the most at-risk children do not have parental support, and many of the sector information sources are partial.[104]

Government should make a single set of comprehensive messages and information available on the Government Digital Service website. This information should be practical, contain the concerns of children and be free of commercial bias.

Public awareness/education is needed to counter the volume of unethical and unbalanced media reporting. Disasters make powerful headlines, but at the same time, there is little coverage of the impacts of digital footprints, data regimes, targeting and the sheer volume of information gathered and shared or the amount of interaction demanded – with the corresponding the impact on user choice and opportunity. This is particularly true of guidance relating to children, who are over associated with a narrow set of online harms and little considered when discussing, data, privacy, fake news, hacking, AI ethics, security and cybercrime. Government could usefully work on a set of clear messages that are sophisticated, broad, non-hysterical and which signpost to its own resources.

Seventh Pillar: Evidence-Based Interventions

There is a growing body of evidence on harms.[105] While there is a need for further longitudinal research, it should not stand in the way of immediate action to protect users, or the steps necessary to promote children's wellbeing.[106] This is a young technology, but it is omnipresent and extremely powerful in dictating behaviours, facilitating contact and making available contracts and content that may not be in a child's best interest.

When looking for evidence on harms, government should consider the following:

- The design of a service is a powerful tool in creating and combating harm.
- There is deep and independent technological expertise outside the commercial

[101] New Guidelines to Help Industry Promote Internet Safety, UKCCIS, 7 February 2018; Cyberbullying Action Plan, The Royal Foundation's Taskforce on the Prevention of Cyberbullying, November 2017; Disadvantaged Children and Online Risk, S. Livingston, et al, LSE Research Online, 2011

[102] Adjust Our Settings, Queensland Anti-Cyberbullying Taskforce, September 2018

[103] Disrupted Childhood: The Cost of Persuasive Design, B. Kidron, et al, 5Rights, June 2018

[104] Google, Teaching Children How to Act Online, New York Times, 23 October 2018

[105] Children's Online Activities, Risks and Safety, S. Livingstone, et al, UKCCIS, October 2017; Youth Pathways into Cybercrime, M. Aiken, et al, October 2016; Research Summaries from the Evidence Group of the UKCCIS

[106] The Precautionary Principle: Protecting Public Health, the Environment and the Future of Our Children, World Health Organization, 2004

sector, namely in academia, standards organisations, professional groups and other sector experts.

- The sector would benefit from further longitudinal studies on the broader societal impacts of technology, including that of child development.
- Research must be, and be seen to be, independent of commercial actors.
- The ability to tackle harms at scale is hampered by a lack of access to commercial datasets. Government must be mandated to license research access to privately held data sets where it is in the public interest to do so.
- Habits learnt in childhood are difficult to unlearn.
- Academia, policy, government departments and regulators together hold deep expertise, but their siloed nature lacks broad overview or oversight.
- Regulation needs to be systemic, rather than dictated by headline or interest groups.
- Government departments must resist the temptation for short-term announcements.

Evidence from children and vulnerable groups who experience harm online must be meaningfully considered. Children and vulnerable groups should be consulted about their views, their experiences and the solutions they would like to see implemented. The outcomes of such consultations must be actioned. 5Rights Foundation's work with children[107] shows repeated calls from children for:

- Consistent community rules across platforms
- Proactive approach to enforcing community standards
- Commitment to stopping or slowing the spread of abuse
- Clear timelines for reporting and resolution
- Practical and emotional support for those who experience problems
- Better content labelling, including: age rating, content warnings, in-app purchases
- Better guidance on achieving a balanced digital life, and the potential mental and physical health risks associated with overuse
- Default settings that support and promote wellbeing (and an end to nudges that do not)
- Greater transparency on how online platforms make money, including the value of users' own behaviour
- Easy ways to take content down
- High default privacy settings
- Personal and portable terms and conditions
- More nuanced and bespoke ways of sharing content
- The ability to easily and quickly review and revise their digital footprints, including tracking the spread of photographs or hostile comments.

All of these measures are technically possible and could be designed into services, but both companies and Government have failed, thus far, to put them into action.

[107] Our ~~Digital~~ Rights, 5Rights Young Scot Youth Commission, 2016; The Internet on our Own Terms, University of Leeds, University of Nottingham, 5Rights, January 2017

Note on the Value of Data

When developing strategy initiatives, it is important to recognise that the data created by children has significant value (children represent 1/3 of all users globally[108]). Characterising data as a currency may go some way to ensuring that gathering, exchanging and holding data is done on equitable terms. Many of the behavioural design strategies that cause harms (as set out above) are deployed to increase the amount of data gathered on users. Government could usefully introduce the following practices:

- Define the user as a consumer with consumer rights.
- Recognise that children need protection from unmediated, direct relationships with commercial companies.
- Require companies that offer 'free' services in exchange for data to also offer an option to pay and those that don't should be given an equitable share of the value of what they are giving up.
- Require companies that charge for services, e.g. Netflix, Uber, Amazon, Apple TV, to protect user's data (as above) rather than double charge in data and subscription charges.
- Show transparency about a company's business model, and whether a conflict of interest exists between the safety of its users and its customers (the advertising industry)[109]
- Give users clarity about how the service is paid for.[110]
- Designate online platforms as "information fiduciaries", i.e. that they must "zealously protect user data" and "pledge not to utilize or manipulate the data for the benefit of the platform or third party".[111]
- Build on the work of US Senator Warner's proposal to regulate the use of corporate behaviour science, e.g. practices that condition user behaviour and design products to be intentionally habit-forming.[112]
- Create a universal contract for users who create content or provide data to have a value subscribed to their content or data.[113]

Making the value of a user's data more transparent will shift the dynamic; users will see themselves as discerning consumers with rights and expectations, and will require companies to be more selective about what they collect. This will result in a reboot of the rules of the attention economy.

[108] One in Three: Internet Governance and Children's Rights, S. Livingstone, et al, Unicef, January 2016

[109] Disinformation and 'Fake News'": Interim Report, Digital, Culture, Media and Sport Committee, House of Commons, Fifth Report of Session 2017-19, 24 July 2018; The Privacy Battle to Save Google From Itself, WIRED, 1 November 2018

[110] A New Deal for Big Tech: Next-Generation Regulation Fit for the Internet Age, Tony Blair Institute for Global Change, 1 November 2018

[111] Information Fiduciaries and the First Amendment, J. Balkin, Yale Law School, 2016

[112] Potential Policy Proposals for Regulation of Social Media and Technology Firms, U.S. Senator Mark Warner, 30 July 2018

[113] Ibid

Conclusion

It is the first duty of government to keep its citizens safe, particularly the vulnerable, which includes children. This duty extends to the digital environment. 5Rights Foundation welcomes the Government's stated commitment to a robust, effective and enforceable Internet Safety Strategy. It must also be comprehensive and ensure (as in every other sector) that the safety of customers and users is primarily the responsibility of service providers, not the individual.

The seven pillars upon which a safety strategy should be built: **parity of protection**, **design standards**, **accountability**, **enforcement**, **leadership**, **education** and **evidence-based interventions** offer a systemic approach in which multiple policy actions could be achieved, some swiftly, some over time, but in every case work toward the overarching need to retrofit societal values about children and childhood into the digital environment.

The notion that the technology sector is nascent and therefore requires special dispensation does not reflect the sector's ubiquity, breadth and power. Equally, the argument that robust standards jeopardise free speech or threaten their economic health must be unpicked to distinguish between principled positions, cynically deployed advocacy strategies and flaws in the business model. A business model that cannot guarantee the safety and security of its consumers is not fit for purpose.

Almost every aspect of a child's life is, or will be, mediated by digital technology and now sits alongside family, peers and schools as the fourth agency of influence on children's mental health and wellbeing. Setting and enforcing standards to militate risk and harm in the digital environment is an urgent task that requires government to take a nuanced and sophisticated approach.

5Rights Foundation does not underestimate the challenge of retrofitting the digital environment to be fit for children and childhood, but this cannot be an excuse for inertia or a partial response. It is for government to set standards and to ensure that there is a fully resourced regulator mandated to enforce them. It is for the tech sector and all those who offer digital services to meet these standards with creativity, alacrity and the recognition that children's rights are non-negotiable, even when inconvenient.

Above all else, it is for all stakeholders, government, tech, business and civil society to create a digital world in which children, the leaders, teachers, parents and workers of the future, can flourish. Because when we uphold the privileges, protections and inalienable rights of childhood we are investing in a positive future for society as a whole.

This report represents the views of the 5Rights Foundation. We are grateful to the many organisations and individuals that generously support us with their resources and expertise. Without them, our Trustees that guide us and the Young Scot Youth Leaders whose thoughtful contributions inform all our thinking, we could not do the projects that we undertake.

For further information visit www.5rightsfoundation.com
To contact us, email info@5rightsfoundation.com

5Rights

5rightsfoundation.com

info@5rightsfoundation.com

0207 502 3818