FREEDOM SECURITY PRIVACY

The Future of Childhood in the Digital World

FREEDOM SECURITY PRIVACY
The Future of Childhood in the Digital World

Published and distributed by 5Rights Foundation

Designed by David Weller and Daniel McGhee

Printed by Park Communications Ltd.

Original cover photograph by Anchalee Yates

5Rights Foundation
Charity number: 1178581
Company number: 11271356

www.5rightsfoundation.com

5RIGHTS
FOUNDATION

FREEDOM SECURITY PRIVACY

The Future of Childhood in the Digital World

ON PRIVACY

ON THE FUTURE OF CHILDHOOD

Introduction

The discourse about children and the digital world is plagued by false binaries. They must pay for responsible corporate behaviour with their freedom, for access with their privacy, for personal security with 24/7 surveillance, and for services with their attention. These binaries protect the business interests of the data-driven companies of Silicon Valley, but they do not adequately meet the needs of children and young people.

The digital world was not anticipated as a place in which childhood in all its complexity would be played out. Yet for a 21st-century child, it mediates every part of their experience: from the most public to the most intimate. Far from providing children and young people with a welcoming and respectful environment, their digital world is high on adult content, low on protections and, in many instances, hides behind the pretence that children are not there at all.

The idea for this volume was born over lunch with someone from Facebook, who suddenly turned to me and said, "you really are the woman who wants to turn off the lights at Christmas." I was horrified: was the cumulative result of everything that I was fighting for going to extinguish the joy of the one billion children and young people online?

Of course, the digital holds within it the promise of unimaginable benefits. Who in their right mind would want to turn the lights off on that? Not me. But what of those one billion kids? Do the protections and privileges of childhood need to be formally integrated into the digital world? Should we demand greater responsibility and transparency from those building the technology itself? Are we all going to *have* to give up some freedom to give children and young people more protection? Does one person's freedom of expression trump the silencing of another person or group of people? Has the idea of freedom itself been undermined by practices of data extraction and digital nudging? What constitutes an appropriate balance of freedom, security (both individual and national) and privacy for a 21st-century child?

The authors of the essays that make up this volume start to answer some of these questions from multiple perspectives. They are loosely divided into four chapters: Freedom, Security, Privacy and the Future of Childhood; although many could have been in more than one chapter. Between them, they offer a much more sophisticated conversation than the public conversation we are currently having. The authors, all experts in their fields and writing in personal capacities, focus on issues of their choosing and, whatever their differences, they overwhelmingly deliver the message that we have failed to properly design a digital world for children.

Lawyers **Susie Alegre** and **Baroness Helena Kennedy QC**, and Executive Director of UNICEF, **Henrietta H Fore,** argue that children have existing rights and that the digital is a part of, not separate from, all other environments. Susie defends a "child's right to dream" and that freedom of thought represents their "budding inner life." Children and young people's inability to realise rights that allow them control over their reputation and personal information concerns New Zealand's Privacy Commissioner, **John Edwards**.

In her uplifting essay, Taiwan's Digital Minister **Audrey Tang** (herself one of the world's youngest government ministers) chronicles the contribution of empowered young people to the democratic agenda, demonstrating what access can mean; whilst **Farida Shaheed**, former UN Special Rapporteur in the field of cultural rights, highlights cultural and language barriers which prevent millions of children and young people from truly participating in the digital space. In her compelling essay, she points out that two-thirds of the world's population live in Asia, but that only one-quarter of internet communication is in Asian languages: "take out Mandarin and that drops to a shocking 7%." Meanwhile **Dr Towela Nyirenda-Jere**, one of Malawi's first female engineers, outlines the specific experiences and hopes of children and young people already online in Africa.

Dr Ing Konstantinos Karachalios, Managing Director of the IEEE Standards Association, takes us back in time to show us the long tail of what is being undermined or challenged (take your pick) by the new world order. Unsurprisingly for an engineer, he has a schema to put things right. Meanwhile, **Kade Crockford**, Director of the Technology for Liberty Program at the American Civil Liberties Union of Massachusetts, considers history, knowledge, power and authority, cautioning that we have allowed technology into the lives of young people without first asking some fundamental questions. "What does Alexa say when a child asks why Daddy hurts Mommy?", Kade demands to know. Director of Digital Civility at Roblox, **Laura Higgins,** takes a different tack, remarking on the media's 'sensationalist' portrayal of the online space, which she fears demonises the digital and diminishes the ability of children to play freely.

In his very moving essay, **Uri Sadeh**, who works on the frontline of child online protection at Interpol (like all our authors, writing in a personal capacity), outlines the tragic way in which children have become collateral damage as governments and businesses fail to put their safety above all other considerations. Similarly defiant are **Dr Ian Levy** and **Jānis Sārts**, of the UK National Cyber Security Centre and NATO respectively. Jānis argues that "not everything should be allowed" and Ian calls for "safe software" that embodies (and prevents) both hazards and harms, as is standard practice in any other area of life. **Professor Hany Farid**, the co-developer of photoDNA, and **John Carr OBE**, one of the world's leading authorities on children's protection online, express deep frustration that both industry and civil governments' inaction is and was "never one of technological limitation", but merely one of corporate and political will.

H.E. Dr Amani Abou-Zeid, the Commissioner for Infrastructure and Energy at the African Union, cites issues specific to Africa (although familiar to all territories) when she says that we must strengthen online security, so that children and young people can access the digital environment safely. Equally significant, **Adrian Lovett**, President and CEO of the World Wide Web Foundation (the organisation that houses the hopes and dreams of Sir Tim Berners-Lee, inventor of the World Wide Web), feels that the utopian vision of the internet has not yet been realised. He points to the Web Foundation's Contract for the Web and sets out nine principles for a child-friendly internet.

Four young people have their say: three from **RX Radio** in South Africa feel that parents are undereducated and young people vastly under protected, while **Francesca Fajardo**, who took part in 5Rights' Data Literacy workshops, writes an excoriating essay which should be compulsory reading for all policymakers and tech titans. She explores how current data practices stigmatise users who may be disabled, LGBTQ+, BAME… Her list is long, and she concludes that "poor ethics are trumping decency".

In the balance of freedom, security and privacy, many authors stand squarely behind a child's need for privacy. Academics **Professor Sonia Livingstone OBE** and **Professor Dr Eva Lievens** make eloquent arguments that seek to "deresponsibilitise" children and parents, placing the burden of privacy directly onto commercial companies who develop products and services. Playwright **James Graham OBE**, author of the brilliant play *Privacy*, argues that the psychological and emotional effects of living in a digital environment are rarely discussed, but significantly affect the way that children and young people develop. Each of these essays put forward the idea that freedom for a child cannot exist unless and until the digital world can be accessed without complex and conflicting pressures and surveillance.

Many made practical suggestions for a better future, including 5Rights' Policy Lead **Jay Harman,** who argues passionately that we must recalibrate our idea of the digital to put children at the centre of its design and development. **Amandeep Singh Gill,** former Executive Director of the UN Secretary General's High-Level Panel on Digital Cooperation, **Elettra Ronchi, Andras Molnar** and **Lisa Robinson** from the OECD's Division for Digital Economy Policy, and **Amy Shepherd**, writing on behalf of Open Rights Group, an organisation focusing on freedom of expression and speech online, all considered routes that would allow under 18s to participate in a digital world that respects and upholds their privacy, security and freedom - including their freedom to be a child.

The strength of this volume is less that the authors came to a consensus about everything, than that they came to a consensus about one thing. This generation of children are a "forgotten mass" upon whom we have allowed a social experiment at an unimaginable scale. An experiment in which we have failed to remember that childhood is the time in which everything you do, see, feel and imagine contributes to your makeup as an adult. It is a volume which offers a debate on issues that are foundational to the future of children and young people across the globe, and therefore future itself.

This book of essays would not have been possible without the generosity of its authors, who busy already, gave much time and thought to their essays. The work of 5Rights Foundation is made possible by the dedication of a small group of brilliant colleagues and a handful of enlightened funders - thank you. For this volume, we are particularly indebted to **Poppy Wood** and **Jessica Smith**, and as ever, to the **hundreds of children and young people** who inform what we do.

For myself, I am reassured. To demand a better deal for children and young people is not a killjoy putting out the lights at Christmas. It is switching on the lights, so that the forgotten mass can see where they are going.

Beeban Kidron

Baroness Beeban Kidron OBE

ON FREEDOM

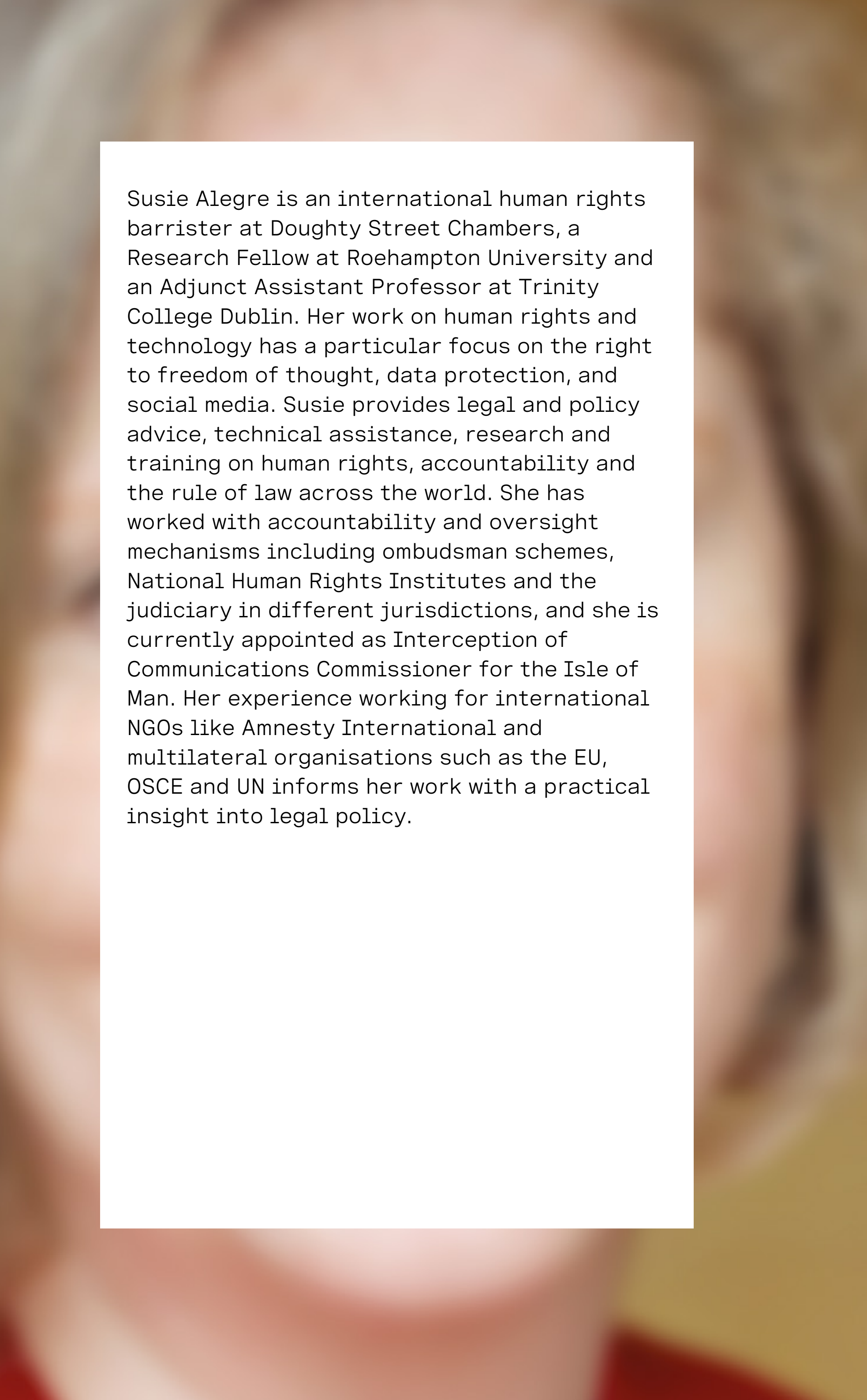
All I want to do is disconnect from my phone for a long period of time, perhaps weeks, but there are always pressures preventing me. I love the way the internet allows for lots of new opportunities, yet it prevents me from doing a lot of things. I love reading, but by the time I've spent an hour too long on my phone, I can no longer read my book. It makes me angry that businesses use specific designs to keep young people on their app/website.

Unless we understand the technologies that we use daily, we can’t control how they make us behave.

People are saying kids are spending too much time (online) but they’re causing it - the companies.

Are we even individuals rather than just algorithms?

5Rights’ Young Leaders



Susie Alegre is an international human rights barrister at Doughty Street Chambers, a Research Fellow at Roehampton University and an Adjunct Assistant Professor at Trinity College Dublin. Her work on human rights and technology has a particular focus on the right to freedom of thought, data protection, and social media. Susie provides legal and policy advice, technical assistance, research and training on human rights, accountability and the rule of law across the world. She has worked with accountability and oversight mechanisms including ombudsman schemes, National Human Rights Institutes and the judiciary in different jurisdictions, and she is currently appointed as Interception of Communications Commissioner for the Isle of Man. Her experience working for international NGOs like Amnesty International and multilateral organisations such as the EU, OSCE and UN informs her work with a practical insight into legal policy.

Susie Alegre

Data Daemons: Protecting the Child’s Right to Dream

In the world of Philip Pullman’s “His Dark Materials”, a child’s daemon changes forms as quickly as their mood. It is only with adulthood that the daemon, the animal incarnation of the soul, settles into a permanent form. The changing daemons of childhood represent the malleability of the child’s mind and the resonance of Pullman’s imagery lies in the fact that we all recognise, from our own childhood experience and observation of the children around us, the magical openness, fickleness and receptivity of children’s minds. Those qualities in a child imply both enormous potential and acute vulnerability: it is the reason we value education and nurturing for developing minds. Why then are we so ready to outsource the moulding of our children’s minds to digital tools of distraction?

The right to freedom of thought is protected alongside the rights to freedom of conscience, religion and belief in international human rights law including Article 18 of the Universal Declaration of Human Rights 1948[1] and Article 14 of the UN Convention on the Rights of the Child 1989.[2] It provides protection for the manifestation of our thoughts and beliefs but crucially it creates a powerful protective fence around the inner space of our mind, known as the “forum internum,” with three key strands:

- The right to keep our thoughts private,
- The right to keep our thoughts free from manipulation, and
- The right not to be penalised for our thoughts.

Freedom of thought is broad in scope. It covers all kinds of thoughts and ideas whether they are profound, fleeting or wrong, as well as emotions and desires. It encompasses the full spectrum of a child's budding inner life.

Most human rights, like the right to private life, the right to freedom of expression and the freedom to manifest religion or belief, can be limited for a range of reasons including national security, public health and morals, and the protection of the rights of others. But the right to freedom of thought in the "forum internum" is absolute. This means that anything that steps across the boundary to interfere with that inner mental space is prohibited in international law and can never be justified.

The right to freedom of thought does not mean that children's minds should be free from influence. We are all affected by our surroundings: the things we read, the people we talk to, the world we see around us. And children need guidance to navigate the world around them and are hungry for information and experiences to develop their full potential and keen to reach out and connect with the society around them. But as our children's minds and emotions are increasingly exposed to and affected by technology, there is an urgent need to define where the boundaries to protect their right to think for themselves lie in the digital field.

Many children in developed countries are learning to navigate the world through Siri in their pocket or Alexa in their bedroom. Voice activated search tools give children access to the online world before they are even able to write. And they also give tech companies access to children's minds and thought processes on an unprecedented level. The anthropomorphic nature of these devices can lull children into a false sense of friendship and security in which they may share insights into their inner lives that they would never share with friends or parents. But it is not only a question of what children say. Their activity on social media and subtle aspects of the way they express themselves reveals much more about their moods and thoughts than they realise. And while they or their parents may have clicked a consent button, there can be no real informed consent to the consequences of this.

In 2017, it was reported[3] that Facebook was selling psychological insights on young people, including 1.9 million high-schoolers in Australia. Leaked documents reportedly showed that the company could monitor and interpret posts and photos that showed when children felt stressed, anxious or stupid in real time and share that information, so that private companies could cash in on the changing moods of young users with targeted advertising. These psychological insights go beyond issues of privacy or freedom of expression: what is being sold is a complex algorithmic interpretation of the child's inner state. The collection and sale of this type of data may well interfere with the absolute right of the child to keep their thoughts private.

Without strict limitations on the ways their data is accessed, analysed and used for targeting and profiling, the data trail that children leave today may be used to create detailed avatars of their inner thoughts which could be used against them now and in the future. These "data daemons" may settle in forms that define their future access to credit, employment or justice, regardless of the way the child's mind develops and changes over time. Children in particular should not be exposed to the risk that their turbulent inner lives will be used to curtail their chances in adulthood.

But the impact of technology on children's minds is not only about data. In 2019, the Children's Commissioner for England published the report "Gaming the system"[4] which found that 93% of children in the UK play video games. Aside from the potential risks for child safety online, the report raised concerns about the impact of gaming on children's development and socialisation and the links between gaming and gambling with the concurrent risk of addiction.

The psychological buttons used to make online gaming attractive are also used in many forms of educational technology, designed to get kids hooked on learning. While the goals and content of those games may be appropriate for children, we need to consider the wider impact that the methods used in this type of gaming have on children's minds. In 2019, the UK's National Health Service established its first clinic dedicated to treating gaming and internet addiction:[5] a problem recognised by the World Health Organisation as a growing global health issue.[6] But the right to freedom of thought puts an obligation on states to protect children from practices that interfere with and manipulate their inner worlds. This kind of deep psychological harm needs prevention rather than cure.

Childhood is a time for dreaming when minds are open, idealistic, flexible and imaginative. Children are using technology as a tool for mobilisation to save the world from climate change and give hope for our future. They need a safe digital space where they can use their minds to realise their potential and fully exercise all their human rights. But they don't yet have it.

In Pullman's world, it is taboo to touch another person's daemon: to do so causes them immeasurable suffering. But in our world, children are increasingly engaging with technology that can monitor and touch their minds both in the present and in the future. We are only beginning to understand the impact this could have on our children and their societies. There is no time to wait and see. States and international organisations need to act now to fulfil their ethical and legal obligations to protect children's fundamental right to freedom of thought. All of our rights depend on it.

[1] Article 18, Universal Declaration of Human Rights, 10 December 1948

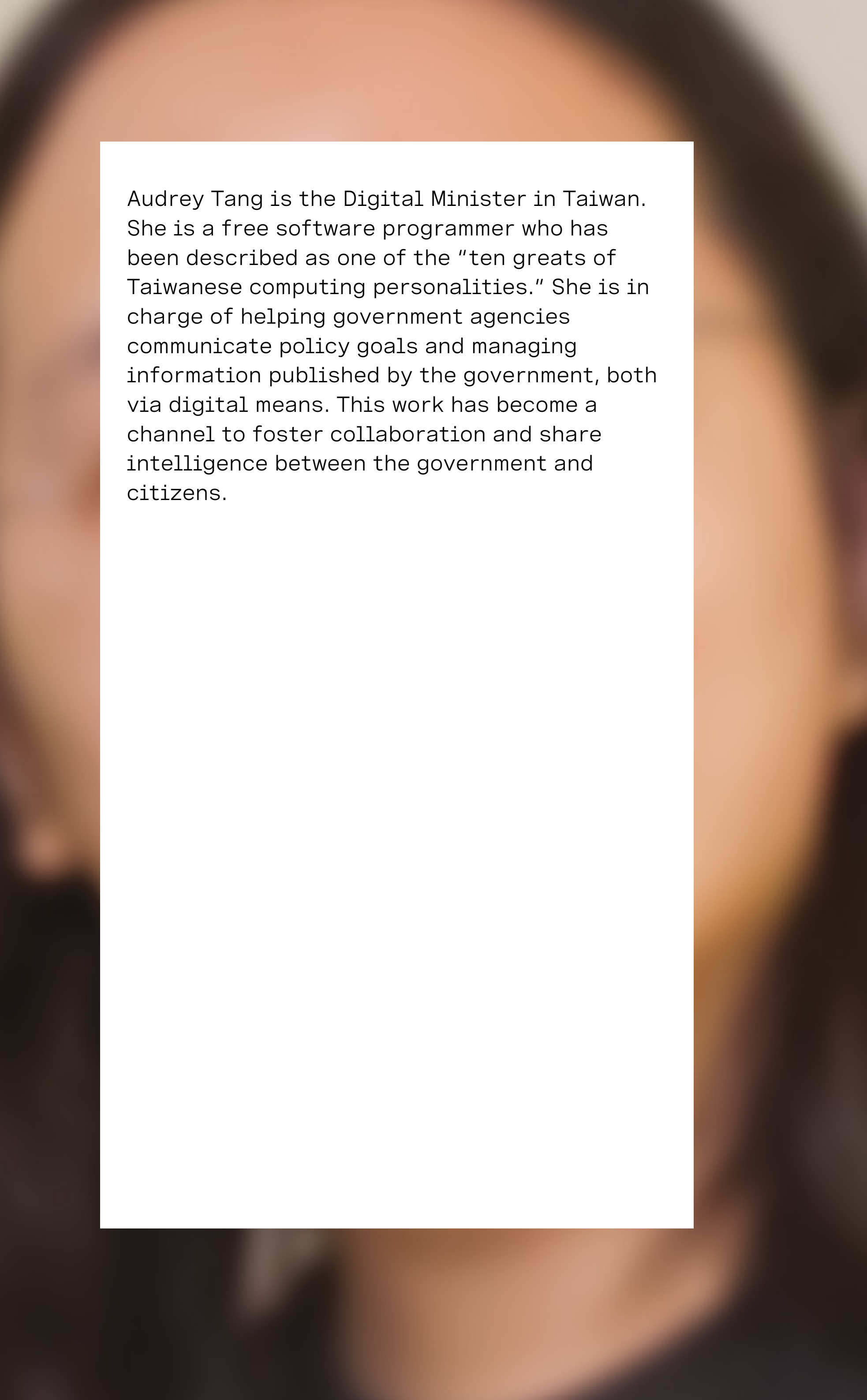
[2] Article 14, UN Convention on the Rights of the Child, 20 November 1989

[3] Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless', The Guardian, 1 May 2017

[4] Gaming the system, Children's Commissioner for England, October 2019

[5] Children treated for computer gaming addiction under NHS Long Term Plan, NHS News, 8 October 2019

[6] Gaming disorder, World Health Organization, September 2018



Audrey Tang is the Digital Minister in Taiwan. She is a free software programmer who has been described as one of the “ten greats of Taiwanese computing personalities.” She is in charge of helping government agencies communicate policy goals and managing information published by the government, both via digital means. This work has become a channel to foster collaboration and share intelligence between the government and citizens.

Audrey Tang

A Young Democracy is a Strong Democracy: Civil Rights of Taiwan's Children

In 2017, when 16-year-old Wang Hsuan-ju found out about the civic participation platform "Join" run by the National Development Council during civics class in high school, she proposed the "nationwide progressive ban on the use of disposable utensils." Concerned about environmental issues, Wang Hsuan-ju estimated that more than eight million tons of garbage flows into the ocean every year. Most disposable plastic utensils cannot decompose and further endanger the survival of marine life.

Wang Hsuan-ju's proposal quickly garnered the support of 5,253 signatories. With this support, government departments, environmental groups, and disposable utensil companies held meetings and discussed solutions, and eventually reached a consensus to accelerate a plastic restriction policy. Due to Wang Hsuan-ju's proposal, the Environmental Protection Administration has restricted government departments, schools, and department stores from providing disposable plastic straws, beginning July 1st, 2019.

Wang Hsuan-ju's story reflects the trend of the current generation of Taiwanese youth participating in public affairs through the internet.

The development of the internet in Taiwan has advanced alongside Taiwan's process of democratization. In 1996, the Republic of China (ROC) government held its first direct presidential election. That year also saw the global rise of the internet. Taiwan's geography, being an island only 394 kilometers long and requiring only an hour and a half to travel its length by high-speed rail, gave the island a major advantage in achieving universal internet access.

Currently, "broadband human rights" have become a core policy of the government. 87% of people over the age of 12 currently have internet access, and for teenagers between the ages of 15 and 19, access is even higher, at 94%. Having been born into a democratic society and the world of the internet, it is only natural that Taiwanese teenagers express and act upon their opinions online.

Many junior and senior high school students joined virtual hands in solidarity through the internet during the March 18th movement in 2014, to protest the Ministry of Education's adjustments to the new curriculum through "black box procedures" in 2015. Close to 300 senior high schools throughout Taiwan used student-led Facebook pages to establish inter-school alliances, triggering a large-scale student movement and the occupation of the square in front of the Ministry of Education, finally prompting all legislative parties to request that the Ministry of Education review the curriculum.

After that experience, the government developed online platforms for citizens to participate in policy discussions together with the civic tech community 'g0v', with the purpose of establishing a channel for direct communication from and between citizens. The Join platform, directly maintained by the government, is one such channel by which citizens can discuss most policy issues. Since its launch in 2015, the Join platform has garnered 10.6 million visitors – almost half of Taiwan's population.

On the Join platform, teenagers comprise the most active contributors in pushing for change. In addition to Wang Hsuan-ju's successful proposal to restrict the use of plastic straws, 17-year-old high school student Jackroy Liu proposed that "human rights issues should not be subject to referendums" on the platform in December last year, receiving swift public response and prompting various ministries and relevant initiative groups to cooperate and discuss the issue. The final draft amendment to the Referendum Act proposed by the cabinet included provisions that human rights issues should not be subject to referendums.

It is not only popularization of the internet spurring youths' participation, but also the implementation of the United Nations Convention on the Rights of the Child (UNCRC) in Taiwan. In June 2014, Taiwan promulgated the 'Implementation Act of the Convention on the Rights of the Child', which was implemented on International Children's Rights Day on November 20th of the same year. Since then, the UNCRC has become an important basis upon which the government promotes children- and youth-related policies.

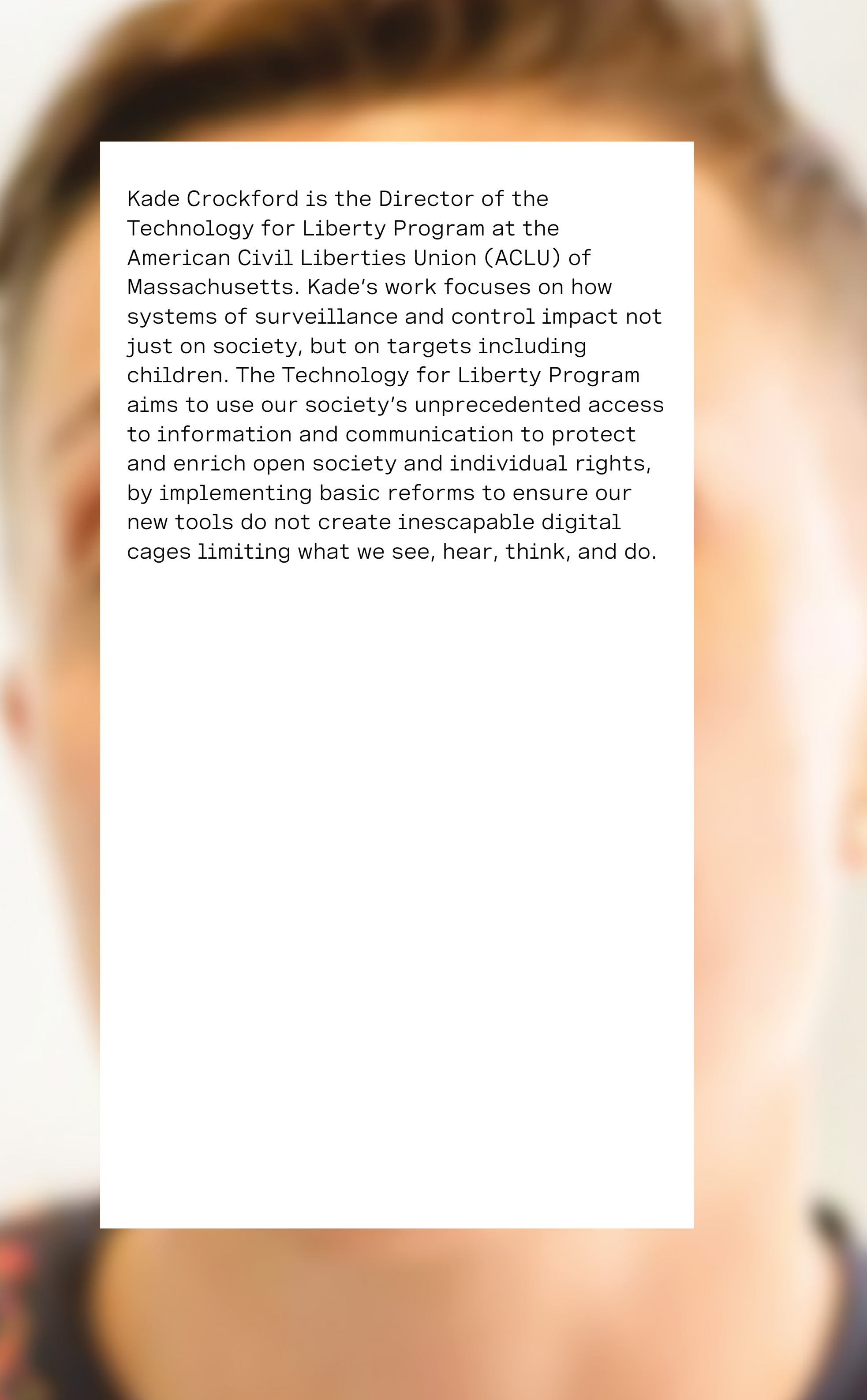
In the cabinet-level Youth Advisory Council meeting held in March 2018, a youth councillor requested that schools below the high school level establish independent feedback reflection units, providing students with safe and effective channels for giving feedback and appealing for assistance. The Ministry of Education has begun planning for establishment of a student appeal platform. In May 2019, the legislature passed the sixth draft amendment of the 'Implementation Act of the Convention on the Rights of the Child', stipulating that the Child and Youth Welfare and Rights Promotion Group established by the cabinet should include child and youth representatives under the age of 18, allowing children's rights of social participation in Taiwan to make another big leap forward.

In Taiwanese society, educational issues that are deeply influenced by young people receive a lot of attention. According to the Taiwanese media's '2019 Social Innovation Survey', the Taiwanese people and the social sector emphasize "quality education" as a sustainable development goal. Currently, 36% of social innovation organizations in Taiwan have made the 4th sustainable development goal of "quality education" their mission, becoming the most popular goal of all social innovation organizations in Taiwan.

In the face of societal expectations, this year Taiwan officially implemented a 12-year curriculum guided by "competencies." In the past, students were assigned to specific academic subjects or departments, but the new curriculum for

6- to 18-year-olds emphasizes the cultivation of learners capable of "taking the initiative, engaging the public, seeking the common good." This allows students to know what they wish to learn, while schools and teachers assist from the sidelines, so that the students eventually become "lifelong learners." Children can design their own learning paths, become their own teachers, and discover their own passions and ambitions.

In Taiwan, online participation has become an important channel for the empowerment of children, and the government has established a foundation for the freedom of expression of children and youths through policy and education reforms. Through modern means of empowering young citizens to speak for themselves, Taiwan is revitalizing its democracy with greater civil rights for children in the digital world.



Kade Crockford is the Director of the Technology for Liberty Program at the American Civil Liberties Union (ACLU) of Massachusetts. Kade's work focuses on how systems of surveillance and control impact not just on society, but on targets including children. The Technology for Liberty Program aims to use our society's unprecedented access to information and communication to protect and enrich open society and individual rights, by implementing basic reforms to ensure our new tools do not create inescapable digital cages limiting what we see, hear, think, and do.

Kade Crockford

A New Digital Divide? Protecting Lower-Income People from Hyper-Digitalisation

Human beings have long classified and categorized one another. It's one of the ways we make sense of the world around us (that person is tall, that person is skinny). Classification and categorization are economically, socially, and politically determined, and they in turn shape our economics, society, and politics. Decisions about which kinds of classifiers and categories matter – and who decides – are enormously influential; they shape not only our understanding of other people but also of ourselves (he is white, she is black; they are dangerous, we are safe).

It's always been difficult to understand oneself in relation to the world, and in relation to oneself. For centuries, human beings have turned to philosophy and religion to help them get closer to understanding. In the 21st century, this project is significantly more challenging, for reasons that are not immediately obvious. Among the central difficulties is that children today grow up in a world where both the boundaries of categories and classifiers and the people who determine those boundaries are increasingly hidden from view, behind algorithmic black boxes. At the same time, the decisions computerized systems make about how to categorize and classify us are too often viewed as neutral. What is data-driven, the mythology goes, is objective. The opacity shrouding algorithmic decision making combined with its (false) cultural imprimatur of neutrality together pose an unprecedented threat to self-determined human subjectivity. Worse still, as these crucial decisions about classification and categorization are hidden and obfuscated by increasingly complex technology like neural networks, it becomes more and more difficult, and in some cases impossible, to democratize the ability to understand oneself and one's world.

I first became aware that classification systems don't always fit the diverse tapestry of human experience when my elementary school teacher said, "Girls line up on the left, boys on the right." I froze, suddenly acutely aware that my gender identity exists somewhere outside the categories provided. It was simple enough for me, then, to ask my teacher why she asked us to divide ourselves up into these categories. Even if her answer didn't satisfy, it was straightforward enough for me to ask the question. I knew what question to ask. I knew whom to ask. I could ask it.

It is not simple, now, for children to ask unaccountable corporations why unnamed engineers, product designers, or executives have categorized or classified them as high risk, likely to succeed, or in need of extra tutoring. In many if not most cases it is impossible. It is not even likely that children will understand that a decision to classify or categorize them has been made by these unaccountable actors. The child may only see an output that ranks them on a supposedly neutral scale, or may not see the ranking at all but will nonetheless experience a restricted set of options as a result of their score, whether they realize it or not. The consequence of this opacity is a loss of control over one's life and, crucially, leaves behind gaping holes where prior generations of children had opportunities to learn how the adult world works, including what society values, how power works, what categories are privileged over others, and many other inquiries that are central to growing up.

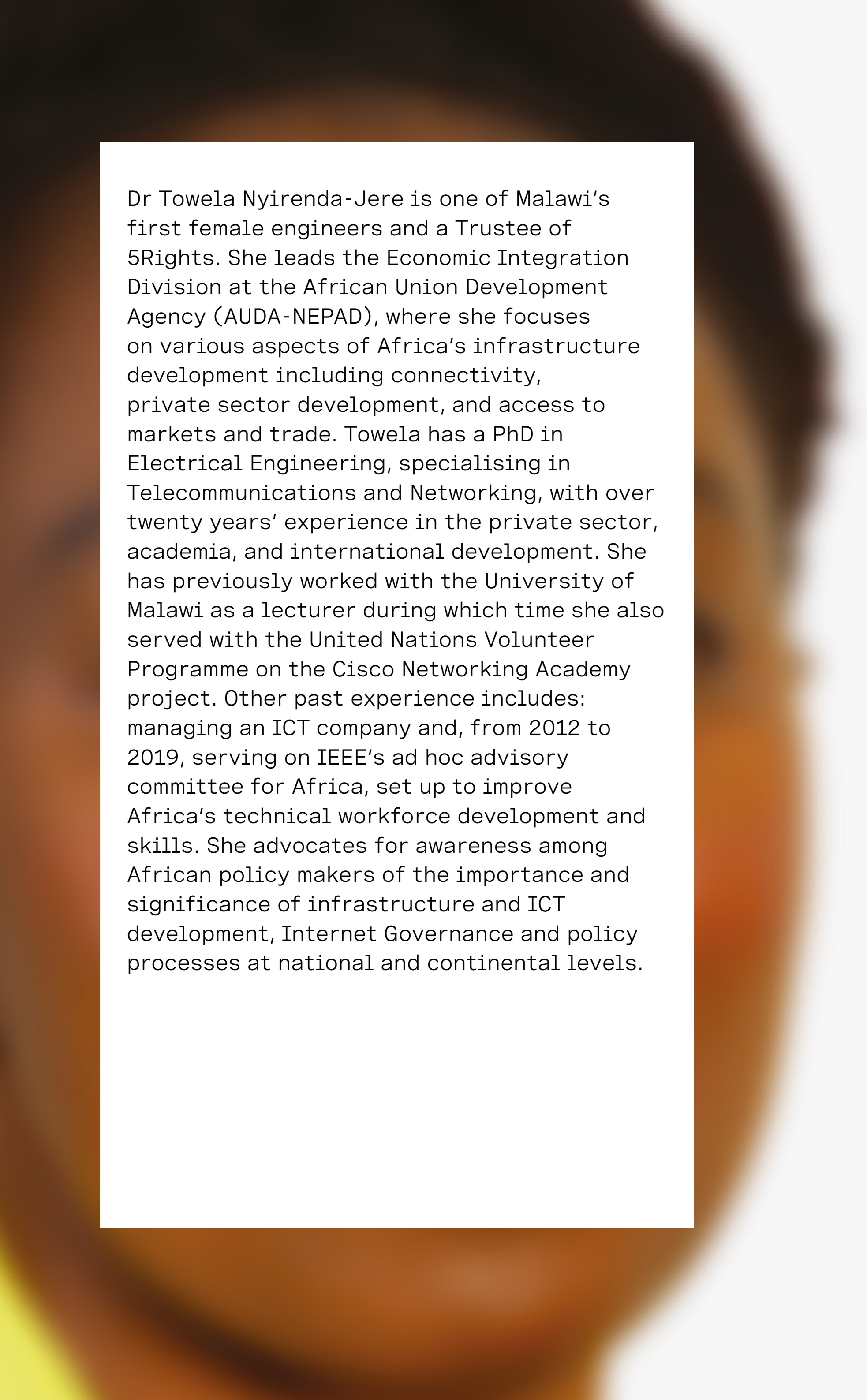
It is likewise unrealistic to imagine that children are capable of interrogating what Alexa or Google Home tells them about their world, or what happens to the words the children speak into these devices when they drift up into the deceivingly-named "cloud." Children, we know, ask big questions. And we know children's brains are like sponges, constantly soaking up everything they see and hear. Recently my five-year-old nephew asked me, "Why is the world unstable?" He probably heard something about global instability on the radio and wanted to know what all the fuss was about. I explained, to the best of my ability, the concept of political instability, and why societies become unstable. I stressed that instability often results from inequity, because people don't like to be treated unfairly. What would Amazon's Alexa product tell a child who asks this question? How about a child who asks about heaven and hell? What does Alexa say when a child asks why daddy hurts mommy?

Scholars have for some time now grappled with questions related to children's privacy rights attendant to the rapid and alarming spread of so-called "smart" devices into the homes of millions of people across the planet. Other scholars are thinking and writing about how students are increasingly being monitored and nudged by "education technology" like Class Dojo and Google's apps for education suite. Others, including those who got very wealthy in Silicon Valley thanks to their involvement in building or selling addictive technologies, have spent the past few years loudly warning parents that children are becoming addicted to their smartphones and devices (like their parents), and fretting about the cost to social and intellectual development.

All of these are important subjects for research and public debate. Unfortunately, the question of how these technological systems of control reduce human agency while obscuring how power operates from the people it operates upon has not been as thoroughly studied or publicly debated.

Ultimately, we don't need research to tell us that in most parts of the world, including my home country the United States, the financial interests of powerful corporations and the direct advertising market currently take legal precedence over the privacy and self-determination interests of adults and children alike. Technology companies have managed to convince many people that exchanging our personal data for the use of their services is not only a good bargain, but the only plausible business model for the digital 21st century. They are wrong.

It’s no surprise that the world’s richest and most powerful technology scions are consciously shielding their children from digital technologies during their formative years. For years, researchers have spoken of a “digital divide” separating the urban and suburban wealthy who have computers and fast internet access, from the rural poor, who don’t. But technology has changed our world quickly, and in many parts of the industrialized world the digital divide is no longer a simple question of who is “connected” and who isn’t. When we conceptualize the digital divide in the 21st century we must also interrogate who has the luxury of avoiding technological systems during their childhood, and who has no choice but to use – and therefore to be controlled by – them. Fighting for equal access to the internet is important. But a dedication to understanding and pushing back against the way power works to construct human beings and knowledge in the digital age must also be our focus as we do the hard work of recalibrating our law and social infrastructure to best advance democracy, human self-determination, and liberty for children in the 21st century.



Dr Towela Nyirenda-Jere is one of Malawi's first female engineers and a Trustee of 5Rights. She leads the Economic Integration Division at the African Union Development Agency (AUDA-NEPAD), where she focuses on various aspects of Africa's infrastructure development including connectivity, private sector development, and access to markets and trade. Towela has a PhD in Electrical Engineering, specialising in Telecommunications and Networking, with over twenty years' experience in the private sector, academia, and international development. She has previously worked with the University of Malawi as a lecturer during which time she also served with the United Nations Volunteer Programme on the Cisco Networking Academy project. Other past experience includes: managing an ICT company and, from 2012 to 2019, serving on IEEE's ad hoc advisory committee for Africa, set up to improve Africa's technical workforce development and skills. She advocates for awareness among African policy makers of the importance and significance of infrastructure and ICT development, Internet Governance and policy processes at national and continental levels.

Dr Towela Nyirenda-Jere

A Child is a Child is a Child: Conversations in Africa About Children in the Digital World

In 2008, after having worked in academia and in the private sector for a number of years, I took a break, and had a year off. In that year, I did leadership facilitation and leadership training, and one of the most important things I learned was that you can't stand on the side-lines wishing for change: you must step up and be involved.

I had reason to reflect and remember this time in my life a few years back when I had another wake-up call: I had been working in the digital space, working on internet governance, on public policy, on people's rights online, but I never thought about the rights of children online. It made me realise how much we miss out on by not focusing on children and young people. I think it also resonated with me as, in Africa, the conversation over the last five years or so has been about the demographics of Africa and how that is changing: 65% of the population are under the age of 20.

**

Culturally, we are different from Europe, America, Asia. In our culture, a child is a child is a child. Children have rights, but they are to the extent that parents are willing to give, or accommodate, those rights. While they can express themselves freely, it is only to the extent that the parents allow them to do so freely. When you talk about digital spaces, it causes a bit of a problem: how do we balance the cultural context, when in the digital space, there is not that cultural context? Parents don't have the same kind of control as in the offline world. That becomes a bit of a challenge, because you then have children caught between two worlds: caught between what culture says, but having to engage in the digital space where the safe container of culture doesn't exist. How does one navigate and balance this?

Because Africa is in the 'catch up' and 'leap frogging' phase of ICT development, there is a big push for giving people access to the Internet and digital opportunities, whether that is young people or not. This means not only access, but affordable access. There is a lot of emphasis on affordable access.

There is also a lot of emphasis on content and localised content, and being able to give content that is meaningful to young people, and that is produced locally. For us, the colonial legacy has made it so that in a lot of countries, the language that is used for business is the language that comes from the colonial legacy: you have anglophone, francophone, lusophone, and so on. However, within all that, we have our own indigenous languages as well. You find that schooling and business are done in English or French, but socially, we communicate and converse in our own languages.

When I'm online, I would like to see content that is in my own language, and content that is culturally relevant to me. If young people are not enabled as content creators, and not enabled to value content in local languages, it means that we will always have bias towards content that is not in our own languages.

What we hear from children is that they want access, and affordable access, yes. But it's also the freedoms: and in different countries, those freedoms exist in varying degrees. More and more in Africa, rights are very politicised and become a very political issue. We all remember the Arab Spring, and since then, all these other instances of young people agitating for political change. That can be challenging, because governments don't really know what to do with this. When you talk about young people having rights, if it's not expressed properly, it becomes a political issue rather than a social issue.

It is also, we see, that young people are looking for entrepreneurial or entrepreneurship opportunities online. But at the same time, they are perhaps lacking in how to protect their ideas: how do they deal with issues of intellectual property? How do they make sure that when they do have an idea, that they can develop that idea and take to market, without it being hijacked by other forces? Those are some things that are important. In some other instances, it's about safe spaces: how do you create safe spaces for young people online, not only for communication, education or social interaction, but also for access to economic opportunities?

We have a very youthful population: we encourage kids to get online and we are encouraging everyone to move towards the fourth industrial revolution. But we are not talking about how to protect children when they are in these digital spaces: how to safeguard them and make sure they can interact safely. In some instances, these so-called digital natives don't understand how vulnerable they are online. You constantly have to tell them to be careful because in online spaces you don't know who is on the other side, you don't know when they ask you for information, *why* they are asking for information, what they are going to do with it, and what that then means for you.

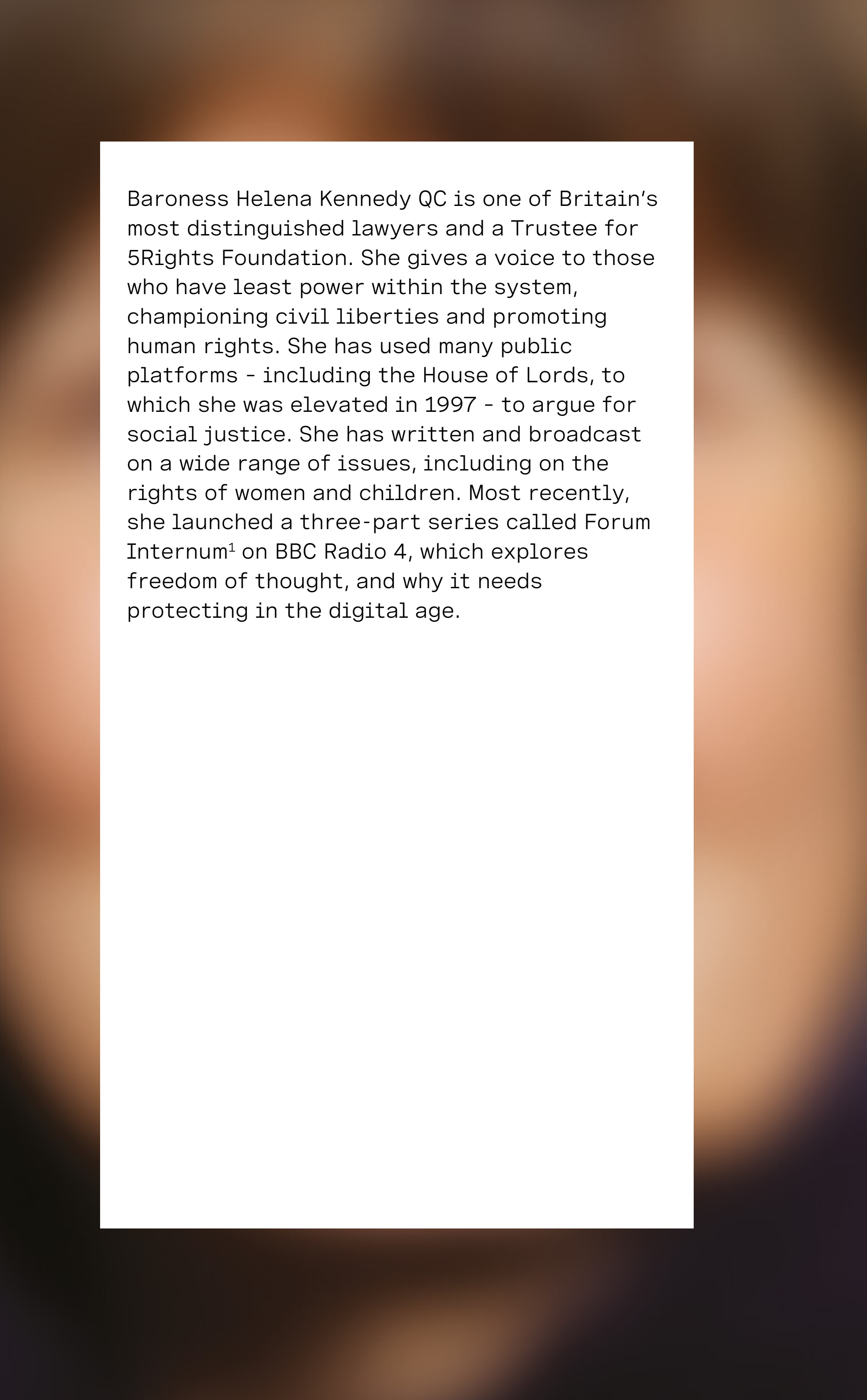
Nowadays, we find a lot of African countries talking about the digital economy and about the fourth industrial revolution. They talk about the need to skill and upskill, which I think is good. What then needs to accompany that conversation is an understanding of the other side which is, when people get online, what does that then mean? How can we ensure that they can engage online safely?

Issues of data protection and issues of online protection are maybe not discussed to the degree that you would see in other places. We are still so focused on the access side of things that we have not grappled so much with the other side of data protection and privacy, and child online protections. But also, what we are seeing as more people come online, and more people are transacting and interacting and engaging online, is that we are seeing more spam, hacking, and identity theft. The need to address data protection and privacy and online protection then becomes more of an issue as a result of these things. But in terms of policymaking, it’s more of a reactive process than proactive: technology tends to advance too rapidly for policy to keep up.

How can we then make sure that when we talk about trade and the issue of trade, we realise that it is only going to be effective or efficient to the extent that we can secure the transactions? If I cannot guarantee that a transaction is safe and secure, then that will affect my ability to trade in the digital space.

One of my main wishes is that our policymakers understand this interaction between cybersecurity, privacy, data protection and trade. I would ask that they see it not that we are just asking them to secure the digital space for the sake of it, but that it does have implications on a lot of other things. Africa right now is focussed on this issue of trade, looking at inter-regional trade, as well as trade with the rest of the world. The only way we’ll be able to do that, the free movement of goods and services, is if we guarantee security of movements and transactions. In this instance, data protection becomes a very big issue. When you look at the fact that more and more, it's young people who are coming online and engaging in these transactions, their online protection and privacy becomes a big issue as well. I really would like to see that link between securing our online spaces, data protection, privacy, online protections, and how we link that to other issues, such as trade.

The context which children and young people are born into in Africa may be different from the West, but they must not be missed in international policy conversations. They too have a right to access the online space, to participate in it as content creators, and to realise economic and entrepreneurial opportunities. African leaders must secure their privacy and security, so that they can access the full benefits of participating in the digital environment. At the same time, young people need to be aware of what exercising their freedoms online entails and how they must be responsible users of the various online and digital spaces available to them.



Baroness Helena Kennedy QC is one of Britain's most distinguished lawyers and a Trustee for 5Rights Foundation. She gives a voice to those who have least power within the system, championing civil liberties and promoting human rights. She has used many public platforms - including the House of Lords, to which she was elevated in 1997 - to argue for social justice. She has written and broadcast on a wide range of issues, including on the rights of women and children. Most recently, she launched a three-part series called Forum Internum[1] on BBC Radio 4, which explores freedom of thought, and why it needs protecting in the digital age.

Baroness Helena Kennedy QC

New Freedom? How the Digital Environment Poses Complex Legal Challenges for the Promotion of Children's Rights

The year 1989 saw the introduction of the Convention on the Rights of the Child (UNCRC). Since then, it has become the most widely ratified international agreement in history. In the same year, the computer code was released that would ultimately lead to the creation of the World Wide Web.[2] In the 30 years since, access to technology has expanded rapidly, allowing all people, including children, greater access to information and to each other. This new freedom has improved life for many, but has also posed complex legal challenges for countries around the world who wish to ensure and protect the rights of children.

The right to freedom of expression and access to information
Like all people, children have the right to freedom of expression under international instruments, including the UNCRC. Article 13 of the UNCRC provides that every child must be free to express their thoughts and opinions, and to be able to seek and receive all kinds of information, as long as it respects the rights and reputations of others.[3] Furthermore, in Article 17, the Convention guarantees the right to access information. This is a right to receive reliable information from a diversity of sources with the goal of promoting the child's social, spiritual,

moral and physical wellbeing. It calls on states to develop guidelines to protect children from material that may be harmful to their wellbeing.[4]

These rights require a balancing act to take place: allowing the exercise of freedom of expression and the freedom to access information, while offering protections to children who are vulnerable by virtue of their age. Occasionally this balancing act is difficult. For example, there are certain restrictions to free expression intended to prevent children from being exposed to gratuitous violence or adult sexual imagery, yet these restrictions have also seen the inadvertent filtering out of LGBTQ+ videos on YouTube.[5] In these cases, the balance must be struck carefully and efforts must be made to mitigate unintended consequences, ensuring at all times that the best interests of the child are served.

The current business model of the sector is dependent on targeted advertising, which allows many services to be 'free.' This makes some argue that, without targeted advertising, child-focussed content may not be created, or may be limited significantly; or that, requiring users to pay would limit access to poorer communities. However, the amount of advertising present can hinder children's abilities to express themselves and access information, or crowd media spaces, making it difficult to receive information without undue influence.[6] These opposing views need to be seen in the context that children are less able to distinguish between general information and paid content.[7]

Managing the right to access information and to freedom of expression, in a way that also protects children, is at the forefront of current debates about content controls. Formal regulation around what may constitute harmful content poses an increased risk of censorship and abuse of content restriction.[8] But equally, failing to enforce current regulation in online scenarios and/or allowing online public spaces to be dominated by disinformation, misinformation or commercially driven information, fulfils neither social norms of information distribution, nor children's rights to a broad set of information, while being protected from harmful information. Equally central to the debate is whether platforms are publishers or mere conduits:[9] but increasingly this binary does not hold the answer. Platforms are often presented as neutral, but increasingly we are understanding that they are mediators of information: content that users consume online is actively recommended by the platforms themselves. The basis of automated decision-making recommendation systems that are governing what we see are increasingly coming under scrutiny. As Tristan Harris, Co-Founder of the Center for Humane Technology, points out, over 70% of the content people watch on YouTube are videos that have been recommended *to them by YouTube's algorithm*.[10] Regulators around the world are considering how to ensure greater transparency and accountability from platforms about *the information they use to make these decisions, the information they distribute, and the way that they distribute it.*

The right to privacy

Article 16 of the UNCRC provides that the law should protect a child from arbitrary or unlawful interference with their privacy, home, family life, and correspondence: this includes protecting children from unlawful attacks that harm their reputation. The right to privacy has been greatly affected by the advent of the internet, and the mediation of technology in all areas of children's lives. In the light of the developing nature of children, both mentally and physically, certain interferences with the right to privacy are justifiable, due to the limits of their cognitive and development capacity.[11] However, due to their lack of autonomy, children are also more vulnerable to having such interferences, many of which occur via technology.

One of the most significant concerns around a child's right to privacy in the digital world is the collection of data by websites and service providers. Corporations collect significant amounts of data from their digital users. Some of it is required to provide a service, but the scale of personal data and information collected is vastly out of proportion to that which is required. Commonly, children are not in a position to fully appreciate that information is being collected on them, and even in circumstances where they have the opportunity to grant permission to the collection and selling of their information, they are not likely to be fully aware of the long-term impact.[12] This data is regularly used by third party companies to profile and target advertisements to specific groups, or to direct user behaviour. Children are particularly susceptible to marketing. Increasingly, vast datasets relating to younger and younger children are used for commercial purposes, with little-to-no-regard for their privacy or best interests.

In order to ensure that corporations aren't encroaching on children's right to privacy, governments need to enact clear laws around the collection, use, and sale of children's data. An important step forward is requiring privacy policies to consider the rights of children when they are being created. The EU has taken steps under the General Data Protection Regulation (GDPR), which places the burden on companies to ensure that the protection of children's rights is upheld by their privacy policies.[13] The UK went further, passing the Age Appropriate Design Code which sets out what this means in practice for users under 18.[14]

One issue affecting the protection of privacy rights is the regulatory variance between countries around the world, which can allow companies that work transnationally to 'game' data protection laws. An example of this is the blocking of certain websites in the EU, subsequent to the enactment of GDPR. Various companies were unable or unwilling to change their policies to meet the new data protection requirements, opting instead to regionally block access to their content for those living in the EU. Therefore, when governments seek to enact laws, corporations should cooperate to ensure ease of compliance without loss of access.[15] Similarly, laws should be drafted in a manner which would not unduly deter the creation of content or diminish access to the digital world for children.

Governments should also ensure that there are extra protections put in place for children in relation to freedom of information requests. Specifically, children's personal information should be exempt from freedom of information requests and databases with children's information should be made anonymous.[16]

The right to a reputation

Embedded within Article 16's right to privacy is legal protection for children from unlawful attacks on their honour or reputation.[17] The internet has created a unique challenge for all people who seek to manage their reputation: this is particularly true when dealing with children. It is common for children, their peers, and their parents to share personal information and images about themselves, or one another. This sharing of information and images may be done with or without the child's consent, often with harmless intentions, however not uncommonly for the purpose of harassment, bullying or exploitation.[18] When information is posted by or about a child, it may not be understood or considered that the image or information posted may resurface at a later date.[19] This could have significant consequences both in the immediate and distant future.

To protect a child's right to both privacy and reputation, amendments should be made in national law to protect children from misuse of their personal information and sharing of their images without consent.[20] This needs to be done with significant care, so as not to criminalise children or stymie the expression of the child themselves and potentially their parents. Rather, it should be framed in a manner that prevents abuse of children through the exploitation of their image or personal information.

Similarly, there should be easily accessible methods for children to request, correct, or delete data collected or published about them without their consent, that they believe could damage their reputation.[21]

Children's rights are different from those of adults, and their age, maturity and evolving capacities must be given more thoughtful consideration when we create legislation, policy and guidance. We must ensure that we uphold *all* their rights, not merely one right at the expense of all others.

[1] Forum Internum, BBC Radio 4

[2] Livingstone, S., Third, A. Children and young people's rights in the digital age: an emerging agenda, New Media and Society, 2017

[3] Article 13, UN Convention on the Rights of the Child, 20 November 1989

[4] Ibid, Article 17

[5] YouTube apologizes after parental-control feature blocks LGBTQ content, CNN, 20 March 2017

[6] Children and digital marketing: rights risks and opportunities, UNICEF, July 2018

[7] Children and parents: Media use and attitudes report, Ofcom, 4 February 2020

[8] Children's rights and business in a digital world: freedom of expression, association, access to information and participation, UNICEF, June 2017

[9] Section 230, Communications Decency Act, 1996

[10] When tech knows you better than you know yourself, WIRED, 4 October 2018

[11] Children's rights and business in a digital world: privacy, protection of personal information and reputation rights, UNICEF, 2017

[12] Ibid

[13] Milkaite, I., Lievens, E. Towards a better protection of children's personal data collected by connected toys and devices, Digital Freedom Fund, December 2018

[14] Age appropriate design: a code of practice for online services, Information Commissioner's Office

[15] Note 7

[16] Ibid

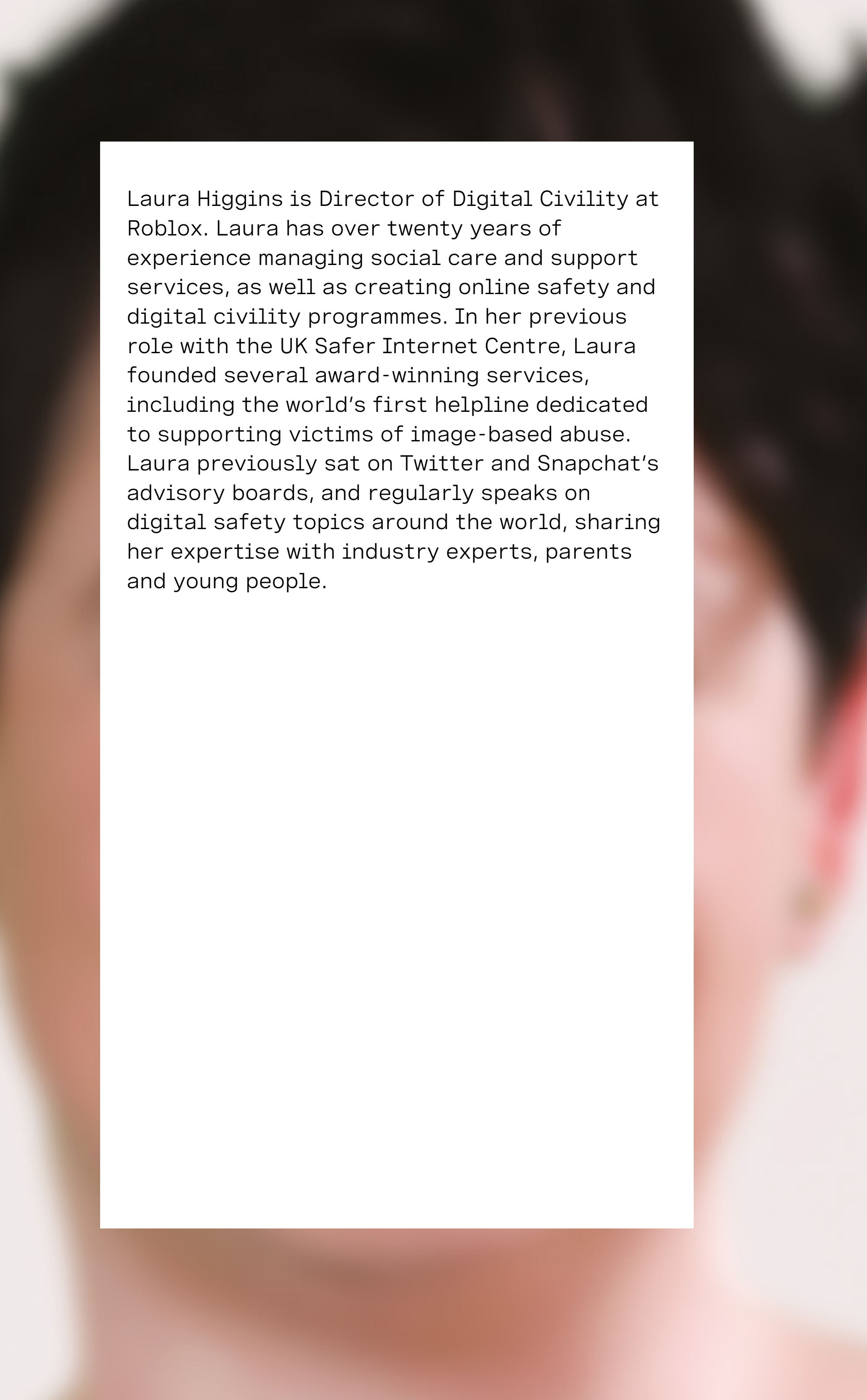
[17] Note 3, Article 16

[18] Note 10

[19] Ibid

[20] Ibid

[21] Protecting children's rights in the digital world: an ever-growing challenge, Council of Europe Commissioner for Human Rights, 29 April 2014



Laura Higgins is Director of Digital Civility at Roblox. Laura has over twenty years of experience managing social care and support services, as well as creating online safety and digital civility programmes. In her previous role with the UK Safer Internet Centre, Laura founded several award-winning services, including the world's first helpline dedicated to supporting victims of image-based abuse. Laura previously sat on Twitter and Snapchat's advisory boards, and regularly speaks on digital safety topics around the world, sharing her expertise with industry experts, parents and young people.

Laura Higgins

How Fear is Affecting Our Ability to Accept Digital Rights to Play. And Our Common Sense...

Kids need to play. Play is an essential human need. It is how all kids learn about the world around them: through it, they learn to communicate, negotiate, problem solve and resolve conflict. And play has other benefits which adults also appreciate: learning new skills, improved cognitive skills, it's a great way to de-stress and most of all it is FUN. Why is it that we immediately label digital play as bad?

The world has changed, kids and teens no longer have the freedoms many of us enjoyed when we were young. You cannot send your child out to play in the street and say 'come in when it gets dark' as was the case for many of us Gen X'ers. Kids have fewer freedoms, often living long distances away from their school friends. Being able to spend time online chatting and playing may be the only time they spend together outside of school. Why do we believe it is a waste of time?

As part of my work at Roblox (one of the world's largest entertainment platforms for kids and teens), we undertook a small-scale survey with UK parents in October 2019.[1] The results were interesting...

89% of parents told us they were worried about their kids' online gaming habits, citing concerns such as addiction, bullying, and contact from strangers, and worry their kids wouldn't make friends in the real world. Half of the parents told us that the source of their worries were stories published in the media and on social media, rather than based on their own experiences.

In contrast, 88% of parents could also recognise the benefits of gaming: improved technical and cognitive skills, social skills, and potential improved career prospects all factored highly. The contradiction is startling. What if we flipped it on its head? What if we stop worrying about the sensational headlines and learn from our kids directly? My first rule for all parents is to be present in your kids' lives, on and offline. Let them show you what their digital world looks like. You can still guide them, in fact, you MUST guide them (you wouldn't let them drive a car without lessons and many conversations to be confident they were safe. The digital world is no different). We are increasingly paranoid and yet increasingly detached: we are potentially leaving kids at more risk than if we get to know what they do online and help them build resilience and appropriate literacy skills to navigate it safely.

A great example of the harm that can be caused by fear-mongering is some of the recent media hoax stories that have appeared, such as the Blue Whale Challenge, or the 48 Hour challenge. Probably the most well-known is 'Momo' (allegedly an online challenge which put kids at risk of suicide, but in truth was a hoax featuring a model designed by a special effects studio in Japan). In the first few days of the story appearing in the media and subsequently being shared by schools and via social media, online searches for 'Momo' increased by **45,000%**, purely fuelled by kids searching for the content and scared parents trying to find out if it was true. In this case, having a few credible and trustworthy sources for the media to speak with, who could disseminate factual information to parents, could have prevented the widespread misinformation and panic that followed. We need to provide the WHOLE community; kids, parents, and most worryingly professionals, with some key critical thinking skills.[2]

Following such stories, many parents clamp down on their kids' online freedoms, limiting access to certain apps, reducing the time allowed online, and often adding monitoring software.

Whilst some of these apps can be a helpful tool (particularly for younger children), for example, if they flag genuinely harmful behaviour, adult content or grooming attempts, most are placing themselves as watchers, allowing parents to see every aspect of their kids' online lives, with access to their messages, friends, and more.

Companies profit hugely from monitoring, yet many are ineffective, or over-block content. We do not allow kids to build critical thinking skills if we remove their option to think! Parents put their faith in these apps and often forget to keep those regular conversations happening, thinking that their input towards online safety is done. Kids are also savvy and are adept at bypassing most restrictions placed on them. It is difficult to build relationships with your family if you constantly feel they don't trust you.

There is a clear cycle I see, when a negative news story breaks: schools jump on the story and further disseminate; parents panic, either confrontational or worried; kids stop talking; parents don't trust kids so they install monitoring software; kids get round this, further building distrust; communication breaks down; kids still engage in risky behavior.

Children need to be kept safe, and we all have a part to play in that. Tech companies must continue to improve, to recognise potential risks and act early on preventing harm.

However, it is difficult for companies to be innovative. We seem to be stuck in an environment where policymakers and governments respond to a big news story (I do not wish to diminish the awful nature of some online harms, whether it be exploitation of a child or suicide), demanding immediate action is taken, forcing companies to respond only to that one concern reactively, rather than organically building out strong effective tools which work across ALL potential harms on their platform.

"Current public policy is increasingly driven by over-emphasized, 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]

Of course, it is true that very young children require a controlled experience online, they need support and guidance. But as we build those skills in kids, we need to allow them more freedom, and potential offenders less. We focus too heavily on locking platforms down and we ultimately risk de-skilling our kids.

Lessons about protecting data and online safety rarely hit the mark. We believe we are talking to our kids but in reality, we aren't getting through. In response to how often parents and teens discussed appropriate online behaviour, 93% of parents and 39% of teens responded "occasionally or often", while 6% of parents and 60% of teens said that this happened "rarely or never".

And still: the main causes of kids having accounts 'hacked' or being scammed? Sharing their passwords with their friends. Such a basic lesson we should be teaching them, why does the message not get through? Companies often provide tools to keep communities safe, including parental controls where this is appropriate, but again, we know that these are used infrequently. We need to find a better way to have these conversations, at home, at school, and through the media.

Digital Literacy skills around privacy and data are an important topic to teach the next generation. All consumers have a right to privacy and increasingly the onus is (rightly) on tech companies to be transparent about what data they collect, how they store it and what they do with it, as well as the right to have data be deleted (under GDPR). There is also a broader discussion about ensuring rights are communicated in a way that is accessible and in language young people can easily understand: we need to move away from the "legalese". Whilst users need to understand they have these rights, limiting what data is collected about themselves or other users can make safety more difficult, and can impede any law enforcement investigations. It needs to be a balance, but understanding the landscape and what your rights are does help!

In conclusion, I believe it is every kid's right to have digital play, and to explore the online world safely and freely. We should focus our efforts on preventing those with bad intent from having those same freedoms.

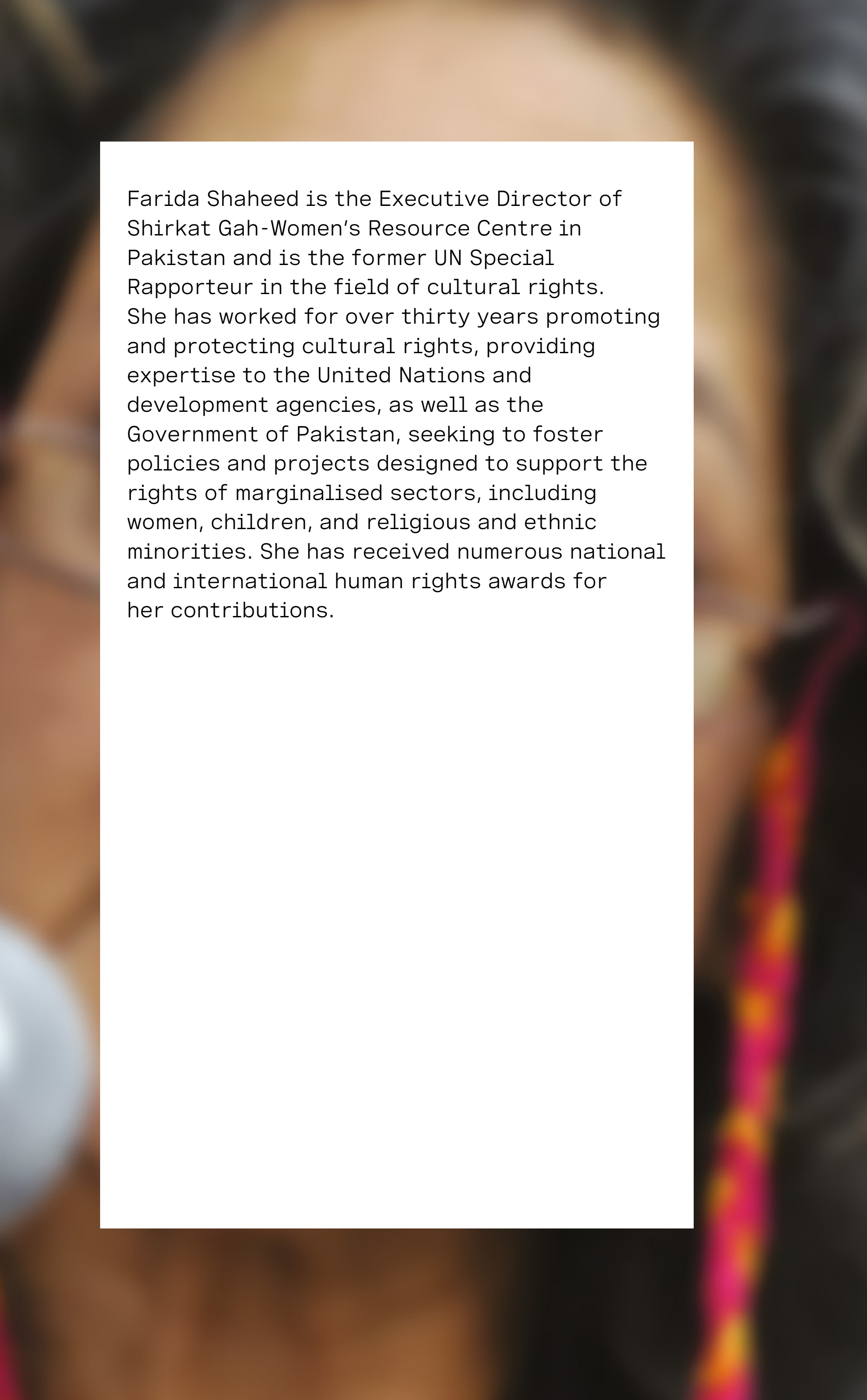
"Our resistance to digital play is just like Socrates's resistance to writing. It is futile. Your kids need your help. And it's easy to provide. Parents, children, and families just need to start playing in the digital world together."[4]

[1] Survey says parents and teens don't discuss appropriate online behaviour, Roblox, 7 November 2019

[2] Phippen, A., Bond, E. Digital ghost stories; impact, risks and reasons, South West Grid for Learning

[3] Brennan, M., Phippen, A. Child protection and safeguarding technologies: appropriate or excessive 'solutions' to social problems? 2019. Also referenced in: 'Over-blocking' online harms may infringe children's rights, digital literacy is the answer, Forbes, 30 October 2019

[4] Shapiro, J. The New Childhood: Raising Kids to Thrive in a Connected World, 2018



Farida Shaheed is the Executive Director of Shirkat Gah-Women’s Resource Centre in Pakistan and is the former UN Special Rapporteur in the field of cultural rights. She has worked for over thirty years promoting and protecting cultural rights, providing expertise to the United Nations and development agencies, as well as the Government of Pakistan, seeking to foster policies and projects designed to support the rights of marginalised sectors, including women, children, and religious and ethnic minorities. She has received numerous national and international human rights awards for her contributions.

Farida Shaheed

Cultural Rights of Children and Young Adults in the Digital World

In an increasingly digitalised world, the lines dividing online and offline life are blurring to such an extent that for many, especially the young, such a distinction is meaningless. In many parts of the world, innumerable aspects of everyday life are digitally dependent: from taking a bus ride to completing school assignments, from grocery shopping to planning holidays. In many instances, social life, especially of the young, seems digitally driven. Digital spaces and tools have become a priority for self-expression as well as seeking information, entertainment, or likeminded people. What does this mean for those officially classified as children, including young adults less than 18 years of age? Although some services have clearly stated and published age restrictions,[†] in reality, ever younger people are digitally active, a "large and growing number of children aged 12 and under are using social media networks, often *with* their parent's knowledge and consent".[1] Even toddlers engage with the digital world. This essay considers a few challenges in promoting children's rights while

[†] Children under 13 are not entitled to open accounts on Facebook, Twitter, Instagram, Pinterest, Tumblr, Kik, or Snapchat; 17 is the minimum age for using Vine, Tinder and Yik Yak; YouTube account holders are required to be 18, but a 13-year-old can sign up with a parent's permission.

safeguarding their security and privacy from the perspective of cultural rights as human rights, that apply equally to children as adults.

Cultural rights have two essential and interdependent dimensions, both connected to our sense of self and world visions. The first is grounded in the notion of free creativity, including the freedom indispensable for artistic creativity,[2] scientific inquiry and technological inventiveness. The second is people's right to access and contribute to both cultural heritage and new thinking. Rights start with the foundational right to access, take part in and contribute to cultural life in all its facets. Access is not confined to one's own cultural life and heritage, however that may be defined, but includes the right to access and benefit from the cultural heritage, cultural life and creativity of humankind as a whole. The right to participate includes the right not to participate in any practice, ritual or process that undermines human dignity. The right to contribute means having the necessary resources, material conditions and opportunities to fully explore and develop one's creative abilities and to share these with others, both digitally and otherwise.

A first challenge concerns access. Increasingly, digital connectivity is a privileged vehicle for self-expression, social interaction, accessing information and opportunities. But access is not equal due to the lack of necessary infrastructure as well as striking language imbalances. English accounts for just over a quarter of all Internet usage (25.3%), fairly close to the one third of global native English speakers (371 million). In contrast, communication in Hindustani and Bengali, with 329 and 242 million native speakers respectively, is virtually invisible.[3] Almost two-thirds of the world's population lives in Asia, but Asian languages account for only 27% of internet communication, a mere 7% without Mandarin Chinese. From a cultural rights perspective, spaces that promote pluralism, debate and dissent, in which everyone can participate and contribute equally without fear, are vital. If young people cannot access digital spaces in their own language, how can they engage, participate fully or contribute in the digital world or know about their rights? Access brings other challenges as well.

Cultural rights protect the rights of each person regardless of age: individually, in community with others, and as groups, to develop and express their humanity, worldviews, understanding of life and development, and to pursue specific ways of life.[4] This demands freedom of expression, belief and creativity in material and non-material forms for all people, young and old. It means that everyone has the right to forge their identity and be part of multiple communities at once; to join, leave and create new communities of shared cultural values, including digital communities, and to leave without fear. Hence, children as others have the right to challenge a cultural identity they may not desire, including those of their cultural heritage. As children increasing rely on the digital world for direction and self-expression, this may lead to tensions and confrontations within the family, with implications for children's security.

The nature of the digital world itself poses its own problems. Digital services are driven by commercial interests of profit derived in large part from advertising and harvesting personal data sold to advertisers. The advertising industry imposed exogenous, partly alien ways of life on people by restructuring consumption habits long before the digital age,[5] and rising consumerism promoted by skilful advertising continues to significantly impact local cultures.[6] Our senses are constantly bombarded by commercial advertising and marketing practices systematically deploying a wide array of tools and methods that impact cultural and symbolic landscapes towards a sameness. Quickly adapting to new technologies, overt and less overt messaging makes it difficult to recognize and distinguish between commercial advertising and other content. The Committee on the Rights of the Child expressed concern that children may regard advertisements as truthful and unbiased, and recommended that States adopt appropriate regulations, encourage business enterprises to adhere to codes of conduct and use clear and accurate product labelling and information that allow parents and children to make informed decisions.[7] However, informed decisions are difficult when parents as well as teachers are less digitally savvy and literate than young adults and even children. This is further complicated when parents or teachers have had no or little access to the digital world and by the bewildering pace at which digital technologies and services are developing. Clearly, there is an urgent need to develop and enhance media literacy in schools and assess the effectiveness of such programmes, but how does one educate parents?

Commercial advertising can deeply influence people's philosophical beliefs, aspirations, cultural values and practices, from food consumption models to burial rituals, tastes and beauty canons. Using advances in behavioural sciences, advertising concentrates on the link between emotional responses and decision-making; it plays on subconscious desires around happiness, youth, success, status, luxury, fashion and beauty, suggesting that solutions to human problems lie in individual consumption and status symbols. Children who are still developing their sense of self and ideas are particularly vulnerable. How do we ensure that digital services and spaces nurture children's creativity and self-expression while instilling critical thinking and a spirit of inquiry?[8]

As UN Special Rapporteur, I recommended that all forms of advertising be prohibited to children under 12, regardless of the medium, support or means used, but how to achieve this in the digital environment remains unclear. Regulations are challenged by advertisers' ingenuity; online regulations lag behind offline regulations, enabling companies to dodge the law by relocating advertising to digital spaces. Increasingly commercial messaging is digital and difficult to avoid in a digitalized world. They use electronic devices, such as computers, tablets, mobile phones, digital billboards and games to disseminate; viral and social media advertising/marketing proliferate using social networks or contracting individuals to enter online communication forums to specifically promote a product; products or services are embedded in programmes, music, videos, and games; branded/sponsored content is designed to appear as editorial-like content. In tandem, online advertising tracks consumers' online activities to supply them with targeted advertising. Disturbingly, many advertisers claim to use neuro-marketing, including brain imaging, to elaborate advertising and marketing strategies.

The free sharing of ideas and world visions is essential, but so too is guaranteeing the ability of individuals to choose freely.

Ever-more sophisticated advertising and marketing strategies, promoting codified messages with unmatched outreach, cultivate certain values. These become significant reference points for children's perceptions about themselves, others and the world,[9] shaping the sociocultural framework within which people think, feel and act.[10] For the digitally connected, especially children and young adults, digital platforms, in particular social media, increasingly drive a sense of self and validation. This can be a source of strength and affirmation but equally of rejection and dejection. For example, the young in particular are so influenced by beauty concepts and digitally enhanced imaging that States have introduced regulations on stereotypes and body image in advertising, requiring disclosures when images have been digitally modified.[11]

The increasingly blurred line between commercial advertising and other content, the myriad advertisements and marketing communications received through digital services, and the resort to neuro-marketing aimed at circumventing individual rational decision-making are worrying, especially with regards to children. Of equal concern is that the representation of violence reinforces the efficiency of advertisements (individuals subjected to emotional stress retain messages delivered better): biochemical reactions make people more inclined to consume food with a high fat and sugar content.

The power of advertising to influence individual choices demands a careful assessment of the digital means advertisers use in the light of children's right to privacy, freedom of thought, opinion and expression, and their right to participate in cultural life, as enshrined in international human rights covenants.[12] The regulation of commercial advertising and marketing practices should accord with the principles enunciated in international and regional instruments:[13] practices must be subject to limitations such as those provided for in Article 19 of the International Covenant on Civil and Political Rights, especially restrictions necessary to ensure respect for the rights of others. More effective safeguards are needed for children, but digital companies, better resourced than many countries, remain absent from human rights arenas and discussions. Nonetheless, countries where these companies are registered have a due diligence obligation to ensure they do no harm. But the advertising industry is not the only issue.

In our digitalized world the use of digital services to circulate images of children by friends and parents needs to be examined, in particular the alarming desire to monetize such images. To become viral or have sufficient hits or followers requires images to be funny or trigger other emotions. Children may be unhappy with the images. At what age should children be included in the decisions? When can they ask for such images to be removed? What would be the procedure? How to deal with the consequences for intra-family relations are only some of the immediate questions that arise and deserve attention. In particular, data privacy regulations are needed for data collected and images and other posts shared digitally.

From a human rights perspective there are many questions that deserve attention, starting with how to ensure that the digital world is not creating huge disparities in the world of children and young adults. How do we balance the freedom and facilities children need for self-realization and self-determination with the rights of parents and other family members? Finally, without equal access and equal say in matters, can young adults and children really be considered as citizens with rights?

[1] Three reasons why social media age restrictions matter, HuffPost, 10 August 2014

[2] See (A/HRC/23/34) Report of the Special Rapporteur in the field of cultural rights - The Right to freedom of artistic expression and creativity, Office of the High Commissioner for Human Rights

[3] What are the most spoken languages in the world? Fluent in 3 months, and World population, Wikipedia

[4] First (A/HRC/14/36) and subsequent reports of UN Special rapporteur in the field of cultural rights. See Special Rapporteur in the field of cultural rights, Office of the High Commissioner for Human Rights

[5] Mass communications and the advertising industry, UNESCO, 1985

[6] Investing in cultural diversity and intercultural dialogue, UNESCO, 2009

[7] Paras. 19 and 59, General Comment 16, Committee on the Rights of the Child, 17 April 2013

[8] Report of the independent expert in the field of cultural rights, Ms. Farida Shaheed, submitted pursuant to resolution 10/23 of the Human Rights Council, A/HRC/14/36, 22 March 2010

[9] Nairn, A., Griffin, C., Gaya Wicks, P. Children's use of brand symbolism: a consumer culture theory approach, European Journal of Marketing, 2008

[10] Arnould, E., Thompson, C. Consumer culture theory: twenty years of research, Journal of Consumer Research, 2005

[11] For example, Argentina, Denmark and Mexico

[12] In particular Articles 17 to 19 of the International Covenant on Civil and Political Rights, and Articles 13 and 15 of the International Covenant on Economic, Social and Cultural Rights.

[13] Article 19 (3) of the International Covenant on Civil and Political Rights holds that restrictions shall only be such as are provided for by law and are necessary for the respect of the rights or reputations of others.

ON SECURITY

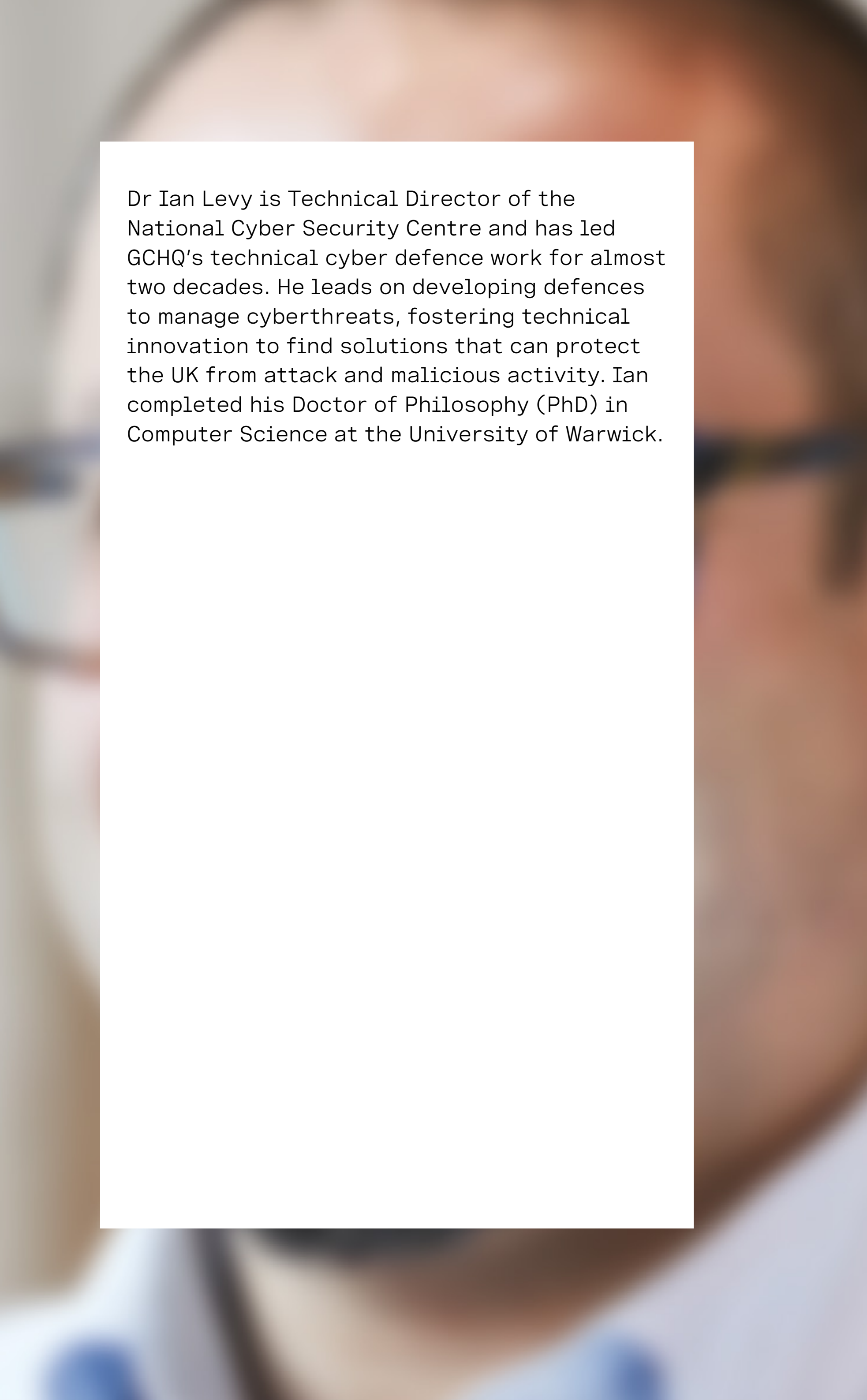
We want to be on the internet to learn and to share, but we are not ready for the whole adult world.

I’ve left all this data lying around. Damn I’m screwed. I can’t lie. If the Nazis were alive, they would be able to tell who was a homosexual. We’re screwed.

Oil and its associated riches have been the cause of war and carnage and misery since its inception. The very fact that we have this parallel with which to compare the data industry, should make us more cautious of how we approach it.

There is too much emphasis on what is illegal and not enough about what is unpleasant or distressing.

5Rights' Young Leaders



Dr Ian Levy is Technical Director of the National Cyber Security Centre and has led GCHQ’s technical cyber defence work for almost two decades. He leads on developing defences to manage cyberthreats, fostering technical innovation to find solutions that can protect the UK from attack and malicious activity. Ian completed his Doctor of Philosophy (PhD) in Computer Science at the University of Warwick.

Dr Ian Levy

On the Need for Software Safety in a Digital World

Society's expectation of children's rights has evolved with our environment, context and technology. We no longer send small children up chimneys or down mines. We no longer believe it's OK for children to drink gin. We try to ensure that children get a decent education. We believe that children should have greater control over their lives and opportunities to express themselves fully. In the digital age, what is the next step in the evolution of children's rights? I believe it's the right to safe software.

We all want our children to be safe and we take actions – both individually and as societies – to try to protect them from hazards and harms. Those hazards and harms fall broadly into three categories.

The first is hazards and harms with obvious protections. For example, it's reasonable to expect adults to know that knives are inherently dangerous products that a child is incapable of handling safely. Individual adults make consistent risk decisions – don't let kids have knives. As a society, we also further bolster that protection by making it illegal to buy a knife if you're under 18. That protection is both for the putative purchaser, but also to try to reduce the second order effects (i.e. youth knife crime). We can't expect children to process complex information in the same way as adults and therefore we can't expect children to fully understand the risks – both primary and secondary – so we put protections in place.

The second is a set of hazards and harms where the details of protections matter but are not obvious. For example, consider child car seats. We all accept that car crashes are a hazard and that a child involved in a crash is at risk of harm. But how many of us could work out the correct density of the material in the car seat that absorbs the impact? Or design ISOFIX mounts, or seat belt loops? It's not reasonable to expect parents to make these assessments, so as a society we use experts to set minimum standards and enforce those standards through law to ensure adoption. These expert-driven standards govern certain parts of our lives, providing protection for everything from toxic paint in toys, to more complex topics such as medical drug safety. Failing to adhere to the standards leads to significant consequences for those promulgating the goods involved.

Finally, there is a set of non-obvious hazards and harms that only experts can conceive before they happen at scale. Given the knowledge at the time, who could have predicted the 'magic mineral' asbestos would have such a terrible effect on health? Who would have predicted that square windows on early commercial aircraft would lead to fatal structural failure? In retrospect, with our knowledge today, these are obvious. Similarly, the mental health impacts of a mobile phone that automatically airbrushed selfies are obvious in retrospect, but they weren't to the software engineer who invented it. Neither were the harms caused by social media-enabled cyber bullying, or by paedophiles contacting children using credible (but false) online personas. Data driven micro-targeting on the internet probably wasn't an obvious consequence of the first supermarket loyalty card to its inventor.

Across these different types of hazards and harms, individuals and societies provide protection for our children before the harms accrue. We engender an implicit right to a safe childhood. What does this look like in the future digital age? What's the digital equivalent of making a safe car seat? Or ensuring toys don't contain lead paint?

I think the physical hazards and harms faced by children today will be broadly the same in the future, but the digital hazards and harms that children already face today will become much more impactful. Currently, our digital identity is secondary to our physical identity, so when a large-scale data breach occurs (as it does all too often), the actual impact on people is relatively small. Of course, there are exceptions, for example, the customer list of a sexual health clinic being disclosed would have a significant impact on those people. On the whole, our digital identities are fungible. For our children, their digital identity will, for all intents and purposes, become their immutable, primary identity.

Today, we take ubiquitous internet connectivity for granted, and its absence is merely an inconvenience. For our children, ubiquitous connectivity will be necessary for them to function in society. With their experiences increasingly lived through and affected by technology, software will pervade every aspect of their lives. It already enables ubiquitous communication, whether a part of our mobile phone infrastructure or the social media platforms we increasingly rely on. Software is what enables our devices and apps to do the apparently magical things they manage to do. Software is what keeps our critical infrastructure working optimally. In the future, software will have more direct impacts on us, and will even be the arbiter of certain parts of our lives, deciding whether we can do particular things. This is what leads me to contend that our children have a right to safe software.

Safe software should, at its most basic, protect itself from cyber-attack. We've seen poor cyber security lead to real world hazards and harms for children; fitness trackers that could be abused by anyone to monitor the location of any child wearing the device. Medical devices that attackers can control to the detriment of the patient. Connected toys that expose young children to malfeasance from attackers close to them, and online services aimed only at children that leave their users' details available to anyone. These examples show that even the most basic security issues aren't always considered when designing digital stuff for children. We should be able to root out this sort of pathological stupidity by setting basic standards and ensuring they're met, something we've started to do with our code of practice for consumer internet of things devices.

In my opinion, this should belong in the first set of hazards we explored earlier: the hazard and harms are obvious, as are the mitigations. Others will say that even the most obvious cyber security mitigations aren't obvious to the majority of the population, and this should sit in the second category. I'm not sure it matters and perhaps this ambiguity is an example of how it's hard for the public to really understand these digital hazards. Either way, there should be no excuse for software to not exhibit basic cyber security. The consumer law that applies in the physical world seems to directly apply here for software, devices and services.

Safe software should minimise the harm directly caused by its use.

Safe software shouldn't help kids get access to damaging content and shouldn't target them for adverts for inappropriate products like nicotine and cosmetic surgery.

Safe software should help engender safe online behaviours in our children and not require them to divulge huge amounts of personal data to access a service. Data consent is impossible for most adults to understand, so it seems ridiculous to expect children to give informed consent.

Safe software should help minimise excessive screen time and design out features that will adversely affect our children's mental health.

Safe software should not track our children's behaviours online, other than to provide a safety net to nudge them when they're doing risky things and to intervene when they're doing dangerous things.

Safe software should provide a simple way for children to ask for help when they've made a mistake and for that help to be provided quickly and painlessly, whether the mistake was sexting someone, remotely opening the house to a burglar or reporting some bizarre symptoms to a future medical AI to try to get out of school.

Safe software should help its users protect themselves in the real world wherever possible.

And probably most importantly, safe software should be built with the safety and security needs of its users top of mind, rather than the profit of its developer. Just as in the real world, many digital spaces are shared between children and adults and yet the software behind them tends to treat all users as adult users. Children's needs are different to adults, but they have a right to have them satisfied.

These are broadly the sort of hazards and harms we see online today, and they will only get more numerous and more impactful as our technological innovation continues apace. However, I believe these hazards and harms broadly fall into our second category: at a high level they're obvious, but the solutions may be complex and require technical know-how to understand. We need to change the narrative we have today, which is largely based on hyperbole, distraction and fear. What is the software equivalent to the ECE R44 'safe car seat' mark to help children and parents make good purchasing choices? Again, consumer law in the physical world broadly translates to the digital world, but we need to better understand standards of due diligence in the digital world.

As we move towards the world where software pervades every characteristic of our lives, I believe we'll move into the third category of hazards and harms that we, as society, can't easily predict (if at all). There's often no physical equivalent, and there's certainly no consumer law protections in place here. Think about the data economy/surveillance capitalism we have today, where we effectively barter for services using our data. Originally conceived to target adverts, we're starting to see the darker side of this economy with intrusive and inappropriate use of these data in cases like Cambridge Analytica. The discoverable power in those data (and the concomitant potential impact on real lives) will continue to increase if left unchecked, leading to an unrecoverable erosion of long-term digital privacy for our children's generation. We now understand this fact: we should do something about it.

We know that use of new technologies in a pervasive way will have effects on users in ways we don't really understand because we've not spent the time researching the downsides. For example, I have real worries about the possibility of biased artificial intelligence algorithms disadvantaging an entire sub-population of a generation in ways we cannot conceive today.

I worry about us building critical services that our children will rely on for their daily lives using infrastructure that was never designed to support this.

I worry about malign nation states attacking the companies that build these systems to ensure they have cyber-attack capabilities or long-term leverage over other nations, and that really means the citizens of those nations.

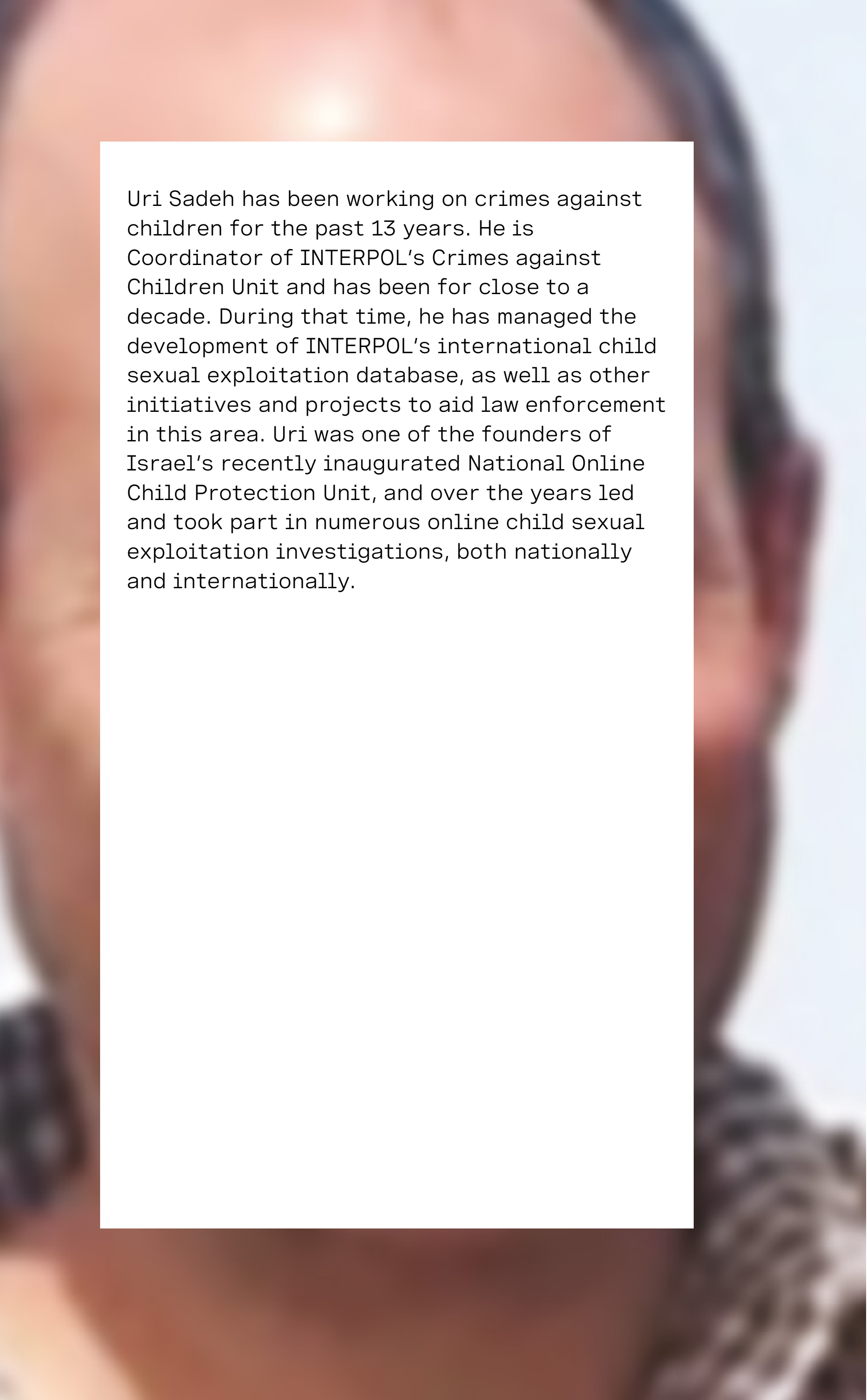
I worry about us continuing to judge the safety and security of large-scale software systems through marketing hype and biased rhetoric, rather than science and evidence.

But most of all, I worry about software taking the place of the people who teach our children social norms, respect for others, and the ability to judge real world risk on a day-to-day basis. It seems that we are destined to repeat the tragedies of the past in the inculcation of software into our lives. The devastating effects of thalidomide in pregnancy were not adequately considered at the time, an event that led to much more stringent drug testing and regulatory regimes around the world. While the effects software will have on our children will be very different, I believe they could be the same order of harm, but at a scale we have not seen before. But we can fix this. We have the majority of the science we need, and we have proven harm reduction approaches in other spheres of life that we can re-purpose. We just need to apply them properly.

I believe in neither the utopian nor dystopian view of our technological future. But I absolutely believe that software will forever change how our children live, interact, work, play and grow. It will change their fundamental relationship with the things around them, including their ability to communicate, exchange knowledge and possibly even their thoughts and dreams. And I know for a fact that the way we build software, the way we deploy software, services and devices, and the way we talk about the very real risks that can accrue from the unwise use of software are wholly inappropriate for the risks our children will face.

We need to learn from the past and other sectors. Software is not benign, and it will never be error free. The companies that build and profit from software are rarely entirely altruistic and will often have incentives that aren’t aligned with the safety and security of our children. As a society we need to decide when it's acceptable to use software, what long term impacts we're willing to tolerate for the service or benefit we get, and how we judge and regulate the systems that enable all this. Pervasive software could be a massive force for good in our children's lives, but it is unlikely to become that if the market is left to its own devices. That's true in digitally advanced markets like the UK, but it is also true in markets where technology is just being introduced where citizens don't yet have the digital skills necessary to operate safely.

I believe a child's right to safe software is essential to ensure their safe and secure future, wherever they live on the globe. And it is our collective responsibility to ensure that right becomes a reality before irreparable harm happens. It's for government, academics and tech industry to provide us with a language to describe these things, but it's up to all of us to demand better from our software, services and devices.



Uri Sadeh has been working on crimes against children for the past 13 years. He is Coordinator of INTERPOL's Crimes against Children Unit and has been for close to a decade. During that time, he has managed the development of INTERPOL's international child sexual exploitation database, as well as other initiatives and projects to aid law enforcement in this area. Uri was one of the founders of Israel's recently inaugurated National Online Child Protection Unit, and over the years led and took part in numerous online child sexual exploitation investigations, both nationally and internationally.

Uri Sadeh

Who Are We Afraid Of?

13 years ago, I got involved in the protection of children from online sexual exploitation. We had little in terms of tools and procedure, and most police forces did not have dedicated and specialised staff working this area of crime.

13 years later, we have many more specialised investigators around the world, sophisticated technology to help us detect and locate such exploitation, and… far more online abuse cases and victims: far more applications, social media platforms and online games are available; far more children are online and at a younger age.

Anyone working to enforce this area of crime cannot escape the feeling that despite increasing investment by governments, we are only reaching the tip of the iceberg. The extent of internet facilitated child sexual exploitation is just overwhelming.

Many good people are working on improving the tools for prevention and detection of child sexual exploitation online, and for identification of offenders and victims. Artificial intelligence, among other technologies, is looked to as a technology that might aid detection of offending on different platforms and aid investigators, in the face of the massive amount of child sexual abuse, its images and its videos, that is online and on offenders' devices.

While 13 years ago children had to sit at a computer at home to get online, now the internet is in their hands or pockets constantly. While 13 years ago few children, of whom were predominantly teenagers, were online and exposed to risks of being groomed into exploitation or being sexually extorted, today it is more and more common to investigate cases of children, eight years old and at times even younger, active online and running accounts on Instagram, Facebook, WhatsApp, Kik, Musical.ly† and numerous other services and applications available to them on their smartphones.

In 2018, providers of online services, such as the above, based in the USA alone, reported 18 million incidents where they suspected child sexual exploitation or crimes against children were taking place.

Eight-year-old children have no ability to protect themselves from the temptations, manipulations and dangers the open web poses for them; nor do ten-year olds or 12-year olds. A huge and international 'army' of child sexual predators are present on pretty much any internet platform kids frequent. The internet is a paradise for those predators, a vast gallery of children they can pray on.

The extent of the danger is alarming, and the number of child victims impacted is overwhelming. Children are commonly victim of crimes ranging from sexual harassment and exhibitionism, to sexual extortion, rape, and suicide incitement online.

Numerous wonderful investigators are working restlessly and successfully to detect and arrest offenders sexually abusing children online. We will continue doing this and continue developing cutting-edge tools to aid us. But this is often after some victims have been harmed, and this is a continuous chase.

It is clear that we have no way of effectively assuring children's safety online, and the above numbers speak for themselves. Parents are not equipped or able to protect their children online, even if they understand that they should. Law enforcement is unable to do it either, and will only get to a fraction of the many offenders and victims. Nor is industry,

† Now TikTok

despite some growth in effort and reporting, able to assure children's safety from avoiding mental and bodily harm on its platforms.

There is, however, one obvious way in which we can effectively protect those children: the same one used in relation to other environments or practices dangerous to children. It is not to let them go there.

We would not give a knife to a child, and certainly not without supervision, as they are neither mature nor responsible enough not to hurt themselves or others. We limit the age at which a teenager may drive a motorcycle or car to an age where they are judged to be mature and responsible enough to not create risks to themselves and others. We set clear limits and do not allow children to buy cigarettes or alcohol, or to enter nightclubs. We set these laws and limits to protect children, to protect their wellbeing, their health, and their bodies. Often to the kids' discontent, but for their own good. Paternalistic? Yes, and in the most basic sense of the word. It is our obligation as society, as adults and as parents.

Why is it that we allow the same immature, naive, vulnerable kids, to go effectively unsupervised, into the dangerous alleys of the internet, where we know they are likely to be harmed in horrible ways?

Allowing your child to go online, open accounts and communicate with others is the equivalent of sending them downtown to walk the streets and interact with whomever they come across: chat to them, hold their hand, perhaps see what their sexual preferences are. In a way it is even worse, as online they never really know with whom they are talking or experimenting sexually with as predators may have any face: a boy, a girl, a model, a soccer star, a friend, and so on.

The argument that the internet opens and exposes the world to your child, ignores the grim fact that it actually opens and exposes your child to the world.

Now, we tell ourselves, 'but I talk to my child, I explain those dangers to them, I warn them, they understand, they would never...'. Would you give your ten-year old the kitchen knife, explaining the danger, and then leave them to use it unsupervised? Send them up to their bedroom to play with it?

In the last few years, my colleagues and I have visited hundreds of homes where a child has been a victim of sexual violence online, including being forced to insert objects into their genitalia (which under legislation in some jurisdictions constitutes rape), or living under sexual blackmail for years. Does anyone think their parents imagined that? Thought this was likely to happen to their kid? These kids look like your kid, and their parents like us. You cannot open the "door" to the vast internet for your child and expect them not to walk through it.

Smartphones and tablets have largely become our babysitters: producing hours of wonderful quiet, while our children stare and interact with those screens. No need to entertain them, no need to go out: they love it in their room.

Those endless screen hours come at the expense of parent-child interaction, relation, creation, attention.

Putting all the above aside for a second, we are exposing our kids to extremely violent material (beheadings, snuff[†]) and above all, pornography. A week ago, I talked to a very informed and able friend. She told me that they have installed parental controls on their 11 and 14-year-old sons' smart phones and now limit them to two hours of internet per day. That is 14 hours per week. A full day, from wake to sleep, of screen-time and exposure. She also said that they were struggling to limit the younger one's consumption of pornography, which started when he was about nine. One can only imagine how the gender perception of an 11-year-old who has been watching pornography for years develops.

What I have found in so many families, in whose lives I unwillingly found myself involved, was a social and parental meltdown. Parents afraid to set rules, afraid to separate their children from their smartphones: even in the face of a police officer home visit. Parents who sit in the living room, unaware of the horrors their child is experiencing in the next room. Parents whose first goal was to obtain the smartphone back from police as their child screams for it. The phone which served to violate their child.

There is some progress. Some schools now remove smartphones from pupils during school time. Some parents roll

[†] Snuff is a genre which shows scenes of homicide and death.

back to 'stupid phones', allowing children texting and calling functions, but no more.

These measures and take-up, however, remain few in number: both the number of schools and the few brave and invested parents. It is high time for government and society to act on their commitment to protecting children: guiding parents and placing responsibility on whoever puts a child at internet-risk.

Governments and society should stop the unacceptable situation where companies, who create dangerous internet environments, accessible to children who are then offended against and harmed, are not held accountable for the crimes they are effectively enabling and facilitating against children. We demand that businesses who operate environments which are dangerous to children ensure that children do not have access to them, or can only enter accompanied by an adult. A bar allowing a child to consume alcohol would be held accountable; a public pool allowing unsupervised access for children would be accountable; failing to install a railing high enough to protect children from falling would render a constructor accountable for an injured child.

It is unacceptable that internet industry operates and profits from platforms which put children at harm, without being held accountable. If they cannot ensure children's safety, they should not allow children onto their platforms. If they do not have effective mechanisms to keep children off their dangerous platform, they should not be allowed to operate it altogether.

Industry, which would obviously not want to let go of children as its consumers and targets of massive advertisement campaigns, could focus on developing child-safe phones, which would simply not allow access to types of platforms deemed unfit and unsafe for children. Phones would allow controlled communication, and minimise, if not eliminate, exposure to risks.

The age at which youth are deemed responsible and mature enough to understand the risks and act accordingly can be discussed and defined by relevant professionals. There certainly is such an age, under which they are not. Relevant professionals can also discuss and define the types of communications a child can use in safety.

Setting such limits to children’s access to the internet would actually constitute true protection of children’s privacy: protection from the inherent exposure of their personal details and being to the world. Allowing a child unsupervised access to internet platforms and accounts is not ‘respecting their privacy’: it is effectively ‘respecting’ their absolute loss of it.

RX Radio is a radio station run by and for children, operating from the Red Cross War Memorial Children’s Hospital in Cape Town, South Africa. It is the first radio station in the world that trains child reporters to broadcast from within a hospital. It seeks to empower all children who are admitted to hospital to tell and listen to stories about issues that are important to them. The presenters strive to improve children’s experiences of the hospital, of theirs’ and adult’s understanding of their illness, and produce quality programmes by, and for, children and young people. In the last three years, RX Radio has trained 100 young reporters (ages four to 18) at Red Cross and Paarl Hospital. A team of seven staff, volunteers and former reporters (ages 18+) work behind the scenes to train, coordinate, and support the reporters, but the children are always behind the microphones and are active participants in the production: they design their own shows, choose the music, invite guests, write interview questions, and even plan fundraising events.

RX Radio

Our Voices: The Importance of Listening to Young People to Make the Digital Environment a Safe and Inclusive Place

It is known that the digital space is not really able to protect its young users from the looming dangers that are brought about by sharing the same environment with 'users' who use it for different reasons. To fully understand the need to be able to control, to some extent, the functioning of the digital space and the inevitable social exchanges that it exposes children to, the different platforms that children navigate on a daily basis should be monitored. And most importantly, children should be part of this process, through encouraging them to express their experiences in the digital space. At RX Radio, we value the input of our young reporters and below they have shared their experiences of privacy, security and freedom in line with their exposure to the digital environment and how they can be protected.

One of the Young Reporters, Alex White (16 years) had this to say:
A major issue with technology and its use by youth today, is that many young people don't understand that sharing personal information could put them at risk, or how at risk they might be when performing different actions in the digital world. This could be because they are simply too young to

understand, because they are more focussed on using the end product that everyone else is using, or simply because they don't have time to read the fine print. This means that often, when teenagers or children enter information to sign up to different products, they don't realise what can be done with that information. Currently, children are at risk of revealing information and exposing data about themselves (that should rather be kept private) without even realising it. There is a lot to ask for when it comes to protecting children and their rights. Since most internet companies are profit-driven, it is regrettable that they take a lax approach.

In spite of this, there should definitely be mechanisms to protect children when they are online, as they are vulnerable in what is a very daunting and overwhelming space. Like driving, the consumption of alcohol and many other actions that could have serious consequences when undertaken at a young age, there should at least be some sensible limitations on what children can access and/or do online, so that they are protected and able to learn about the space before they are exposed to it.

Age restrictions do already attempt to deal with this issue on most platforms, however they are generally still flawed in their implementation, and sometimes it is as easy as entering the right birth year for children to sign up to platforms that they are too young to access.

At RX Radio, we rely heavily on the internet: our young reporters use the internet on the production side when it comes to preparing for shows, finding news stories and downloading music. Since many of the children involved with RX Radio access the internet when they visit the station, we have included clear rules and guidelines in our station's Code of Conduct, regarding how to properly act online. This was stressed again in a special station-wide meeting that we had in order to train all reporters as to what is okay to do online while at the station (and in general), and what is not. Through this, all the reporters are aware of the dangers that come with the internet and are able to use it responsibly, to help with their work at the station. There are consequences if the internet is misused and we engage with reporters to address issues, and find solutions. It just goes to show that proper awareness training and education can go a long way to protecting children online.

If listeners aren't based at the hospital, then they have to tune in online, either through our website, or the RX Radio app. Since we know that our content is going to be viewed by children, we make sure that all our pages are safe and don't contain any inappropriate links like pornography, strong language or violence. While there is only so much we can do on our side to protect listeners, we definitely realise, due to our unique position as a children's radio station, that the internet does have massive benefits. There are dangers, but they can be managed through awareness, policies and responsible internet usage.

It's important for families to talk to their children about the internet and its inherent dangers. The more children are able to understand, the better. If parents are able to convey the issues that children might be faced with online, it will only be beneficial in the long run since so many children have a desire to be online, and to 'explore' the world. The safer they start out, and the better their initial habits are, the safer they will be.

Tech companies should see it as their responsibility to try to implement 'child-friendly' modes of their online products wherever they can, so that children are able to learn and browse the internet as freely and as safely as possible. An example of this would be Google's Safe Search, Netflix's Kids Mode, or YouTube's Safe Mode.

Tarique Kenny, RX Radio Young Reporter (18 years) also had this to say:

It's not a fair trade for young people's private information to be given to online services as a term of use. While analytics and marketing are companies' business models, there is a fear that children's private information will fall into the wrong hands. Technology companies need to put policies in place to ensure the privacy and security of young users. For instance, in the description of the website or app, it should be stated who can access the user's data and with whom the data will be shared. Users should be educated as to what data they can safely give out, depending on the app or website. They should also do thorough research to determine how reputable the site is that they are using. This is why it is important for the parent/legal guardian to educate themselves on the digital environment, so that they can pass knowledge down to the younger generations. Parents/legal guardians should take responsibility for educating themselves on exactly what the digital environment is and what it consists of, as well as all the positives and negatives that come with it.

The digital environment should be used as a platform for young minds to educate and express themselves freely, and to communicate and share opinions with one another. The digital environment also shows great promise for future entrepreneurs. Despite the amazing potential for the digital environment to support children throughout their developmental stages, there are certain harmful things to a child's sensitive mind that could have a negative impact on their developmental growth and result in poor characteristic traits.

Once a parent is educated about the digital environment, they should sit down and explain to their child the features of electronic devices that are important for their development, while explaining there will be certain content that will be harmful, and which parents should steer them away from.

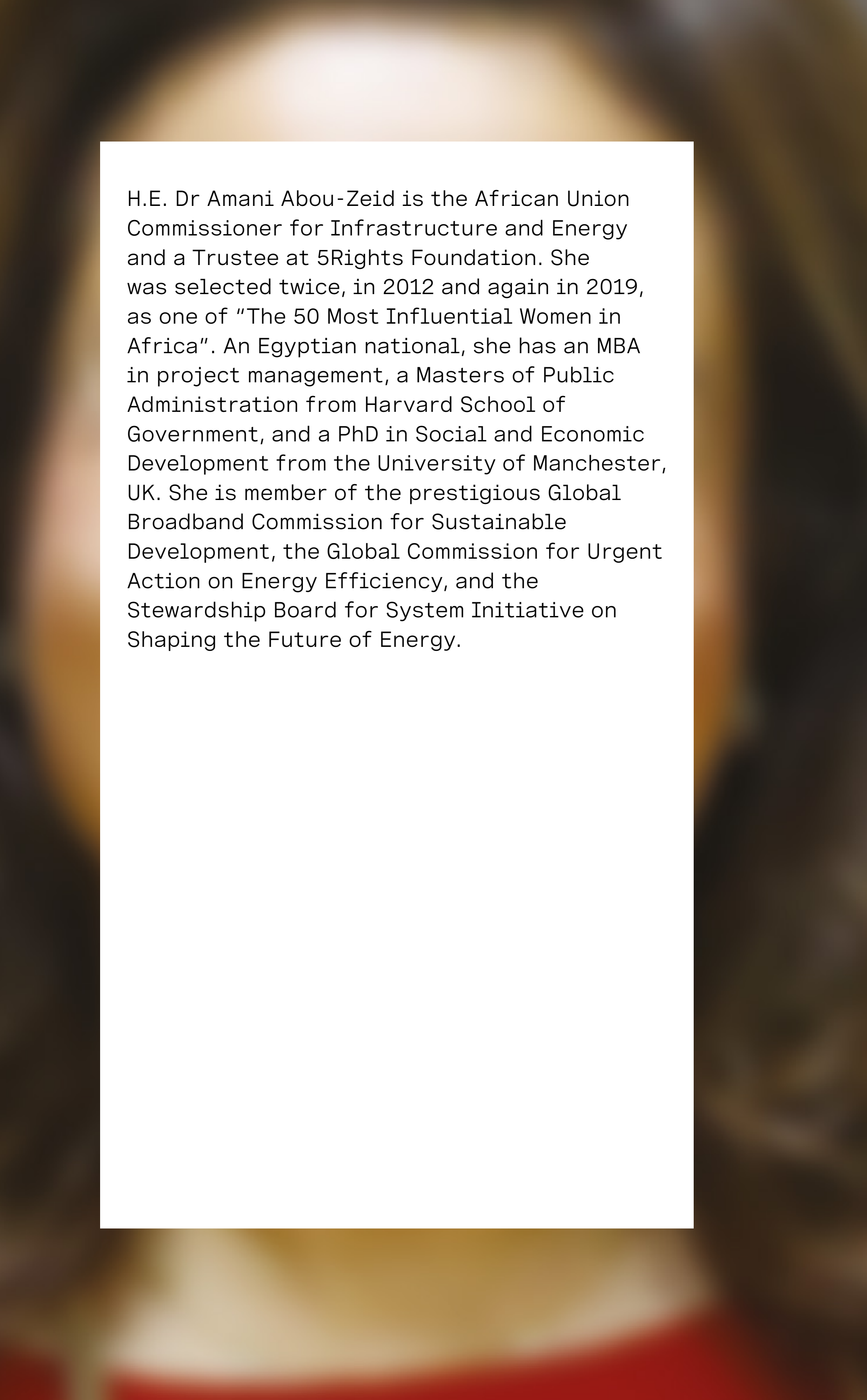
Children will always have a curious mind-set which is why if a child receives an electronic device from any age below 15, the child should be monitored from time to time. This could be done by restricting access to certain websites and occasionally checking the child's phone, as developmentally, these are the ages when children are most likely to be curious and experimental. Once the child reaches the age of 16 and starts to emerge into adulthood, parents should allow them more freedom and privacy, as the child should already know what is acceptable and unacceptable, with the freedom to make their own distinctions as to what they feel is correct. However, there should still be guidance from a parent/legal guardian.

With all that needs to be done to make the internet environment a safe space, young people in South Africa still experience challenges accessing the internet. Let me share a bit about my internet struggle. The way for me to have freedom to access the internet is by taking a walk to the local library. However, I am not entirely safe due to the area that I reside in. I am in danger of getting robbed or even murdered by gangsters. RX Radio is the safest environment for me to have access to internet: it's also free and I have no time restrictions as to how long I can use it. However, another big hurdle is the cost of traveling to RX Radio and the time it takes to travel. The duration of my travel time is two hours, and if I leave RX too late, I risk coming home to an area where gang violence escalates, particularly in the evening time.

**

The views expressed by our reporters reiterate the fact that a lot still needs to be done to make the digital space child friendly. Their feedback also highlights the importance of parental involvement in making sure that the digital space influences children positively, through showing an interest and familiarising themselves with all the corners of the sites that their children navigate. As noted earlier, sometimes children are unaware of the landmines that they come across and detonate when they unknowingly engage with harmful content in the digital environment: it is always a click away. Sometimes parents don't know how to protect their children from the digital environment as this environment was not part of their childhood. As Tarique has mentioned, educating parents on the ins and outs of the digital environment could be very beneficial, especially parents who live in communities that still continue to exclude them.

The digital village is not really a safe space for children, even in countries where its use is prominent and monitored, and it is even worse for children who use digital spaces without supervision and protection. They become easy targets and therefore, it can be said that a lot must still be done to improve it. The digital space has become an unavoidable part of children's current spaces and can be used positively, but that will begin when children are engaged, and can understand the extent of the influence that the digital environment has on them.



H.E. Dr Amani Abou-Zeid is the African Union Commissioner for Infrastructure and Energy and a Trustee at 5Rights Foundation. She was selected twice, in 2012 and again in 2019, as one of "The 50 Most Influential Women in Africa". An Egyptian national, she has an MBA in project management, a Masters of Public Administration from Harvard School of Government, and a PhD in Social and Economic Development from the University of Manchester, UK. She is member of the prestigious Global Broadband Commission for Sustainable Development, the Global Commission for Urgent Action on Energy Efficiency, and the Stewardship Board for System Initiative on Shaping the Future of Energy.

H.E. Dr Amani Abou-Zeid

Harnessing the Power of Digital Transformation for Young People in Africa

Digital Transformation can be the catalyst for the African continent to vault into the 21st century and will accelerate us toward achieving the UN Sustainable Development Goals and the Aspirations of the African Union Agenda 2063. Undoubtedly in the African context, the digital revolution will be led primarily by its young population. According to the United Nations population estimates and projections, 41% of the African population is under the age of 15 and roughly 60% is aged below 25 years. UNICEF's State of the World's Children: Children in a Digital World report in 2017 discloses that one in three Internet users is younger than 18 years.

However, the increasingly digital and data-driven information society comes with risks and challenges. New rules are required that would generate trust, while protecting and securing data across the entire value chain, particularly for vulnerable and marginalized groups, including children.

With this goal in mind, the Executive Council of the African Union (AU) endorsed in 2018 "The African Union development of the Digital Economy" and adopted "Cybersecurity as a Flagship project of the African Union Agenda 2063".

Back in 2014, AU Summit adopted the African Union Convention on Cyber Security and Personal Data Protection ("the Malabo Convention"). The Declaration set a strong objective of African action on cybersecurity and personal data protection to deliver benefits to all Africans. Section II, Article 29 of the Convention pertains to offences specific to Information and Communication Technologies, and requires States to take necessary legislative and/or regulatory measures to make the production or dissemination of child sexual abuse through digital technologies a criminal offence.

To facilitate implementation of the Convention, the African Union Commission (AUC) developed the Privacy and Personal Data Protection Guidelines for Africa ("the Guidelines") in collaboration with Internet Society (ISOC) in 2018. The Guidelines were created with contributions from regional and global privacy experts, including industry privacy specialists, academics and civil society groups. The AUC also published in 2016, in cooperation with Symantec and the US State Department, a report on Cybersecurity and Cybercrime trends in Africa.

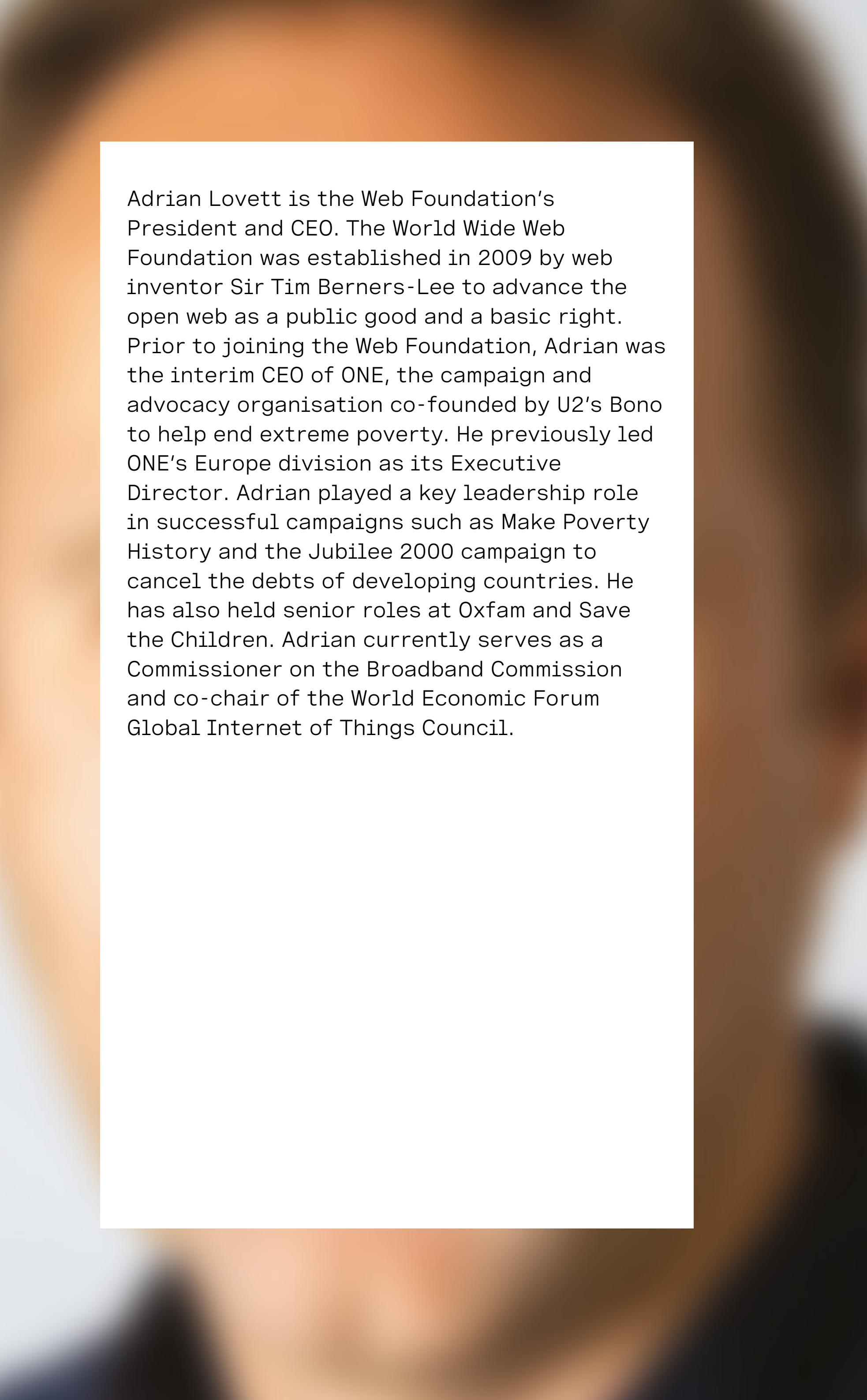
Since the adoption of the Malabo Convention, the AUC has been organizing cybersecurity capacity building workshops, in collaboration with our key partners, Regional Economic Communities (RECs) and Member States. This work promotes cybersecurity culture and builds trust and confidence in the use of ICTs by, and for, the African citizens. The workshops provide guidance on cybersecurity policy and strengthen cyber capacities of various stakeholders on issues including: cybercrime prevention; online privacy and personal data protection; preparation of cyber-strategies and cyber-legislation; and setting up incident response mechanisms such as Computer Emergency/Incident Response Teams (CERT/CIRT).

However, there are major challenges faced by Member States of the AU. They include achieving a level of technological security adequate enough to prevent and effectively control technological and informational risks in cyberspace, particularly for children; as well as building an information society that respects values, protects rights and freedoms, and guarantees the security of the property of individuals, organizations and nations. They also include how States can support citizens to contribute to the knowledge economy, guarantee equal access to information while stimulating the creation of authentic knowledge platforms, and creating a climate of confidence and trust, that is predictable, organized, protective of consumers and citizens, secured, and integrated into international order.

To overcome the abovementioned challenges, Member States of the AU must develop and update national cyber-security strategies in line with international standards and practices, and support the creation of a national governance structure for cyber-security. They must adopt and implement legal frameworks for online privacy and personal data protection to allow African citizens to safely and securely use ICT for their socio-economic development (health, education, commerce, governance, etc) as a sine qua none condition for peace and stability.

States should develop human and institutional capacity building in cybersecurity and prevention/prosecution of online crimes, particularly against the vulnerable groups, and implement ICT/cybersecurity awareness classes in early stages of children's education. States must enforce the existing national criminal laws and adapt them to the realities of the digital environment to effectively fight against all kind of cybercrime and cyber-attacks, and develop legal and regulatory frameworks and specific provisions related to cyber legislation: with more emphasis on child online protection. Similarly, States should develop technical capabilities to monitor and defend national networks to protect Institutions against threats and attacks capable of endangering their survival and efficacy, and build and operate CERT/CIRTs. Finally, they must develop continental and regional mechanisms to increase regional and international cooperation on cybersecurity and the protection of children online.

It is important to move from establishing measures which purely protect children online, to those that actively empower them and provide them with the right competencies they need to ensure their wellbeing and fully enjoy their rights online. There is, therefore, an urgent need for a global structural approach, based on effective policies to benefit children in Africa and elsewhere, harnessing the power of digitalization so that they become active digital citizens. This requires that girls and boys are equally empowered with appropriate digital skills.



Adrian Lovett is the Web Foundation’s President and CEO. The World Wide Web Foundation was established in 2009 by web inventor Sir Tim Berners-Lee to advance the open web as a public good and a basic right. Prior to joining the Web Foundation, Adrian was the interim CEO of ONE, the campaign and advocacy organisation co-founded by U2’s Bono to help end extreme poverty. He previously led ONE’s Europe division as its Executive Director. Adrian played a key leadership role in successful campaigns such as Make Poverty History and the Jubilee 2000 campaign to cancel the debts of developing countries. He has also held senior roles at Oxfam and Save the Children. Adrian currently serves as a Commissioner on the Broadband Commission and co-chair of the World Economic Forum Global Internet of Things Council.

Adrian Lovett

As The World Wide Web and the Convention on the Rights of the Child Both Turn Thirty, the Web Can Help to Secure Children's Basic Rights

Three decades ago, as the 1980s came to an end, revolution was in the air. The Berlin wall came crashing down and the dust that rose from it carried the hopes of a generation of Germans for reunification and peace, and a sign of hope to a watching world.

At the same time, 700 miles away at the CERN laboratory[†] near Geneva, a young software engineer named Tim Berners-Lee was focused on his own revolution, triggered by the difficulties in sharing information between the computers in CERN's vast network. Tim had written a memorandum to his boss called "Information Management: A Proposal". In its modesty and apparent ordinariness, it could hardly have felt more different from the sense of history in the making under the Brandenburg Gate. And yet, the World Wide Web Tim envisioned in that memo would go on to change our world, expanding access to knowledge and freedom of expression more than any other development in modern times.

But there was one more quiet revolution underway in Geneva. While Tim was tinkering at CERN, over at the Palais des Nations, UN negotiators were concluding a ten-year

[†] The European Organization for Nuclear Research

process involving governments, activists and experts worldwide to negotiate a set of fundamental rights held by children.[1] The Convention on the Rights of the Child (UNCRC) was adopted by the United Nations General Assembly on 20 November 1989 and since then, it has transformed millions of children's lives around the world.

While these were three separate phenomena, today they seem intertwined as one thread. The demolition of a barrier to the dreams of a new generation. The creation of a means by which those young people could access, share knowledge, and claim their rights like never before. And a radical charter to articulate and defend those rights, for the youngest members of society.

Just over half of the world is now online and UNICEF estimates that one in three internet users are children. All around us, we have examples of young people using the web to innovate, express themselves, share knowledge and connect with people globally, in ways that weren't possible three decades ago.

But for all of the web's great benefits, it is not the unambiguous public good it was intended to be. Many children and young people don't have it at all, and those who do face a growing number of risks online. We need to make sure all children can access the web and use it safely.

Half the world is still missing out on the web's benefits. Those offline are disproportionately female, poor and live in rural areas. About 29% of youth[†] worldwide are not online, around 346 million individuals.[2] Gender and economic inequalities mean men are 12% more likely than women to be using the internet, and 60% of young people in Africa are not online, compared with only 4% not online in Europe.[3]

For those who are online, the web is delivering tremendous benefits, but it is also coming at a cost. The web children access today has a host of problems, from data breaches and censorship, to misinformation, bullying, surveillance, discriminatory algorithms and risks of child abuse and

[†] Aged between 15 and 24

exploitation. And the challenges facing children online are growing. For example:

The recently released report of the Broadband Commission, of which I am a member, on child safety online shines a light on the harms facing children including sexual abuse, online harassment, exposure to misinformation and age-inappropriate content.[4]

In the UK, 79% of 12-15-year-old internet users claim they've faced at least one potentially harmful experience online in the past 12 months.[5]

At the Web Foundation, our own research with teenagers in low and middle-income countries shows the challenges of social media and privacy. We've heard from teenagers including an eleven-year-old outlining how *"Sometimes, I feel like I don't have privacy anymore. Even if I do not post often in my accounts, people will still see me in tagged posts, comments, from albums of someone else. Social media has become invasive."*[6] The dry words of the UNCRC, stating that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy" suddenly seem deeply relevant.

This is not the web that Tim Berners-Lee intended and it must not be the web of the future.

When I joined the Web Foundation as CEO in 2017, my colleagues told me about a boy in a community they had worked with in Pretoria, South Africa. This child was disappearing from home every night for several hours. After a while, his parents discovered he was travelling several miles across town to use a free public Wi-Fi connection. When they asked him why he did it, he said: *"At home, I live in a shack. When I go online, I don't live in a shack".*

That boy's story stuck with me. It's impossible not to be thrilled at the possibility and adventure the web has opened up for him. The web he connects to today is complex, more resembling an entire city than the limited information-sharing system of CERN 30 years ago. As Tim Berners-Lee himself has said, *"The web has become a public square, a library, a doctor's office, a shop, a school, a design studio, an office, a cinema, a bank, and so much more."*[7] Though exciting, this expanding online world is also disconcerting. Just as it gives young people like this boy new opportunities, it exposes them to a new world of threats. We have a duty to protect young people from the harms they face online.

In the physical places where we live, children are - at least to some degree - protected.

What if we thought about the web in the way we think about our villages and towns, with children in mind? A child-friendly approach to the web would create an online experience that is accessible, safe and empowering for children. And given the challenges all of us face online, it might just appeal to a lot of adults too.

Imagine a web where all children have access, where their rights are protected, where design takes account of their distinct needs, where significant spaces are specifically for children and where harms to children are not tolerated. How would that look? How can that be achieved?

Nine ideas to get us started come to mind:

> **Safe spaces for children online.** The entire web community (including governments and companies) should ensure there are allocated safe spaces for children online, just like playgrounds in the offline world where they can explore and play under supervision.
>
> **Child-focused risk assessments.** Governments and companies who provide online services to children should have dedicated methods for identifying and mitigating risks, primarily through risk assessments.
>
> **Data protection and consent.** Children should not have sensitive data, like health or location data, collected about them without their parents' consent as well as their own.
>
> **Strong privacy settings by default.** Websites should set default privacy settings to "high", which is good

for children and adults alike. Users of any age shouldn't be burdened by having to choose more privacy-protective settings.

Protections from adult contact. Governments and companies should ensure meaningful protections are in place to prevent adult strangers from contacting children online via social media.

Features to help children stay safe. Companies should use "nudges" to help children have a safer and more empowering experience online, from reminding them to check their privacy settings to encouraging them to report bullying or harassment to companies, parents, educators or law enforcement.

Digital literacy training. Governments should invest in digital literacy training and curricula for children, with a focus on how they can use the web in ways that are safe and empowering.

Tools for parents. Parents need tools to talk to their children about using apps and services, and ways to review their children's privacy settings.

Restrictions on advertising. Targeted advertising to children should be strictly limited and online marketing of certain products, such as high fat, salt and sugar food and drinks, and alcohol, should be prohibited.

These kinds of protections are consistent with an online community that looks out for children, as any community should. Around the world, some cities are going even further to improve the lives of children through "child-friendly city" initiatives guided by the UNCRC.[8] These cities are taking additional steps to ensure children have active, engaged and safe lives, and are protected from exploitation, violence and abuse, supported by governments, civil society, companies, academia and with children themselves at the centre.[9]

If we can build a child-friendly city, perhaps now is the time to build a child-friendly web. We'll need the same broad involvement of actors to make this a reality. The community needed to protect young people on the web must include parents and schools to equip children to be safe online, governments implementing protections such as legislated standards and default privacy settings, and companies proactively managing their platforms in the interests of children. Child-focused organisations, such as 5Rights and UNICEF, and global internet governance organisations such as the Broadband Commission should also be involved.

Finally, to protect children online, we need a coordinated global effort to safeguard the web itself for all humanity. To do this, Tim Berners-Lee and the Web Foundation are building a Contract for the Web grounded on human rights to safeguard the future of the Web. The process has involved nearly 300 companies (including Google, Facebook, Microsoft, Telefonica, Twitter, and Pango), more than 100 civil society organisations (including Avaaz, CIPESA, The NewNow, and the Wikimedia Foundation), ten national governments (including France, Germany, Gambia, Ghana, Italy, Spain, Switzerland, the UK and Uruguay) and more than 8,000 citizens from around the world.

In November 2019, we launched the Contract for the Web. Now for the first time ever, we have a global plan of action created by experts and citizens from across the world to make sure our online world is safe, empowering and genuinely for everyone.

The Contract lays out a vision for the web we want and provides a roadmap for the policies and actions we need to get there. It sets the standards we must meet to achieve a safe and empowering web for all, and lays out the direction for future policy solutions. These standards include making sure everyone can connect to the internet all of the time, ensuring our data is protected, and reducing online hate by strengthening community-building online. It provides governments, companies and citizens with concrete actions they can and must take to build a better web.

The Contract will also give civil society and individuals a tool to push governments and companies to adopt the right laws and policies. And it gives us a way to measure how well those governments and companies are doing so we can hold them accountable.

Together we can create an approach that protects the web as an open and free space, and one that is accessible, safe and empowering. That would be great for children. It might just make a better web for all of us, too.

[1] Frequently asked questions on the Convention on the Rights of the Child, UNICEF

[2] The state of the world's children 2017: children in a digital world, UNICEF, 2017

[3] Ibid

[4] Child online safety: minimizing the risk of violence, abuse and exploitation online, Broadband Commission for Sustainable Development, October 2019

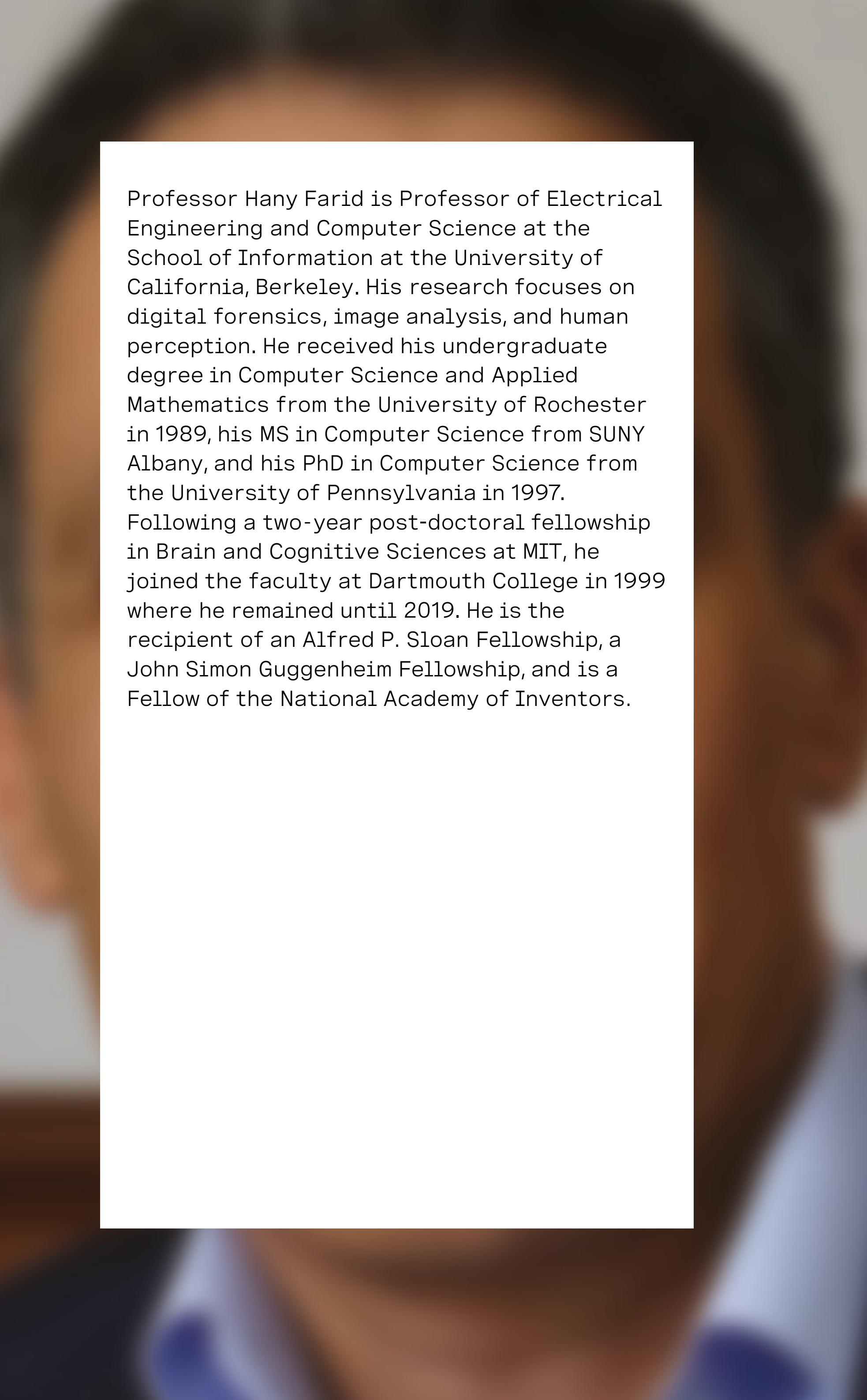
[5] Internet users' concerns about and experience of potential online harms, OFCOM and Information Commissioner's Office, May 2019

[6] Teenagers on social media: Understanding and managing privacy, Web Foundation, 4 September 2018

[7] 30 years on, what's the next #ForTheWeb? Web Foundation, 12 March 2019

[8] What is a child-friendly city? UNICEF

[9] Ibid



Professor Hany Farid is Professor of Electrical Engineering and Computer Science at the School of Information at the University of California, Berkeley. His research focuses on digital forensics, image analysis, and human perception. He received his undergraduate degree in Computer Science and Applied Mathematics from the University of Rochester in 1989, his MS in Computer Science from SUNY Albany, and his PhD in Computer Science from the University of Pennsylvania in 1997. Following a two-year post-doctoral fellowship in Brain and Cognitive Sciences at MIT, he joined the faculty at Dartmouth College in 1999 where he remained until 2019. He is the recipient of an Alfred P. Sloan Fellowship, a John Simon Guggenheim Fellowship, and is a Fellow of the National Academy of Inventors.

Professor Hany Farid

Protecting Children Online: The Past, Present, and Future

Let’s begin with some sobering statistics: in 2018 alone, the US-based National Center for Missing and Exploited Children (NCMEC) received to their CyberTipline over 18.4 million reports, constituting over 45 million pieces of child sexual abuse material (CSAM). This is a rate of approximately 2000 reports per hour, every hour, every day, every week, every month of the year. These reported images record the sexual assault of, for the most part, children under the age of 12 (and often as young as a few months). Since its inception in 1998, the CyberTipline has received a total of 55 million such reports, meaning that the reports from 2018 alone constitute approximately half of all reports over the past two decades.

Even with these staggering numbers, they are only the tip of the spear, as we are only accounting for one reporting agency, and are not accounting for the entirety of online services (many of whom don’t actively participate in programs to report CSAM), services that use end-to-end encryption, peer-to-peer networks, personal correspondences, and for the entirety of the dark-web.

How, in 20 short years, did we go from the promise of the internet to democratize access to knowledge and make the world more understanding and enlightened, to the horror that is the internet today?

The past

The landmark case of New York v. Ferber made it illegal to create, distribute, or possess child sexual abuse material (CSAM). The result of this ruling, along with significant law enforcement efforts, was effective, and by the mid-1990s, CSAM was, according to the NCMEC, on the way to becoming a "solved problem." By the early 2000s, however, the rise of the internet brought with it an explosion in the global distribution of CSAM. Alarmed by this growth, in 2003, Attorney General Ashcroft convened executives from the top technology firms to ask them to propose a solution to eliminate this harmful content from their networks. Between 2003 and 2008 these technology companies did nothing to address the ever-growing problem of their online services being used to distribute a staggering amount of CSAM with increasingly violent acts on increasingly younger children (as young, in some cases, as only a few months old).

In 2008, Microsoft invited me to attend a yearly meeting of a dozen or so technology companies to provide insight into why, after five years, there was no solution to the growing and troubling spread of CSAM online. Convinced that a solution was possible, I began a collaboration with Microsoft researchers to develop technology that could quickly and reliably identify and remove CSAM from online services. Within a year we had developed and deployed such a technology: photoDNA, a robust hashing technology. Robust image hashing algorithms like photoDNA work by extracting a distinct digital signature from known harmful or illegal content and comparing these signatures against content at the point of upload. Flagged content can then be instantaneously removed and reported. PhotoDNA has, in the intervening decade, seen global adoption (it is licensed at no cost) and has proven to be effective in disrupting the global distribution of previously identified CSAM: more than 95% of the 18.4 million reports in 2018 to NCMEC's CyberTipline, were from photoDNA.

This story illustrates an important point. The issue of inaction for more than five years was never one of technological limitations, it was simply an issue of will: the major technology companies at the time simply did not want to solve the problem. This is particularly inexcusable given that we were addressing some of the most unambiguously violent, heinous, and illegal content being shared on their services. The issue was, in my opinion, two-fold: (1) Fear. Fear that if it could be shown that CSAM could be efficiently and effectively removed, then the technology sector would have no defense for not contending with myriad abuses on their services; and (2) Priorities. The majority of social media services are driven by advertising dollars which in turn means that they are motivated to maximize the amount of time that users spend on their services. Optimizing for the number of users and user engagement is, in many cases, at odds with effective content moderation.

The present

In the intervening decade following the development and deployment of photoDNA, the titans of tech have barely done anything to improve or expand this technology. This is particularly stunning for an industry that prides itself on bold and rapid innovation.

In the defense of the technology sector, they are contending with an unprecedented amount of data: some 500 hours of video uploaded to YouTube every minute, some one billion daily uploads to Facebook, and some 500 million tweets per day. On the other hand, these same companies have had over a decade to get their house in order and have simply failed to do so. And these services don’t seem to have trouble dealing with unwanted material when it serves their interests. They routinely and effectively remove copyright infringement material and adult pornography.

During his 2018 Congressional testimony, Mr. Zuckerberg repeatedly invoked artificial intelligence (AI) as the savior for content moderation (in five to ten years’ time). Putting aside that it is not clear what we should do in the intervening decade, this claim is almost certainly overly optimistic.

Last year, for example, Mike Schroepfer, Facebook’s chief technology officer, showcased Facebook’s latest AI technology for discriminating images of broccoli from images of marijuana.

Despite all of the latest advances in AI and pattern recognition, this system is only able to perform this task with an average accuracy of 91%. This means that approximately 1 in 10 times, the system is wrong. At the scale of a billion uploads a day, this technology cannot possibly automatically moderate content. And this discrimination task is surely much easier than the task of identifying the broad class of CSAM, extremism, or disinformation material.

By comparison, the robust image hashing technique used by photoDNA has an expected error rate of approximately one in 50 billion. The promise of AI is just that, a promise, and we cannot wait a decade (or more) with the hope that AI will improve by nine orders of magnitude when it might be able to contend with automatic online content moderation.

End-to-end encryption

Earlier this year, Mr. Zuckerberg announced that Facebook is implementing end-to-end encryption on its services, preventing anyone (including Facebook) from seeing the contents of any communications. In announcing the decision, Mr. Zuckerberg conceded that it came at a cost:

"At the same time, there are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services," he wrote. ˋEncryption is a powerful tool for privacy, but that includes the privacy of people doing bad things. When billions of people use a service to connect, some of them are going to misuse it for truly terrible things like child exploitation, terrorism, and extortion."

The adoption of end-to-end encryption would significantly hamper the efficacy of programs like photoDNA. This is particularly troubling given that the majority of the millions of yearly reports to NCMEC's CyberTipline originate on Facebook's Messaging services. Blindly implementing end-to-end encryption will significantly increase the risk and harm to children around the world, not to mention the inability to contend with other illegal and dangerous activities on Facebook's services.

We should continue to have the debate between balancing privacy afforded by end-to-end encryption and the cost to our safety. In the meantime, recent advances in encryption and robust hashing technology mean that technologies like photoDNA (i.e. robust image hashing) can be adapted to operate within an end-to-end encryption system. We should make every effort to find a balance between privacy and security, and not simply sacrifice one for the other.

Counter-arguments

The argument against better content moderation and end-to-end encryption usually fall into one of several categories.

Freedom of expression. It is argued that content moderation is a violation of the right to freedom of expression. It is not. Online services routinely ban protected speech for a variety of reasons, and can do so under their terms of service. Facebook and YouTube, for example, do not allow (legal) adult pornography on their services and do a fairly good job of removing this content. The reason they do this is because without this rule, their services would be littered with pornography, scaring away advertisers. You cannot ban protected speech and then hide behind freedom of expression as an excuse for inaction.

Marketplace of ideas. It is argued that we should allow all forms of speech and then allow users to choose from the marketplace of ideas. There is, however, no counter-speech to child sexual abuse material, bomb-making and beheading videos, threats of rape, revenge porn, or fraud. And even if there was, the marketplace of ideas only works if the marketplace is fair. It is not: the online services have their thumbs on the scale because they promote content that engages users to stay on their services longer and this content tends to be the most outrageous, salacious, and controversial.

Sunshine. It is argued that "sunshine is the best disinfectant," and that the best way to counter hate-speech is with more speech. This, again, assumes a fair marketplace where ideas are given equal airtime, and that the dialogue around competing viewpoints is reasoned, thoughtful, and respectful. Perhaps this is true at the Oxford debate club, but it is certainly not the case on YouTube, Twitter, and Facebook where some of the most hateful, illegal, and dangerous content is routinely shared and celebrated. Perhaps sunshine is the best disinfectant: but for germs, not the plague.

Complexity. It is argued by technology companies that content moderation is too complex because material often falls into a gray area where it is difficult to determine its appropriateness. While it is certainly true that some material can be difficult to classify, it is also true that large amounts of material are unambiguously illegal or violations of terms of service. There is no need to be crippled by indecision when it comes to this clear-cut content.

Slippery slope. It is argued that if we remove one type of material, then we will remove another, and another, and another, thus slowly eroding the global exchange of ideas. It is difficult to take this argument seriously because in the physical world we place constraints on speech without the predicted dire consequences. Why should the online world be any different when it comes to removing illegal and dangerous content?

Privacy. It is argued that end-to-end encryption, without safeguards or access under a lawful warrant, is necessary to protect our privacy. Erica Portnoy, from the Electronic Frontier Foundation (EFF), for example, argues that *"A secure messenger should provide the same amount of privacy as you have in your living room. And the D.O.J. is saying it would be worth putting a camera in every living room to catch a few child predators."* On the first part, we agree: you have certain expectations of privacy in your living room, but not absolute privacy. On the second part, we disagree: first, the DOJ[†] is not asking to place a camera in every living room. It is asking to be allowed to view content when a lawful warrant has been issued, as it can in your living room. And lastly, is the EFF really comfortable referring to 45 million pieces of CSAM content reported to NCMEC last year as "a few child predators?"

[†] Department of Justice

Conclusions

We can and we must do better when it comes to contending with the horrific spread of child sexual abuse material. I reject the naysayers that argue that it is too difficult or impossible, or those that say that reasonable and responsible content moderation will lead to the stifling of an open exchange of ideas.

ON PRIVACY

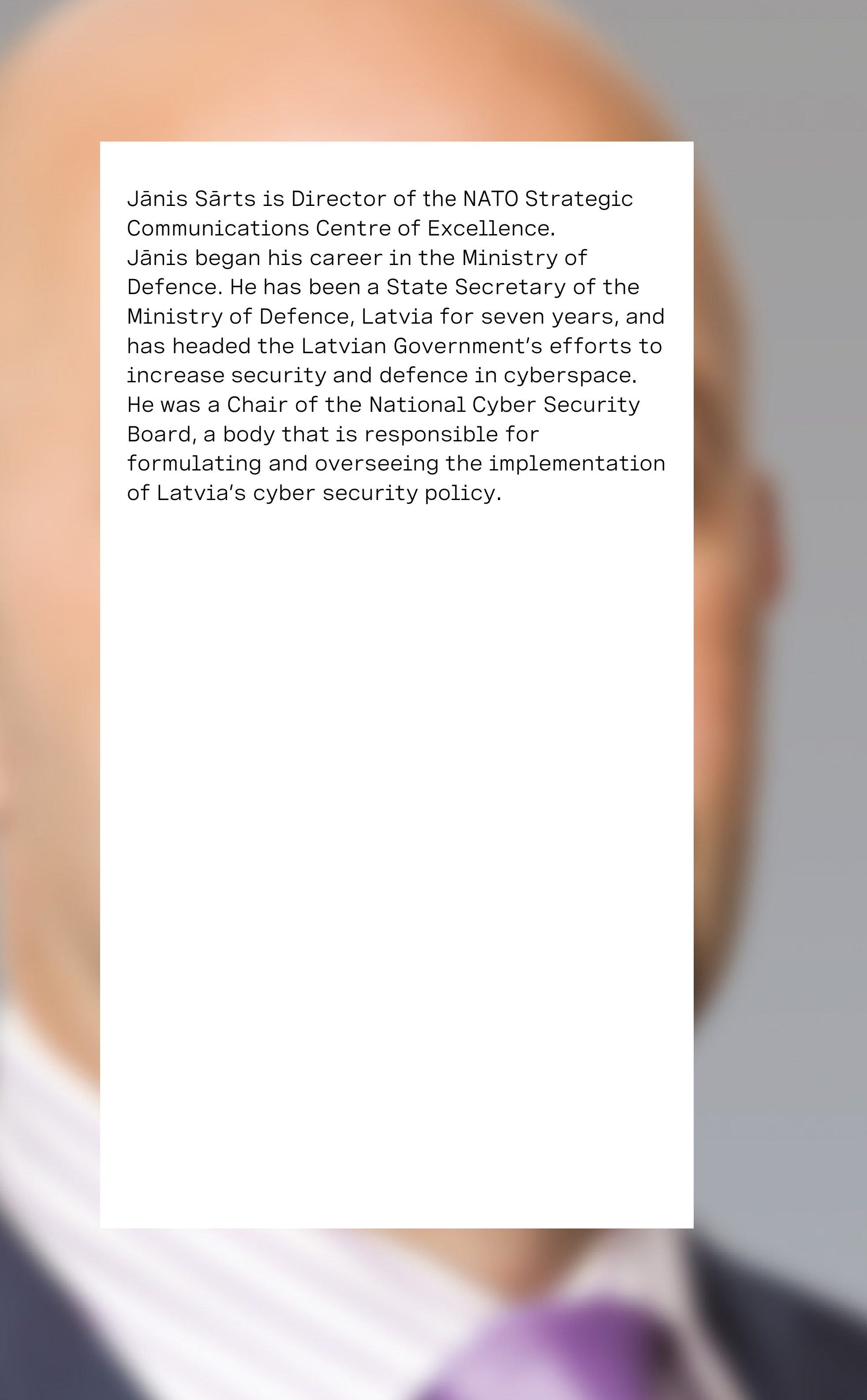
I didn’t know the internet
knew that much about you.
I thought it’s just what you
put out there.

It surprises me how
much data is collected
about you every day
and how much they know
about you.

I don’t want people I don’t know, knowing stuff only I or my friends should know.

I’m telling the companies to stay away from my data! If they want it, they should ask.

5Rights’ Young Leaders



Jānis Sārts is Director of the NATO Strategic Communications Centre of Excellence.
Jānis began his career in the Ministry of Defence. He has been a State Secretary of the Ministry of Defence, Latvia for seven years, and has headed the Latvian Government's efforts to increase security and defence in cyberspace. He was a Chair of the National Cyber Security Board, a body that is responsible for formulating and overseeing the implementation of Latvia's cyber security policy.

Jānis Sārts

Securing Digital Natives!

Recently I was at a party with friends, where one of them, knowing the issues I work on, came to me with a story that had deeply disturbed him. He told me how, one evening, he and his wife were discussing the need to have a short break from their intensive work schedules and to take a short escape trip to a European city. After some deliberation, they settled on Barcelona. The same evening, he was spooked that, when opening his Facebook account, the first posts he found there were recommendations for Barcelona, despite the fact that they had not started any search for flights or hotels. His conclusion was that Facebook was listening to them; a deduction he wanted to confirm with me.

That was not the first time I was asked that question while hearing similar stories. What I answered was that, for all we know Facebook does not listen to our private conversations: it just has very rich data sets and increasingly good artificial intelligence algorithms (AI) that give it the ability to predict our future behaviors. I could see my friend was not fully convinced. It is hard to accept that we are so predictable and easily influenced.

To me, this story once again illustrated how unprepared we are as societies and individuals to face a data-driven world. As we as people emit ever-larger amounts of data in the digital world, players with increasingly sophisticated technological tools who are equipped with the latest research from the field of cognitive sciences are starting to get deeper insights into our behavior patterns and decision making. This allows for increased influence by a few, over many. However, the scale and efficiency of these operations are unclear since there is a limited amount of publicly available, reliable data on technology-driven influence on peoples' behavior.

To assess the potential practical effects of data-based impacts on behavior, the NATO affiliated Center of Excellence on Strategic Communications conducted an experiment in 2018.[1]

During the experiment, a team of researchers was imbedded into the red team during a NATO military exercise. They were tasked with seeking open-source data about military personnel involved in the exercise and based on available datasets seek to impact their behavior patterns during this exercise. The results were very disturbing. Researchers were able to incite military personnel to act against the orders they were given (leaving the positions they had to defend), and induce other types of behaviors that were counterproductive to the successful outcome and the security of this military exercise. It is worth mentioning that these were full time, professional military personnel that had received training on the risks of the digital environment.

Although this was a limited experiment with narrow focus, I believe it gives an insight, at least, into how big data, AI and cognitive sciences can be misused and their potential power to induce behaviors: even ones that are clearly counterproductive to the best interests of the individual in question and their organizations.

What, in my view, are the wider implications of such conclusions? Emotional and instinctive human decision-making is an easy target for these kinds of impacts, and rational assessments of the information we are consuming can be circumvented rather easily. Data that we as citizens of increasingly digitalized societies are producing is very rich and easy to retrieve. Some of the richest datasets have been produced by us and by people that are very close to us, clearly not understanding what this data can tell about us and how data emitting from different sources can be interrelated to profile an individual. The longer people have been "digital", the richer data becomes, the more accurate insight on an individual one can have, and therefore the more efficiently behaviour can be impacted.

Interestingly enough, in the current digital environment it is very hard to detect if anybody is using such technology and similar techniques to change behaviour, because of a lack of transparency.

Clearly, children and youngsters are one of the most vulnerable groups. Many of them are digital natives from the moment they are able to walk (sometimes even earlier). One of the effects is how rich the data may become throughout their lives. In terms of privacy, that would mean that companies and AI can not only attain a reasonably full picture of who you are, what you do, and how you act currently, but track these datapoints over the course of many years, potentially giving very deep insights into personality and its driving factors.

Another risk is for youth decision-making. As the experiment described above demonstrates, it is easy to trigger an adult's instincts and emotions to produce a desired behaviour.

Youngsters, especially adolescents, are especially prone to making emotional and instinctive decisions. This behaviour typically coincides with a younger age group who excessively use digital interaction and communication tools, thus enriching available data considerably (relative to other age groups). This group may be the most vulnerable to psychological influence in the digital arena. Of course, at the same time, we have seen youth groups develop through multiple experiences in their digital life and develop organic resilience to some of those effects that we do not see in older groups.

In sum, if data is the oil of 21st century, youth is one of the richest, *if not the richest*, future oilfield in the human landscape, and we have very little understanding of who and for what purpose this oilfield is being drilled.

I agree with those believing in the potential of new technologies to make our lives and societies significantly better. However, currently most data systems are used to create better-targeted ads and impact our user choices. This technology can and should be used to create better healthcare, develop individualized education, more efficient public transport, better use of public resources, etc. But, as we are striving for it, we should always remember the inadvertent negative effects technologies can help to create. I think balance lies in developing technologies which consider the societal effects and possible risks, while creating regulatory frameworks that do not impede technological development.

Some potential ways forward

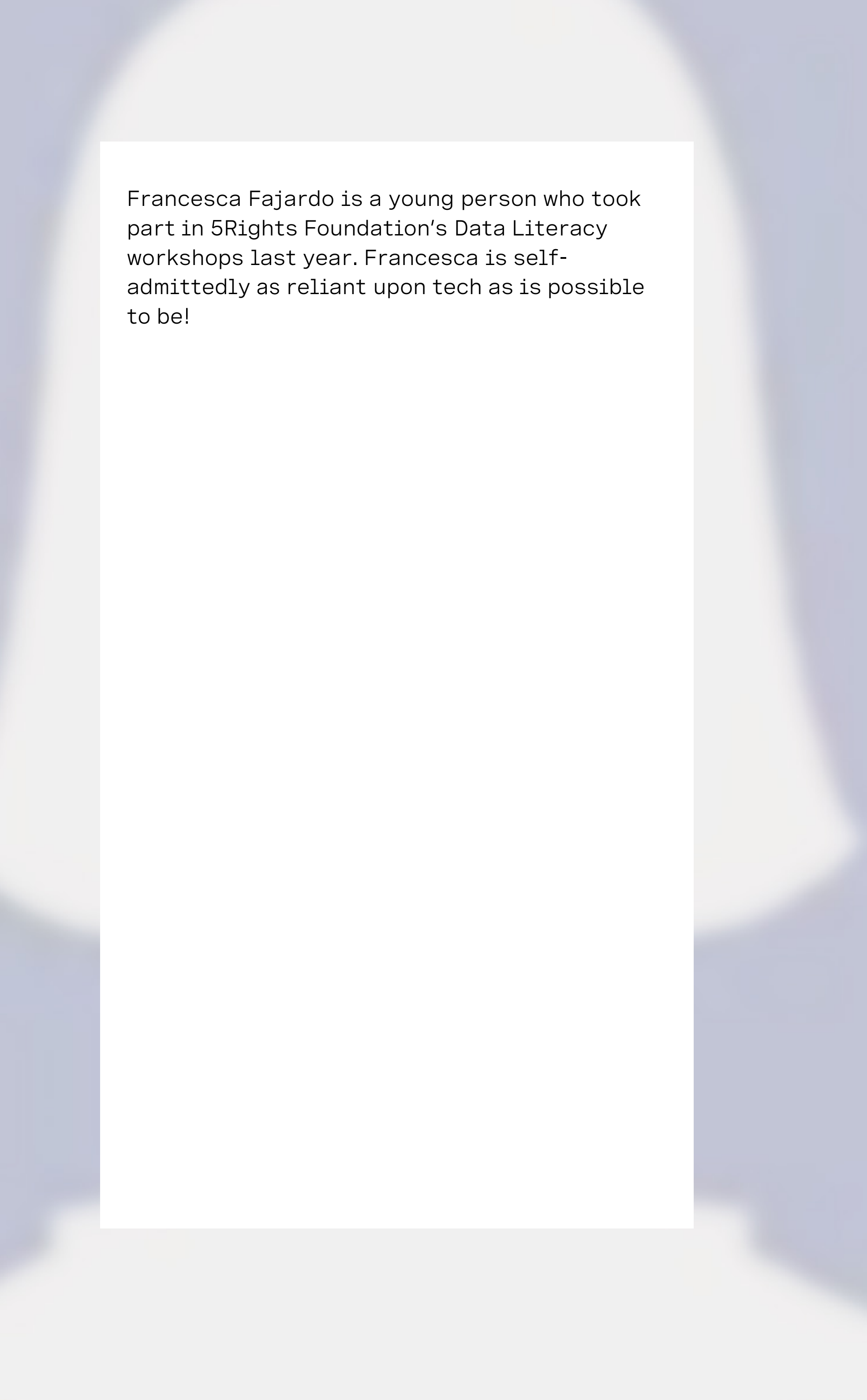
We clearly need to agree upon what constitutes the ethical and moral use of data! As AI develops, data will provide more and more opportunities. With the introduction of 5G infrastructure and the internet of things (IoT) the amount of data that can be generated will grow exponentially. I do not believe we should be embracing every opportunity given by new technology. I think we need clear rules to identify where AI is, and prevent AI from, making us behave differently. For establishing these rules, we need to see how human rights and human freedoms can be applied, to set the rules for the digital environment.

Secondly, we clearly lack transparency. How is my data being used? Is someone trying to affect my behaviour based on harvested data? Is somebody buying my data? Although GDPR has given some controls to the individual, it is not enough.

If data is so powerful, should we (and under what circumstances) allow data on children under the age of 18 to be collected? I see a case where we would allow such data collection (for education or healthcare) on minors *only under strictly defined*, and very few, circumstances.

Of course, the introduction of digital hygiene training in school curriculums from the very first years of school is a clear requirement. We also need to invest in new educational tools for digital hygiene and secure online behaviour for minors through relevant games, using virtual reality and augmented reality technologies to enhance the learning experience, while also making it appealing, contextual and fun.

[1] The current digital area and its risks to serving military personnel, NATO Stratcom Centre of Excellence, January 2019



Francesca Fajardo is a young person who took part in 5Rights Foundation's Data Literacy workshops last year. Francesca is self-admittedly as reliant upon tech as is possible to be!

Francesca Fajardo

My Data Isn’t Even Mine

I’m eighteen, I’ve had a phone since I was eleven and computers have been an ordinary object to own in my lifetime. My generation was the first to think nothing of a smart phone as a first phone. We possess phones owned by companies that know more about us in our teen years than our own parents. This is generation Z.

The generation prior was lucky to have had a brick phone and a home PC in their late teens.

Generation X (mainly the parents of generation Z, branded the tech generation) grew up pre-Apple, pre-Google and on the advent of new, time saving devices and applications, jumping full body towards the technological river, soon integrating newer technology in old institutions, schools, hospitals in other personal and professional capacities.

The more we became reliant on unchecked systems, the harder it became to hold them accountable.

We are held in a form of Stockholm Syndrome with our apps and manufacturers. Ordinary people don’t have an option to refuse to input their data. If you’re not on the work WhatsApp group, you won’t be privy to changes in schedule. If you won’t input your data when searching for a job at the job centre, you will be sanctioned.

Once our medical records told the story of our health, now it's our search engines holding on to our every symptom: deepening our paranoia by signposting us more symptoms of related diseases. In most cases, we are not diseased. The system however is! When our concern means our "clicks" and our clicks mean profit, ethics quickly disappear. Legislation is not keeping up with the speed of technology and, as with any unregulated revenue source, poor ethics are trumping decency.

After researching my mother's arthritis, I was signposted towards links for medical CBD, vitamin supplements, arm supports and menopause advice.

Educing and then abetting paranoia must be seen for what it is, and not heralded by an entire industry as enterprising.

Our own NHS is falling victim to the data savagery that is now the most profitable resource even ahead of oil, according to a 2017 article in The Economist. The oil industry is a good indicator of what power data companies hold. Oil and its associated riches have been the cause of war and carnage and misery since its inception. The very fact that we have this parallel with which to compare the data industry, should make us more cautious of how we approach it. On a personal note, I am fearful that any individual actions are meaningless when the companies update their policies and data usage to keep the law two steps behind.

I am not ashamed to say that techno jargon washes a foot above my head, but no one wants to admit that they do not read the terms and conditions before they click "ok". We need these services: we rely on them to organise protests against governments and group chats of governments themselves.

Ads are targeted towards us, based on our political preferences; not just our choice of take-away. The role of Cambridge Analytica in the Trump and Brexit campaigns was in combing through data and targeting those susceptible to be influenced in the interest of the campaigns funding Cambridge Analytica.

Like our shame admitting our inability to check every "cookie" notice, we are similarly ashamed to admit that our opinions and thoughts can be influenced. This induced shame is keeping us silent. We feel personally accountable. We have been told to feel personally accountable despite most of us being separate from the class of people designing our digital space. As participants in the virtual climate, we deserve to understand in layman's terms, what the bloody hell is going on.

Compiling data on a demographic with common interests and then predicting their future actions based upon past actions of others within the same group, could be harmful to minority groups already stigmatised.

Almost everyone I know belongs to a stigmatised section of society, be it they are poor, disabled, LGBT, BAME, etc., and none of them wish to be judged by the interests of others from their group. Data stereotypes us based on the demographic the algorithm assigns to us. Though, in many cases the algorithm gets it right, it can hurt to see your interests placed in front of you as a stereotyped version of what the algorithm dictates your interests to be. In the United States, Senator Alexandria Ocasio-Cortez spoke of facial recognition systems deployed by criminal justice agencies to locate criminals and immigrants perceived as illegal. Her findings illustrated the inability of the algorithm to distinguish between non-white faces. Most employees of data companies are white male and heterosexual. It is not wild to assume that that has an impact on the consensus formed by those working for the industry. As data companies do not have a diverse employ, how are their conclusions applicable to diverse populations? The assumption by those sharing common consensus isn't necessarily applicable to those excluded from the mainstream (who are vastly under-represented) and in the case of data, this can mean being left out of systems entirely.

Google relies on the power of suggestion. We subscribe to click bait as it releases serotonin in our brains. Our biochemistry is being used against us like a drug and the pharmacist is getting ever richer at our expense.

There is legislation on alcohol, drugs, gambling, etc., but money-making click bait websites, causing the same endorphin releases and hooking us, just as gambling does, remain free to entrap us for hours on end, as we desperately try to get our fix of feel good hormones.

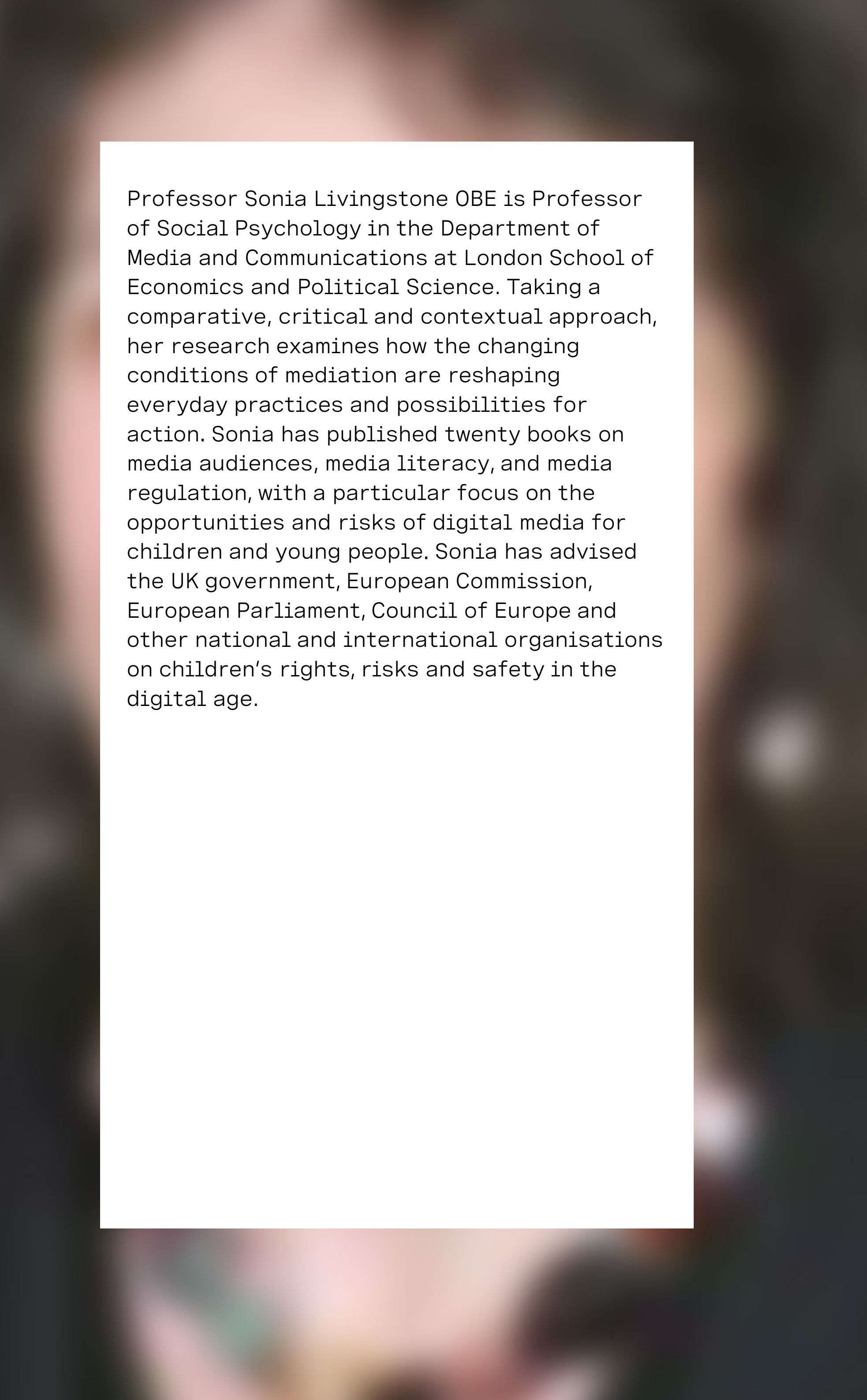
Companies are playing with our senses: making us feel good, then pushing us to spend more and more time on websites; giving more and more data, absolutely not to our benefit but lining the pockets of big data, meanwhile taking in adverts and considering a new pair of shoes.

They take our data and while they extract it, they suggest we spend some money. They are doubly quids in whereas we are doubly broke. Robbed first of our privacy and then of our funds. Data is capital and they are stealing it.

Keeping us on such a narrow track of interests (or rather the algorithms' perception of our interests) will create ghettoised online communities. There is already an enormous problem amongst young men terming themselves as 'incels'. Surely, there must be a burden of responsibility not just to show people like-minded discussions, but things outside of their immediate interests.

Our news feeds are targeted, based on interests, this means we only see some, not all news. We feel informed, but are denied from growing by data's profit made by hemming us in. It's tried and tested: if we like it, we click; profit ensues. We remain in echo chambers. Vulnerable people remain ghettoised by the algorithm. The algorithm makes us feel as though our opinion is the dominant one, everyone agrees with us, lulling us into a false sense of security. This leaves us unprepared for encountering those with whom we disagree. We obtain most, if not all of our information from the digital landscape, yet there is less legislation on digital companies and how they obtain information, than on conventional media. They must be held accountable. Deregulation and laissez faire policies mean ethics are a thing of fantasy: they are down to the individual interpretation of the companies.

Our data is being pedalled away by conmen and that is not ok.



Professor Sonia Livingstone OBE is Professor of Social Psychology in the Department of Media and Communications at London School of Economics and Political Science. Taking a comparative, critical and contextual approach, her research examines how the changing conditions of mediation are reshaping everyday practices and possibilities for action. Sonia has published twenty books on media audiences, media literacy, and media regulation, with a particular focus on the opportunities and risks of digital media for children and young people. Sonia has advised the UK government, European Commission, European Parliament, Council of Europe and other national and international organisations on children’s rights, risks and safety in the digital age.

Professor Sonia Livingstone OBE

"It's None of Their Business!" Children's Understanding of Privacy in the Platform Society

Facebook's advertising campaign, launched in August 2019 to recover public trust[1] following the Cambridge Analytica scandal,[2] announced:

"We all have our own privacy settings. So, when it comes to your privacy on Facebook, we think you should have the same controls."

It pictured a screenshot of privacy options (public, friends, close friends, only me) with the last option ticked. The implication is that, now, Facebook gives the public what it wants and deserves. But choosing 'only me' makes no sense in a networked world: who wants privacy at the cost of social isolation? Anyway, 'only me' does not solve the Cambridge Analytica problem, where people's personal data were used for commercial and political purposes without their meaningful consent. For whatever you tick, none of your actions are private from Facebook itself.

This phrasing of a Facebook advert illustrates, even perpetuates, a wider confusion in society between interpersonal privacy and what is being called data privacy.[3] Parents, teachers, government and businesses tend to talk to children as if privacy only means privacy from other people. When children are accused of lacking a sense of privacy by sharing their personal information with all and sundry, when parents worry about cyberbullying or grooming,[4] even when the media panic about accidental data leaks from the 'internet of toys' or smart home devices, the focus is children's interpersonal privacy and its safety implications. Policy responses centre, respectively, on better e-safety education, parental awareness and responsibility, and the regulation of product security. These are all important and urgent.

But adults say little to children about how to protect their privacy in relation to institutions (such as their school, doctor, or police) or businesses (most of which now collect personal data online in one way or another). Yet much of what a child does online – their searches, posts, likes or views – is immediately shared within a lucrative global data ecology. So if they are an Instagram or WhatsApp user, the child's data will be shared with dozens of Facebook's partners, since user profiling is the currency for real-time advertising auctions[5] that target users.[6] Attending to one's privacy settings will not impact on data privacy, where there is no real 'only me' option.

Privacy from whom?

Privacy is not a singular property that an individual 'has' or controls. It must be understood in context, depending on whom one wants privacy from. Historically, interpersonal contexts have been the most important for children. But under today's conditions of intense datafication, privacy contexts include not only interpersonal but also institutional and commercial contexts. The un-met challenge to children's privacy stems from the widespread and carefully planned collection and use of children's personal data, with consequences now and into the future. So now one must ask critical questions about children's privacy from both (usually trusted) institutions and commercial enterprises of diverse kinds (many of the third-party users are unknown by and thus practically inaccessible to users). Our surveillance society has been remarkably slow to start worrying about organisational uses and abuses of people's data, including children's.[7]

Even in the interpersonal sphere, privacy is always relational and contextual.[8] It is shaped by a host of cultural norms and expectations, often locally negotiated. If we don't attend to the context, as experienced by those involved, we won't understand what privacy means to people. For instance, a child may seek privacy in the (public) street if there are too many people at home. A few years ago, a teenager told me she felt private on Twitter (where tweets are formally 'public') but not on Facebook (where her privacy settings were high), because her many 'friends' only used the latter.[9]

As we argued in our recent 'Children's Data and Privacy Online' project,[10] it is vital not to confuse interpersonal with institutional and commercial contexts for privacy, for these contexts differ hugely in who or what one might seek privacy from. And these contexts are changing in complex ways. The privacy to walk down a street unobserved is now undermined by the mass introduction of surveillance cameras, though a child seeking escape from nosy siblings may not realise this. Whether your friends see what you do on Twitter or Facebook is unrelated to the data collected from you by the platforms, though neither company explains that clearly to their users.

This isn't children's confusion but ours. As a society, we conceptualise privacy first and foremost in interpersonal terms.[11] Our visceral response to privacy intrusions derives from a perceived affront to our personal agency and dignity in relation to others that we know or can imagine. People with reason to distrust the state extend this visceral grasp of privacy to institutional contexts, demanding the fairness and accountability from the state that they expect in interpersonal contacts. But most people in modern democratic countries trust the authorities (government, police, health, school, transport, etc.) with their personal information and anticipate no real institutional risk to their privacy. This is because, until recently, our interactions with businesses, also, were built on interpersonal trust (you could talk to the shopkeeper, visit your bank manager, see for yourself what the market traders did). Hence the recent dramatic drop in public trust,[12] and explosion of policy concern, now that global and proprietary digital platforms underpin both our interpersonal relations (where we expect to exercise agency), and our relations with institutions and business (where we are obliged to place our trust).

So, when adults talk to children about privacy, they assume an interpersonal context. For instance, to manage their online privacy, children are advised to choose who can see particular posts, and to delete messages that they regret or that might upset others. These are tactics for interpersonal privacy only, and they are ineffective for managing their privacy in institutional and commercial contexts. From Instagram or Snapchat or Amazon (and, probably, from their school or health provider) there is no realistic option to choose, to consent, or to delete.[13]

Children's understanding of their data privacy

The assumption of interpersonal privacy is reflected in children's understanding of the digital ecology. When we held participatory workshops with 11- to 16-year-olds around the UK,[14] we saw how children tended to (over)extend what they know of interpersonal relations to the operation of platforms. For example, they might talk trustingly of Instagram because so-and-so's father works in technology, and he would surely play fair. They assume ethical reciprocity: if they would never track someone without their knowledge or keep images against someone's will, why would a company? Or they assume that the tactics that keep their activities hidden from their parents or enemies (pseudonyms, ghost mode, incognito search, clearing one's history) also keep their data private from companies.

Inevitably, children's experience of the operation, regulation and norms of institutions and businesses is relatively limited, especially when they are young. Children's tendency to trust these organisations is also down to us. Who does not teach their child to trust their school or doctor or even the shopkeepers and other commercial services with which they have early dealings? Is the solution to privacy in a datafied world really to teach children to distrust? And who does teach children, including in school, about business practices, including the global nature and complex proprietary practices of the digital ecology?[15] We found few children who know what Oracle or Experian do with their personal data or how this might shape their future.[16] Should we be teaching even primary school children about platform business models? Would it enhance their agency if we did?

In our workshops, when we encouraged children to think not only about e-safety or how their parents shared embarrassing photos, but also about how their data are processed by their school, doctor, search engine, social media platforms and more, the conversation turned. Their confident expressions of agency and expertise would falter, and they would say, outraged: it's creepy, platforms shouldn't be poking around in the online contacts, I want to control who they share my data with and, most tellingly, it's none of their business![17] If only.

Shifting the burden of privacy protection from user to service provider

Of course, we need earlier and better digital education.[18] But the challenge of protecting privacy in a digital world goes beyond expecting children to understand and manage their personal data. Increasingly, the challenge is one of redesigning the conditions under which their data are collected, inferred, profiled and used by others. These conditions are, currently, systematically opaque to users. How can we expect children to be responsible for their data privacy when their parents, teachers or even policy experts don't understand it? Even if transparency were dramatically increased, what use would it be if not linked to granular, meaningful and easily-implemented choices about what to share, with whom, and for what?

When a service's Terms and Conditions state that users' data will be shared with hundreds of data brokers and other third parties, yet no realistic alternatives to use of the service are provided, we must conclude that the burden of privacy protection has shifted from the user to the service provider. Others in this volume have proposed legislative, regulatory and business solutions, and doubtless these will be hotly debated in what Forbes' Magazine has announced as "the year of digital human rights."[19]

It is a particular challenge for child rights that, in a datafied world, individuals tend to be addressed algorithmically in the aggregate (as students, patients, customers, the public) rather than according to their differential needs and rights. Even when digital services are 'personalised,' this tends to serve commercial or bureaucratic logics rather than those determined by citizens and users. It may not even be in the provider's interest to distinguish its treatment of adults' and children's data, impeding any chance of realising children's best interests.[20]

Children cannot learn to act as agents and make wise choices, nor to have their voices heard as is their right, when adult society systematically talks to them about their data and privacy online in purely interpersonal terms. Society cannot expect to protect children's right to privacy[21] if it confuses interpersonal and data privacy and fails to critically examine the conditions for each and the relations between them. We must stop advising children and parents that they can and should control the flow of their data in circumstances when they cannot, or when the result would be exclusion. We should call out businesses which claim that they respect people's privacy when they do not.[22]

We have created a situation in which children learn that they don't matter, that they have no agency, that their competence is misguided. In our workshops, children told us of their irrelevance – why would companies care what they did or thought? They referred to a dystopian Black Mirror world in which the machine has taken over. This sense of inevitability, in turn, reduces the pressure on service providers to develop user tools which provide children with meaningful choices about how their data are used. It is time to demand that institutions and businesses redesign their digital offer in ways that serve children's best interests. And for society to hold them to account.

[1] Trust in tech is wavering and companies must act, Edelman, 8 April 2019

[2] Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 17 March 2019

[3] Hintz, A., Dencik, L., Wahl-Jorgensen, Digital citizenship in a datafied society, 2019

[4] These risks of online harm matter, of course but are not my primary concern here. For evidence of the interpersonal risks, see Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group, 2017

[5] In-house mediation with server-to-server bidding, Facebook for Developers

[6] Facebook shared user data with 60+ companies, Investopedia, 4 June 2018. Facebook may also monetise non-users' data, via the construction of 'shadow profiles' - see Shadow profiles: Facebook has information you didn't hand over, Cnet, 11 April 2018

[7] Zuboff, S. Surveillance Capitalism, 2019

[8] Nissenbaum, H. Privacy as contextual integrity, Washing Law Review, 2004

[9] Livingstone, S., Sefton-Green, The class: living and learning in the digital age, 2016

[10] The project is funded by the Information Commissioner's Office, Children's data and privacy online: Growing up in a digital age

[11] Laufer, R. S., Wolfe, M. Privacy as a concept and a social issue: a multidimensional developmental theory, Journal of Social Issues, 1977

[12] 2019 Edelman trust barometer: global report, Edelman, 2019

[13] The UK's proposed Age-Appropriate Design Code (discussed elsewhere in this volume) should provide children with greater privacy in these contexts, as might a sterner application of the GDPR than yet witnessed, and the new California Privacy Act.

[14] Livingstone, S., Stoilova, M., Nandagiri, R. Children's data and privacy online: Growing up in a digital age, London: London School of Economics and Political Science, 2019

[15] Deceived by design, Forbrukerradet, 27 June 2018

[16] Christl, W., Corporate surveillance in everyday life, Cracked Labs, June 2017

[17] Livingstone, S., Stoilova, M., Nandagiri, R. Children's data and privacy online: Growing up in a digital age. Research findings. London: LSE, 2019

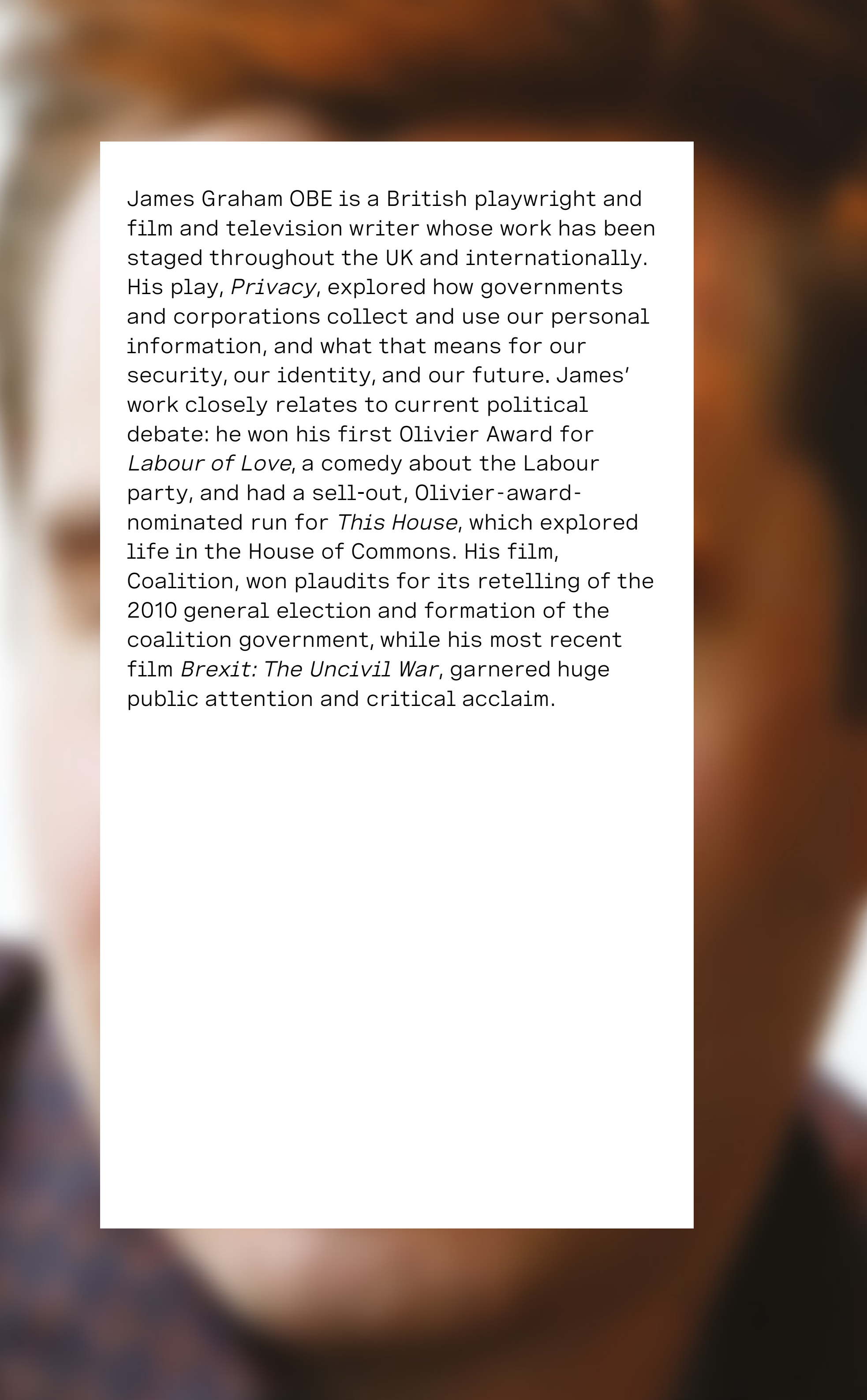
[18] Livingstone, S. Media literacy - everyone's favourite solution to the problems of regulation, 2018

[19] Why 2020 will be the year of digital human rights, Forbes, 26 December 2019

[20] UN Convention on the Rights of the Child, 20 November 1989

[21] Article 16, UN Convention on the Rights of the Child, 20 November 1989

[22] Facebook claims its built privacy into its products 'just like Apple.' The i newsletter, 8 Jan 2020



James Graham OBE is a British playwright and film and television writer whose work has been staged throughout the UK and internationally. His play, *Privacy*, explored how governments and corporations collect and use our personal information, and what that means for our security, our identity, and our future. James' work closely relates to current political debate: he won his first Olivier Award for *Labour of Love*, a comedy about the Labour party, and had a sell-out, Olivier-award-nominated run for *This House*, which explored life in the House of Commons. His film, Coalition, won plaudits for its retelling of the 2010 general election and formation of the coalition government, while his most recent film *Brexit: The Uncivil War*, garnered huge public attention and critical acclaim.

James Graham OBE

Past Norms, Future Dangers and Acceptable Compromises: What Does Freedom, Security and Privacy Mean for the Future of Young People Online?

In a debate that can range from pessimism to tin-hatted paranoia, I actually begin from a place of optimism when it comes to young people and their awareness and articulacy surrounding data and internet privacy.

Having spent time fretting about, talking to and attempting to represent on stage and screen people's views and experiences of how modern technology impacts upon their privacy, I'm convinced that a lot of younger people are savvier and more attune to the dangers and compromises that come with new communication platforms than many older generations. And that, with their advocacy for privacy rights and mental health protections in particular, they will probably save us, rather than us saving them!

That doesn't mean this awareness is universal, or all encompassing. Or that the problem will solve itself. Only that many net natives have at the very least an emotional awareness of the negatives of social media, for example, and are capable of making personal choices to mitigate their effect.

What they might understandably lack, however, is a historic, political or cultural context for how quickly things are changing, what a Wild West period we're in for during this sea change in communication, and how it might be improved or controlled.

In this, I think our job is to educate and empower them through data literacy as to past norms, future dangers, and what they should never consider as acceptable compromises from private institutions or the state.

How can we get people to care about their privacy?

I wrote a play called *Privacy* that premiered at the Donmar Warehouse in London in 2014 before moving to New York in 2016, starring Daniel Radcliffe. It was an interactive show where an audience could engage on their phones during the performance, thereby encouraging them to interrogate what data and information they give away about themselves without thinking, on smart phones, customer loyalty cards, Fitbit devices and more…

The overwhelming reaction in discussion with people, collaborators, interviewees, friends, family and audience members in advance of the show on the topic was always the same. "I don't really care", or "I'm fine with it" when it came to the exchange of their private data for something convenient, like a taxi showing up at your workplace or a package to your door. Cookies, third party access, government surveillance… "I've got nothing to hide".

Few believed that they were important enough or interesting enough to either warrant surveillance by an institution (surveillance in most people's minds being a Spy-type person, rather than algorithms or software) or be hacked by an outside party; or that there was even anything compromising about what they shared online.

The most effective way to get people to question this default response and to care more about their privacy was more often about addressing the emotional or human impacts of unrestricted data distribution, rather than political questions about the contract between citizen and state. How is this damaging my relationships, my opportunities, my sense of self?

For example, four years before the Cambridge Analytica stories broke, we worked with the designers of that same behavioural prediction algorithm in our play, using their software for the 'game' they built for our audiences. At the time, 'Apply Magic Sauce' was an interactive way to demonstrate that what we Like on Facebook can impact the profile the platform has on us; which it sells to third party advertisers (that range from shoe manufacturers to political parties). The software demonstrated with incredible effectiveness that it could identify aspects of your character, from religion to political views to sexuality, to an alarming degree. In some cases, it reached 96% accuracy rate, regardless of whether the content you Liked related to this category or not. Indeed, with over 100 Likes available from you, it claimed to know you better than your friends. Over 300, it began to know you better than you knew yourself...

The implication for personal privacy on our audience was stark. We asked them to imagine a 14-year-old child who may be, or grow up to be, gay. It isn't just a breach of accepted privacy norms that Facebook knows you might be gay without you deciding to tell it. Worse, it isn't even that Facebook might know that you're gay before you've told anyone else, from family to friends. It's that now, Facebook may know you're gay before you know that you're gay. That's the new threshold of privacy violation that seemed to effectively shake audience members from their complacency. No, that doesn't mean a Human Being in Silicon Valley is watching and judging you, but it does affect the content, contacts, filters and frame through which you see the world, and the world sees you.

We also discovered a basic lack of awareness, young and old, of the structures that built up the digital world. What actually happens when you share an intimate photo of yourself via a digital messaging app for example? In most people's minds, they're sending that photo from one device to another, and therefore it is, to all intents and purposes, 'private'. From A to B, via no concerning C. But of course, as we know, this isn't the case. That intimate photo of yourself passes through a physical network of pipes that pass different nations and jurisdictions to find itself sat on a physical server (which is owned by a private company with shareholders and investors to make profit and whose ownership can change, rather than exist for social good), where it will sit for an undetermined amount of time. A small academic point, perhaps, but it was an impactful thought experiment for our audience to accept that their 'penis' wasn't just in the possession of an intimate contact, but now the property of a corporation.

The challenges for young people

I believe that awareness around the dangers young people face – from contact by predatory individuals to the potential for revenge porn to wreck a person's life, or publishing something controversial on a social media platform that can damage future college admissions or job prospects – is far from universal, but is becoming more prevalent in the national consciousness.

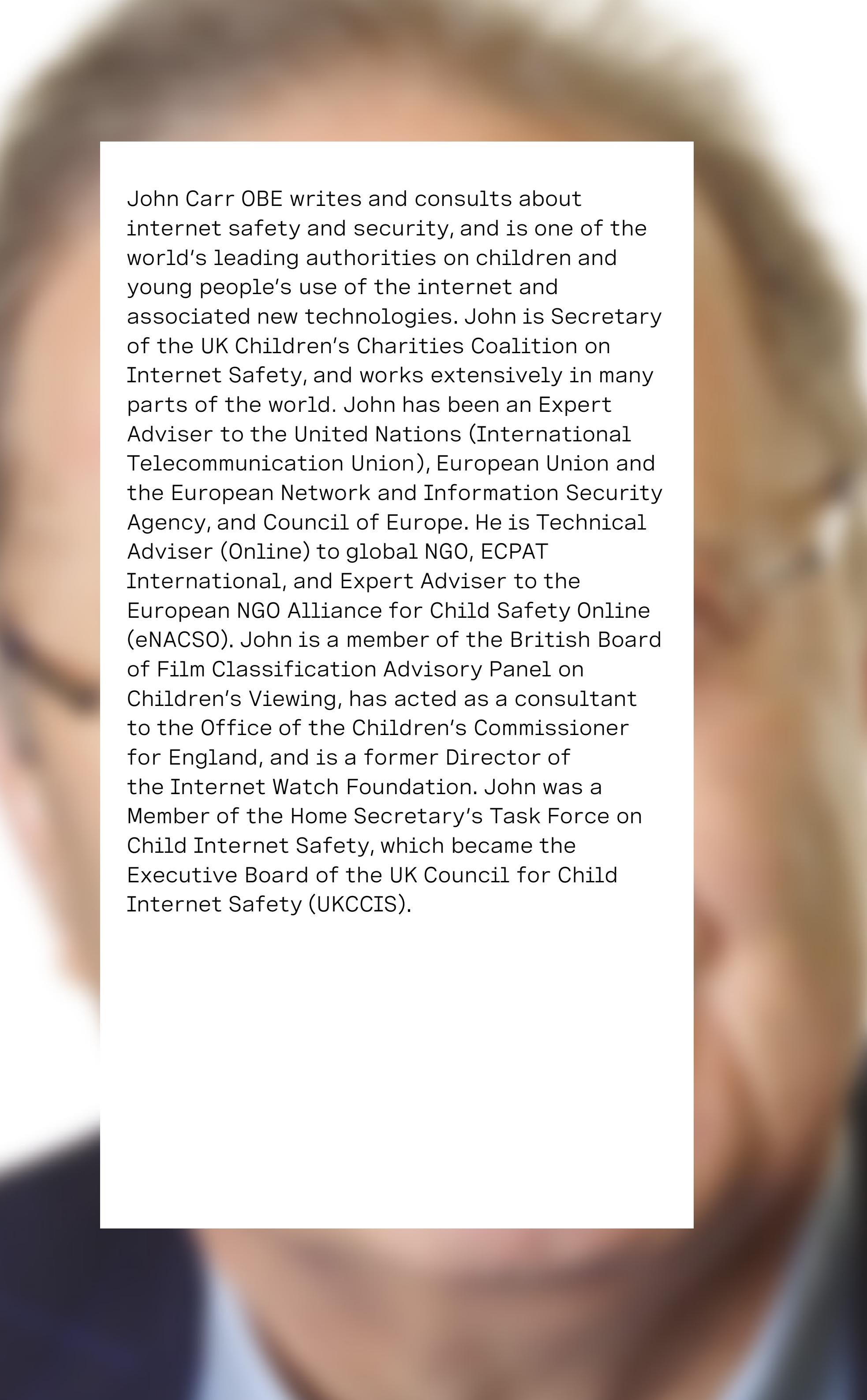
The areas here I think we have not yet found an effective language for cover the more psychological and emotional compromises being made by the unrestricted free for all on data.

What will happen to a generation who does not feel able, capable or comfortable making mistakes? The net has indirectly led to a culture whereby every element of our identity, every expression of thought or sharing of an opinion is cultivated, crafted and edited for fear of Getting It Wrong, and having permanent consequences. This includes social communication: a generation of young people speak much less on the phone, because on the phone you are talking live, you are vulnerable, you may trip up, say the wrong thing, or accidentally say what you mean. But it is in these vulnerable moments that we show who we are, and learn about who we are. Anecdotally, therefore, we hear of college and university cultures now where students prefer to receive written feedback first, so they may curate the right response, rather than receiving feedback or criticism face to face. We hear of an anxiety culture when it comes to social or intimate reactions from a generation under intense pressure to craft the perfect image of themselves online, far removed from the natural human flaws and frailties we used to be able to embrace and enjoy because they left no lasting footprint.

We hear of a generation that suffers from an empathy deficit (though this is far from unique to young people), as defined by MIT Professor Sherry Turkle with whom we developed the show *Privacy*. Empathy comes from looking into the eyes of the person you are having an interaction with and bearing witness to the impact of what you say. And while the web has meant that marginalised groups might have desperately needed access to like-minded people far beyond the confines of their street or town (for example the LGBTQ+ community, or people with disabilities), an online model that is built on giving you what you want, rather than what you might need to see, means young people's access to different views or experiences outside of those they grew up with may also be narrowing, based on the data profile that has been built up of themselves. Might that explain the diminishing tolerance for those with different political views when it comes to 'campus culture', and the polarising of entire populations around political extremes? How can we create an awareness and thereby encourage a culture among young people to shake free from this?

When the digital spaces that have replaced physical ones don't naturally promote empathy, tolerance, a safe space for vulnerabilities or forgiveness, but do increase levels of anxiety, social pressure, unhappiness and impossible standards... when an online data model narrows, filters and restricts the frame through which users view the world rather than opening it up, encouraging diversity, and creating surprises... these are the psychological, emotional and even philosophical questions I would like to see feature in the debate and in the minds of young people as they go out into the digital world.

A world of genuine privacy for children and young people online would probably have the same feeling of security the offline world does (or should), where accepted norms around what we share with our employer, our neighbours, our political representatives, and our friends is something that has clear customs and accepted boundaries. It would have a fluidity to it, that means we can choose to open up and share more at a pace and in a manner that is controlled by us, and our growth into adulthood. It would wipe away minor youthful transgressions and silly statements as we hit 18 by law. And our data would be ours to offer up to the institutions, companies and people around us, but not merely as currency to spend within a transactional exchange to buy a book, hail a cab or order food. It would be seen as an opportunity to engage, connect, invite and learn: because it would be ours to share.



John Carr OBE writes and consults about internet safety and security, and is one of the world's leading authorities on children and young people's use of the internet and associated new technologies. John is Secretary of the UK Children's Charities Coalition on Internet Safety, and works extensively in many parts of the world. John has been an Expert Adviser to the United Nations (International Telecommunication Union), European Union and the European Network and Information Security Agency, and Council of Europe. He is Technical Adviser (Online) to global NGO, ECPAT International, and Expert Adviser to the European NGO Alliance for Child Safety Online (eNACSO). John is a member of the British Board of Film Classification Advisory Panel on Children's Viewing, has acted as a consultant to the Office of the Children's Commissioner for England, and is a former Director of the Internet Watch Foundation. John was a Member of the Home Secretary's Task Force on Child Internet Safety, which became the Executive Board of the UK Council for Child Internet Safety (UKCCIS).

John Carr OBE

Privacy Lawyers Need to Up Their Game: An Internet that is Safer and Better for Children is Going to be Safer and Better for Everyone

"Protecting Child Privacy" was the title of a day long symposium I recently attended (November 2019) at the Institute for Privacy Protection, part of Seton Hall Law School in the USA. The organisers had attracted a star-studded cast of American speakers and there were two speakers from Europe: myself and Max Schrems[1]. Now if there is anyone who can claim rock star status in the world of online privacy it is probably Schrems. The fact that he is young, and looks and dresses like a rock star only adds lustre.

Here is a key excerpt from his brilliant presentation:

> *In preparing my comments for today I talked to lots of lawyers from the privacy world. However, I found it very difficult to find any who specialised or claimed expert knowledge in relation to children and privacy.*

OK, Schrems may have a limited circle of associates but what he said struck a chord with me. It exactly mirrored my own experience.

There is a substantial and growing body of lawyers who specialise in privacy. The GDPR has pretty much guaranteed and created a "privacy industry". But it's still very early days. I can still only think of a handful of lawyers or other experts who have developed and sustained a major interest in children's privacy rights, or have a deep understanding of the real-world consequences for children of this or that decision about how to draft or interpret a law or regulation with a privacy dimension. Sadly, few of these lawyers are working for the European Commission. Neither are they working for many of the major Data Protection Authorities around Europe nor, come to that, the European Data Protection Board. The same was true for its predecessor, the Article 29 Working Party.[2]

In its entire 19-year life, Article 29 only produced one major report on children.[3] It was published in 2008 and it concerned the protection of children's personal data in schools. An important issue to be sure, but...

Article 29 and its associates doubtless became distracted in the run up to the publication of the draft text for the GDPR. In December 2011, Statewatch leaked a late draft.[4] In it, the Commission had proposed that for persons under the age of 18, where consent was to be the basis for processing personal data, it would be necessary for the service provider to obtain parental consent. This was widely interpreted in the media as meaning Facebook and other platforms would be closed to all persons under the age of 18, unless their parents agreed to let them use it. The balloon went up. The idea was dropped. A month or so later when the official text finally appeared, 18 had been replaced by 13. It was to apply in every EU Member State. No variation. Why was 18 ever considered to be an appropriate minimum? We can guess, although no real explanation was offered. But why did the Commission officials then shift from 18 to 13 so rapidly? It seems unlikely the shift was based on any new research that had suddenly become available, and neither was it based on any consultations with experts in the field.

This time Commission officials did offer an explanation, but not a very good one. They simply said 13 was to be preferred because that was what the Americans were already doing, and it had therefore become a de facto standard. Other than that, no actual evidence was produced to show why 13 was a good pick. When it came to the final decision, the politicians threw it out. Without more, the mere fact the Americans were already doing it and that it had become a de facto standard did not convince the French, Germans and many other Governments that the whole of the EU should choose to go the same way. Conceivably, this cack-handed approach even encouraged European governments to actively look for an alternative. That is how we ended up with a hotch-potch of ages between 13 and 16, with 16 as the default age of consent. Again, no evidence was produced to justify or explain the decision, and no obvious thought had been given to the possible consequences of having different age standards for children in different countries connecting with each other using the same Apps, at the same time.

Consent as the basis of processing data is the most easily understood (if often poorly implemented) basis for engaging with an online service and, in respect of children, it offers a route which at least encourages the possibility of parents being involved with their children's online activity.

Yet privacy lawyers and those involved in writing the GDPR constantly stressed how, when considering which Article 6[5] grounds to use as the basis of processing personal data, it would generally be "better" for companies not to rely on consent but, instead, to use one of the other grounds mentioned. In that light we have to ask: could or should these same lawyers have anticipated how these other grounds might, effectively, cut parents out of the loop? By allowing companies to use, for example "legitimate interest" or contracts to apply in relation to children's involvement with their products and services, the issue of parental consent is made redundant and with it, at least some possibility of parental engagement. Facebook took the opportunity in effect to create a whole new class of membership or type of user. It side-stepped parents altogether.

Sticking with the shortcomings of the GDPR, by which I mean sticking with the child-unaware shortcomings of those who drafted it, let us not forget the scourge of child sexual abuse materials (CSAM) that continue to circulate on the internet, and the gigantic harm the mere fact of circulation does to the victims depicted.

Under existing rules, companies that sell domain names are meant to collect accurate information about the identity and contact details of the person or entity buying the domain. Historically, these data were meant to be made immediately available to everyone via a publicly accessible database called WHOIS. Yet in 2018, the UK's Internet Watch Foundation (IWF) identified over 1,000 websites that seemed to have been established solely in order to distribute child sexual abuse material.[6] In the entire passage of the GDPR, in the draft text, in the Parliament and in Committee, WHOIS was never even mentioned. Not once. On the contrary what came out the other end meant law enforcement and other interested agencies that might want to track down whoever is publishing CSAM via a website now have to jump through many time consuming and expensive hoops to see who the supposed owners are. This could and should have been avoided. The law must be changed as soon as possible. It provides another example of how the absence of knowledgeable input during the drafting of the GDPR has led to poor outcomes for children.

Finally, thanks to some prolonged and intense lobbying, the ePrivacy Regulation has been temporarily shelved. But if it had gone through in its original form, it would have become illegal for companies providing messaging services to continue using tools such as photoDNA to try to detect the presence of already known CSAM.[7] What were the draftspersons thinking of when they put that together? Not children.

For all of the above reasons, the work of the 5Rights Foundation is hugely important, both in respect of helping develop the UK's Age Appropriate Design Code and on the General Comment on children's rights in the digital environment with the Committee on the Rights of the Child.

Yes, there are challenges associated with squaring the privacy circle for children without trespassing on adults' rights but, up until now, too many people, too many lawyers who ought to have known better, have put children's privacy in a box marked "too difficult" and ignored it while they addressed other issues. It is vital that we break out of this circle of uncertainty by developing a corps of lawyers, activists and institutions who understand the importance of privacy for children.

[1] Max Schrems, Wikipedia

[2] Article 29 Working Party, European Commission

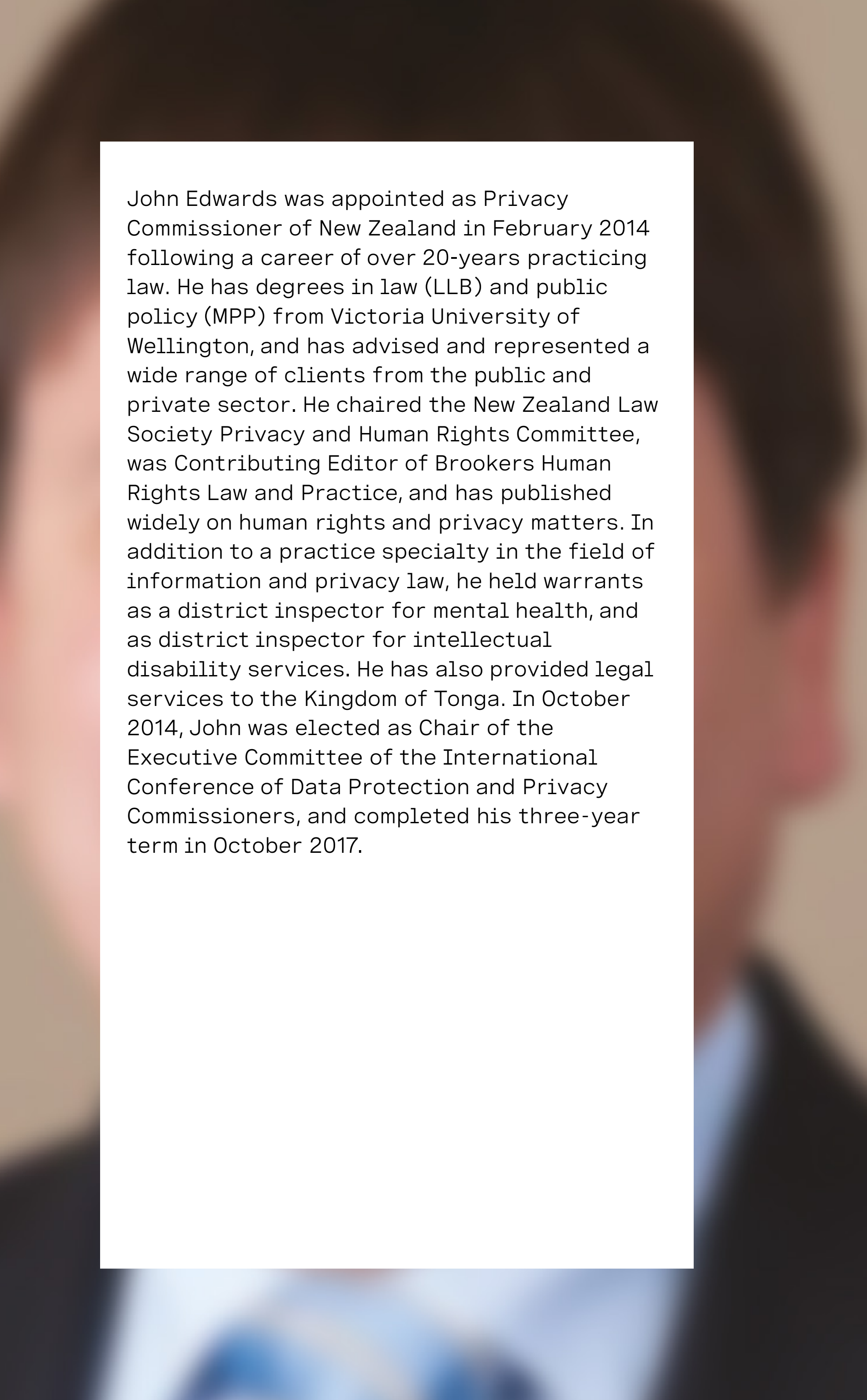
[3] Working document 1/2008 on the protection of children’s personal data (General guidelines and the special case of schools), Article 29 Data Protection Working Party, 18 February 2008

[4] Macenaite, M., Kosta, E. Consent for processing children’s personal data in the EU: following in US footsteps? Information and Communications Technology Law, 10 May 2017

[5] Article 6, General Data Protection Regulation, 2016/679

[6] Final version of the letter to the NTIA, Desiderata, 20 July 2018

[7] Another update on the e-Privacy Regulation, Desiderata, 20 February 2019



John Edwards was appointed as Privacy Commissioner of New Zealand in February 2014 following a career of over 20-years practicing law. He has degrees in law (LLB) and public policy (MPP) from Victoria University of Wellington, and has advised and represented a wide range of clients from the public and private sector. He chaired the New Zealand Law Society Privacy and Human Rights Committee, was Contributing Editor of Brookers Human Rights Law and Practice, and has published widely on human rights and privacy matters. In addition to a practice specialty in the field of information and privacy law, he held warrants as a district inspector for mental health, and as district inspector for intellectual disability services. He has also provided legal services to the Kingdom of Tonga. In October 2014, John was elected as Chair of the Executive Committee of the International Conference of Data Protection and Privacy Commissioners, and completed his three-year term in October 2017.

John Edwards

Children and Privacy Online: It's Time to Change the Dynamic – More Responsibility on the Platforms, More Autonomy for the Kids

Not so long ago, the best advice available for keeping children safe online, was to locate the family computer in a common area. Thus, the theory went, if children strayed into an unsafe corner of the internet, were exchanging messages with an unknown correspondent, or were accessing materials inappropriate for their age and maturity, a wise and caring parent could intervene.

Such an approach now seems quaint. First for the obvious reason, that most online activity is now mobile, and can be carried from room to room, accessed at the bus stop, the playground, or under the bedclothes late at night.

But the naivete was there before the mode of access shifted to portable devices. The advice imposed a degree of transparency, but the burden of that transparency was borne by the end user, the child, and the presumptively vigilant and savvy parent. In other words, this represented an abdication of responsibility from content providers and online services targeting children, indifferent to whether children accessed their sites and hosted materials.

Parents should be the first line of defence for children and young people. This was recognised by the OECD Recommendation on the Protection of Children Online in 2012.

But even then, the limitations of parents' ability to effectively counsel and supervise children online was recognised as a significant limiting factor.

That limitation increases with every technological innovation and social media iteration. By the time parents are aware of Snapchat or TikTok, the young have moved on to the next thing.

The digital world has enormous potential to enhance and protect children's rights. But the sword cuts both ways. The very same characteristics that allow children to independently access information in their best interests and further their autonomy and self-development, allow a delivery mechanism for harmful and exploitative content, for the harvesting of data and for the indefinite retention of ill-judged, intemperate or simply regretted posts.

The age of user generated content is a particular challenge. Children, their parents and others in the community can take private moments, and upload them for permanent and infinitely reproduced consumption, editing, manipulating and recontextualising, by anyone in the world with an internet connection.

Children can be induced to innocently participate in online "challenges" on widely used platforms, that are in fact intended to harvest fodder for fetishists.[1] As recently as October 2019, the Guardian reported that Facebook can identify, and sell advertising targeted at "children interested in alcohol and gambling".[2]

New functions can be added to existing platforms with little testing or safeguards. Livestreaming, for example, while promoted by Facebook's Mark Zuckerberg as a way for a Dad to tune in remotely for an eight-year-old's birthday party, can just as easily be used to expose that same eight-year-old to the horror of a mass shooting, as happened in Christchurch, New Zealand in March 2019. In the aftermath of that atrocity, Facebook could not even answer the question of how many instances of child abuse, rape, suicide and murder its insufficiently tested application has facilitated since launch.[3] The magnitude of those shortcomings, including the rush to market the livestreaming product before it was adequately tested, was revealed. Six weeks after 51 people were shot to death in their place of worship, and their pain and anguish was pushed onto the tablets and phones of unsuspecting children and adults the world over, Facebook introduced measures which, had they been in place at the time, would have prevented the terrorist from broadcasting his attack.[4]

At least three of the rights in the 5Rights Framework speak directly to children's privacy. The need for children, and their parents, to have good, clear, timely and easily understood information about the consequences of interacting with their sites is fundamental to making the digital world safe for children and young people. The Right to Know, and the Right to Informed and Conscious Use have formed the basis of data protection and privacy laws around the world for at least 40 years. That today, it is necessary to make a special case for tech and content companies to comply with those principles in respect of children is a stark illustration of the failure of the regulatory model to date, and the success of the digital oligarchs in keeping ahead of politicians and regulators.

The third privacy right advocated by the 5Rights Framework that allows some mitigation of the accreted harms of data harvested under opaque, misleading or absent pretences is the Right to Remove.

We are seeing the first generation of children born in the social media era mature into adulthood. For many, their every developmental step will have been documented and shared online, often innocently by a parent who lacked the knowledge or foresight of the surveillance capitalist business models that were to come.

I have had to confront a case in which an adult traumatised by childhood experiences of abuse sought to regain control and restrict dissemination of nude images of her 13-year-old self, which had become part of an artist's portfolio and gallery collections.

But a child should not have to wait until adulthood to exercise some autonomy over the dissemination of private images. And nor should she be required to justify exercising that right by the kind of extreme example as the one my Office encountered.

The Right to Remove is a challenge to a number of foundational principles of the digital economy. It is a specific challenge to those which have emerged from a culture that regards the right to freedom of expression almost as supreme law. Freedom of expression has been invoked to such an extent that civil rights (!) organisations will seek to overturn laws which attempt to support victims of revenge porn: believing that one person's right to post an intimate image of another, in breach of confidence and trust, trumps the subject's right to that image.

It is probably for this reason that the Right to Remove is expressed in such modest terms by 5Rights as "the right to easily remove what you yourself have put up".

While worthy, and sufficiently moderate to win some acceptance among the US digital oligarchs, I would suggest it is an insufficiently ambitious attempt at reclaiming agency and autonomy. Why stop at simply being able to control material that has been uploaded or provided by the child?

Should a child not have a right to assert, even against a parent, that an amusing image of toilet training still accessible on the parent's Facebook page, might be fodder for the bullies tormenting them and ought to be taken down? That the video of their distress at not having received the Christmas present they were hoping for at eight is not an amusing memory to be shared with the world for a 12-year-old?

As far back as 2015, Kate Eichhorn in 'The End of Forgetting: Growing Up with Social Media' noted that British parents posted on average, nearly 200 photographs of their child online each year, and that the terms on which those images are hosted, packaged and analysed change unilaterally and arbitrarily. The New York Times recently reported that hundreds of thousands of images of children uploaded to Flickr in 2005 ended up in a facial recognition/AI training database.[5] That we only learn about these secondary and tertiary uses of information, 14 years after the fact demonstrates the impossibility of parents making sound judgements for their children in the face of an overwhelming information asymmetry. The Right to Remove can rebalance that asymmetry.

Children should have the presumptive, no-questions-asked right to delete content which they have submitted, or in which they appear; regardless of the relationship between them and the "owner" or poster of the image or information. Should that be an absolute right? Perhaps not, but it should be incumbent on an adult or commercial enterprise to justify why they have not acceded to a child's preference. The burden and the cost of making and defending such a judgement should be borne by the agency seeking to profit from the engagement and the content.

Knowing that their business model depends on the ongoing licence to maintain the content, and that they will incur the cost and administrative burden of removal requests, might well motivate digital industries to better address the rights to informed and conscious use, to know, and to digital literacy.

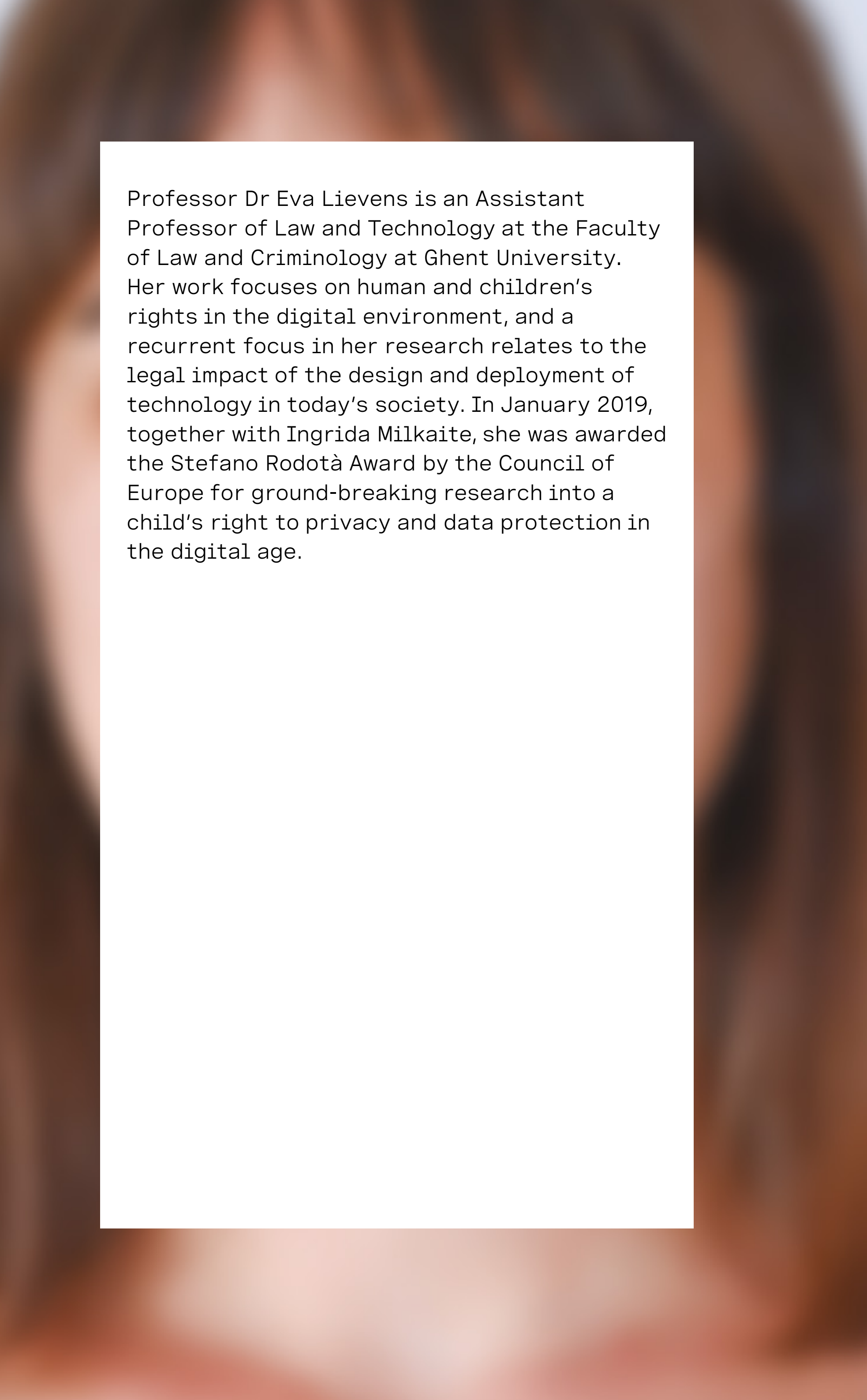
[1] 'Hello, my name is Ally' - how children are being exploited by YouTube predators, The Spinoff, 21 November 2016

[2] Children 'interested in' gambling and alcohol according to Facebook, The Guardian, 9 October 2019

[3] Facebook are 'morally bankrupt liars' says New Zealand's privacy commissioner, The Guardian, 8 April 2019

[4] Facebook changes livestream rules after New Zealand shooting, CNN, 15 May 2019

[5] How photos of your kids are powering surveillance technology, New York Times, 11 October 2019



Professor Dr Eva Lievens is an Assistant Professor of Law and Technology at the Faculty of Law and Criminology at Ghent University. Her work focuses on human and children’s rights in the digital environment, and a recurrent focus in her research relates to the legal impact of the design and deployment of technology in today’s society. In January 2019, together with Ingrida Milkaite, she was awarded the Stefano Rodotà Award by the Council of Europe for ground-breaking research into a child’s right to privacy and data protection in the digital age.

Professor Dr Eva Lievens

The Rights of the Child in the Digital Environment: From Empowerment to De-Responsibilisation

The digitalisation of our society has a substantial impact on the lives of children and on the rights that are specifically attributed to them by the United Nations Convention on the Rights of the Child (UNCRC), Article 24 of the EU Charter of Fundamental Rights, and many national constitutions. The 2018 Recommendation that was adopted by the Council of Europe's Committee on 'Guidelines to respect, protect and fulfil the rights of the child in the digital environment' acknowledges that the digital environment is "reshaping children's lives in many ways, resulting in opportunities for and risks to their well-being and enjoyment of human rights". There is no doubt that the digital environment has enormous potential for the empowerment of children, but I argue that, at the same time, an urgent need for de-responsibilisation of children (and parents) in light of certain digital practices is emerging.

The use of digital devices and services provides children with many opportunities to effectively realise a number of rights, such as the right to freedom of expression, the right to association and the right to engage in play. Greta Thunberg has three million followers on Twitter where she raises awareness regarding climate change and inspires young people all around the world. Ryan Kaji is a young boy with his own YouTube channel 'Ryan's world' with more than 22 million subscribers. Children and young people communicate, share and create content, often across borders, on social media and through mobile apps. Yet, the platforms that provide children with these fora to exercise their rights are deeply commercial and are built on business models that are data- and advertising-driven.

At this moment in time, it is hard to assess and to predict the impact that practices such as exploitative data collection, processing and profiling activities in commercial environments will have on children's lives in the long term. Aside from a potential substantial impact on the right to privacy and data protection, there might be direct and/or collateral effects on the right to development, freedom of thought, freedom of expression and association, as well as the right to protection from commercial exploitation. The Council of Europe's Committee of Ministers has warned in its 2019 'Declaration on the manipulative capabilities of algorithmic processes'[1] that "fine grained, sub-conscious and personalised levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions". The Committee also acknowledges that "these effects remain underexplored but cannot be underestimated". Similar questions are raised about the effects of practices by public actors, such as the deployment of facial recognition technology and other surveillance mechanisms, for instance in schools and other educational environments. The Swedish Data Protection Authority recently fined a municipality for using facial recognition technology to monitor the attendance of students in school because of non-compliance with the EU General Data Protection Regulation (GDPR).[2] But aside from violations of data protection obligations, growing up in constantly surveilled environments - in which their movements, behaviour and relationships are monitored - might also negatively affect children in the long term. The EU's Fundamental Rights Agency, for instance, has recognised that the deployment of facial recognition technologies might lead to a chilling effect on the right to freedom of expression and to freedom of assembly and association.[3]

At this moment in time, it is hard to show that the practices described above lead to actual harm on the well-being of children. This makes it hard to advocate for stricter regulation or prohibitions on the deployment of certain technologies. Regulation imposes restrictions on certain behaviours or actors and, hence, there should be a compelling reason to regulate. However, with respect to delicate issues, such as the well-being of children, the 'precautionary principle' should be borne in mind. Simply put, this concept, which finds its origins in environmental policy, embraces a 'better safe than sorry' approach. The precautionary principle compels society to act cautiously if there are certain – but not necessarily absolute – scientific indications of a potential danger and if not acting upon these indications could inflict harm. The Wingspread statement on the precautionary principle, adopted by academic experts at an environmental conference in 1998, stated that "[w]here an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically".[4]

Current legal frameworks that are relevant to the practices in question often prescribe 'empowerment measures' as a means of protection. Such measures include transparency towards data subjects (including children), and giving them rights to control the data that is collected and processed. Examples of rights that are included in the Council of Europe's Convention 108+ and in the EU's GDPR are the right to information, the right to access, the right to erasure, the right to object, and the right not to be subject to automated decision-making. Yet, as certain practices are so opaque and complex, and their effects difficult to grasp, 'being informed' or 'having rights' often does not amount to being protected. The responsibility for understanding how data is processed and assessing whether it is fair cannot be placed solely on children's shoulders, nor on those of their parents. On the contrary, fair processing of children's personal data requires legal restrictions on certain practices – keeping the precautionary principle in mind; enhanced responsibilities for data controllers – both public and private actors; and stronger enforcement by Data Protection Authorities. 'De-responsibilisation' of children and their parents inevitably leads to '(re)responsibilisation' of policymakers, data controllers and regulators. They should take the 'best interests of the child' (Article 3, UNCRC) as a primary consideration in how they make decisions about processing children's personal data. Children's Rights Impact Assessments that consider potential effects on the full range of children's rights should guide such decisions.[5] Investing in longitudinal, fundamental and empirical research into such effects is, in that respect, of primordial importance.

[1] Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, Adopted by the Committee of Ministers on 13 February 2019

[2] Facial recognition in school renders Sweden's first GDPR fine, European Data Protection Board News, 22 August 2019

[3] Facial recognition technology: fundamental rights considerations in the context of law enforcement, European Union Agency for Fundamental Rights, 2019

[4] Wingspread statement on the precautionary principle, Intergovernmental Forum on Chemical Safety, 26 January 1998

[5] Children's rights in impact assessments: A guide for integrating children's rights into impact assessments and taking action for children, UNICEF, December 2013

ON THE FUTURE OF CHILDHOOD

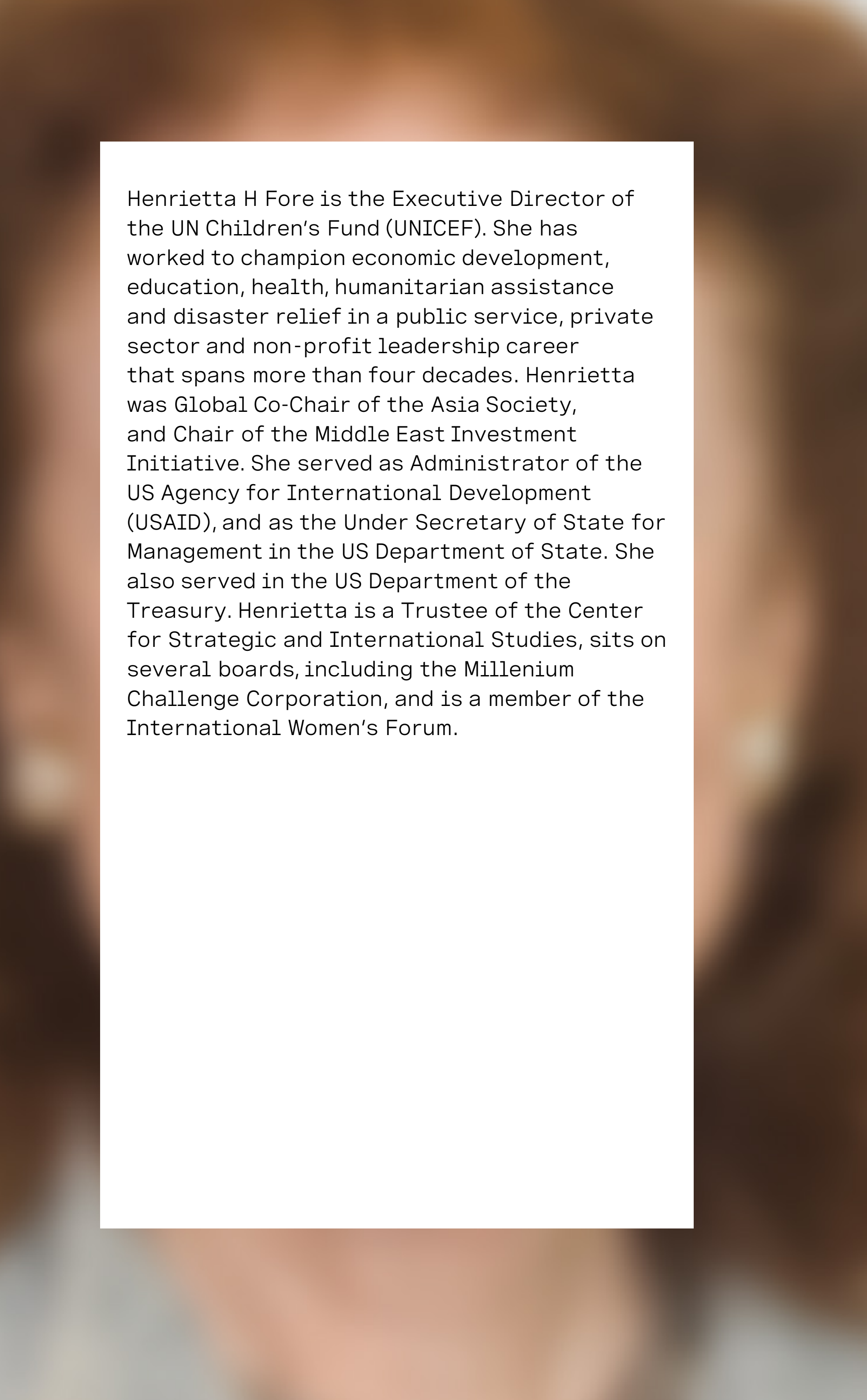
Data does not define me.

I think it is important that the views of young people like me are heard when rules and decisions are made which affect the way young people like me live our lives.

I imagine that the digital world in the 22nd century will be advanced, brilliant and safe for all children to use effectively and creatively.

There must be a law for this.

5Rights' Young Leaders



Henrietta H Fore is the Executive Director of the UN Children's Fund (UNICEF). She has worked to champion economic development, education, health, humanitarian assistance and disaster relief in a public service, private sector and non-profit leadership career that spans more than four decades. Henrietta was Global Co-Chair of the Asia Society, and Chair of the Middle East Investment Initiative. She served as Administrator of the US Agency for International Development (USAID), and as the Under Secretary of State for Management in the US Department of State. She also served in the US Department of the Treasury. Henrietta is a Trustee of the Center for Strategic and International Studies, sits on several boards, including the Millenium Challenge Corporation, and is a member of the International Women's Forum.

Henrietta H Fore

From Privacy to Power: Children's Rights in a Digital Age

Privacy is critical for children as they develop their individual personalities and identities; as they grow, play, learn and study; and as they speak their minds, and learn to express themselves freely.

Privacy is also a fundamental human right, for all people, including children. Now marking its 30th anniversary, the Convention on the Rights of the Child (UNCRC) recognizes that children have sovereignty over their personal information and must be protected from "unlawful interference with their correspondence."[1]

In other words: children have a right to control how information about them is collected, used and shared.

At the intersection of privacy and expression

Today, the space in which correspondence and self-expression play out is as much digital as physical; perhaps more so. Revolutions in information and communications technology make it easier and faster than ever before for children to transmit and receive information.

As children increasingly use these digital, online tools, they are leaving longer and wider trails of digital information about their interests, locations and preferences, even their appearance and daily routines; but also that of their friends and peers.

They post images, pictures, texts and memes that express different aspects of their personalities. They socialize and communicate with friends and peers; next door and around the world in chatgroups. Many use technologies to engage in civic and political discussions, to help them with schoolwork, or to look for a job.

In many cases, online information gives children access to facts and data on topics that may be perceived to be taboo in their societies; sexuality, reproduction, physical changes, and mental health, for example. This is particularly true for girls, who often have difficulty accessing information about their changing bodies and how to manage menstruation, for example.

How this information is accessed, used, stored or destroyed is obviously a fundamental concern. Children's right to privacy demands that they are able to access this information - and express themselves - in private, without interference from third parties, including governments and the companies who own the platforms that children frequent.

But just as "almost every act online is an act of expression"[2] it also generates indelible traces of information which can be seen by unintended parties.

What happens to children's data?

In an increasingly interconnected world, personal data has become a new commodity. Data generated through social media platforms and internet browsing is used to enable better and more personalised experiences, customize health and education information, improve welfare services, and track health risks and pandemics.

But it is also used to profile and track children for targeted marketing and advertising, including for products that are harmful or inappropriate for them. This is an enormously powerful and self-perpetuating tool that companies can use to extract more and more data from their users, including children, to generate more revenue.

This data has no age restriction. Children's data is collected, used, stored and sold in exactly the same way as adults' data. Even data created by parents, friends or schools, or data gathered through tracking and monitoring devices, can shape a child's data profile. In some cases, data may even have been gathered before birth and certainly before children are able to knowingly consent to its collection and use.[3]

What we can do

For parents, governments and the technology industry, this represents not just a concern, but a fundamental responsibility to develop proactive, preventative and protective measures, that transfer some control and power to children and young people over their data, while finding ways to keep them safe and protected.

For the most part, regulatory structures have not kept pace with this astonishing rise of digital data collection and usage. Therefore, we call on governments and the technology industry to work together to strengthen policies and regulatory frameworks that protect children's data across its entire life-cycle: from data creation and collection, through its use, storage and processing, to its destruction.

This includes the right to have personal data erased – the 'right to be forgotten' – which is especially important for children as they navigate their path through childhood, and forge digital identities along the way.

The European General Data Protection Regulation provides a useful model. It indicates that internet users, including children, should be given clear and transparent privacy notices that explain to children how their data will be collected and processed. It also goes one step further, saying that everyone, including children and young people, should have access to their personal data and the chance to fix any incorrect information.

This is especially important when privacy terms and conditions on social media platforms are often barely understood by highly educated adults, let alone children.[4] Children need to have real opt-in or opt-out opportunities in relation to how their data are used by the provider or other commercial entities, and terms and conditions need to be clear and understandable for children. As some children have argued themselves, this should extend to deleting historical social media profiles, for example.

As we call on governments and industry to take action, we also call on parents and guardians to take an active role in coaching their children to use online tools responsibly; to understand the risks, and to take steps to ensure that their data are protected.

Of course, while younger children may require greater parental involvement, those who are approaching adulthood may not require such stringent parental data protection oversight.[5] This flexible approach is consistent with the UNCRC's concept of the "evolving capacities" of children and young people to exercise rights on their own behalf.

Parents can also be good role models in their own use of digital platforms, and openly discuss with children the risks of using them. This can all be done while respecting children's individuality and right to express themselves, allowing the child "to develop a healthy sense of self, apart from his and her parents."[6]

As any parent knows, monitoring children's online behaviour is an almost impossible task. But having open, constructive and positive conversations about the safe and responsible use of digital platforms can make a critical difference.

By joining forces, governments, industry, parents and children themselves can build trustworthy products, services and governance structures that balance the interests of individuals, groups and industry,[7] and ensure that every child's right to privacy and protection when online is upheld.

The UNCRC, adopted in the same year in which the World Wide Web was invented, remains a powerful lens to examine and uphold universal values and principles; ones that are applicable today as much as they were over 30 years ago. As these values and principles are being translated into national and international regulations, guidance and standards, children stand to gain more freedom, more protection and more power over their own digital footprint.

[1] Article 16, UN Convention on the Rights of the Child, 20 November 1989

[2] Two sides of the same coin – the right to privacy and freedom of expression, Privacy International, 2 February 2018

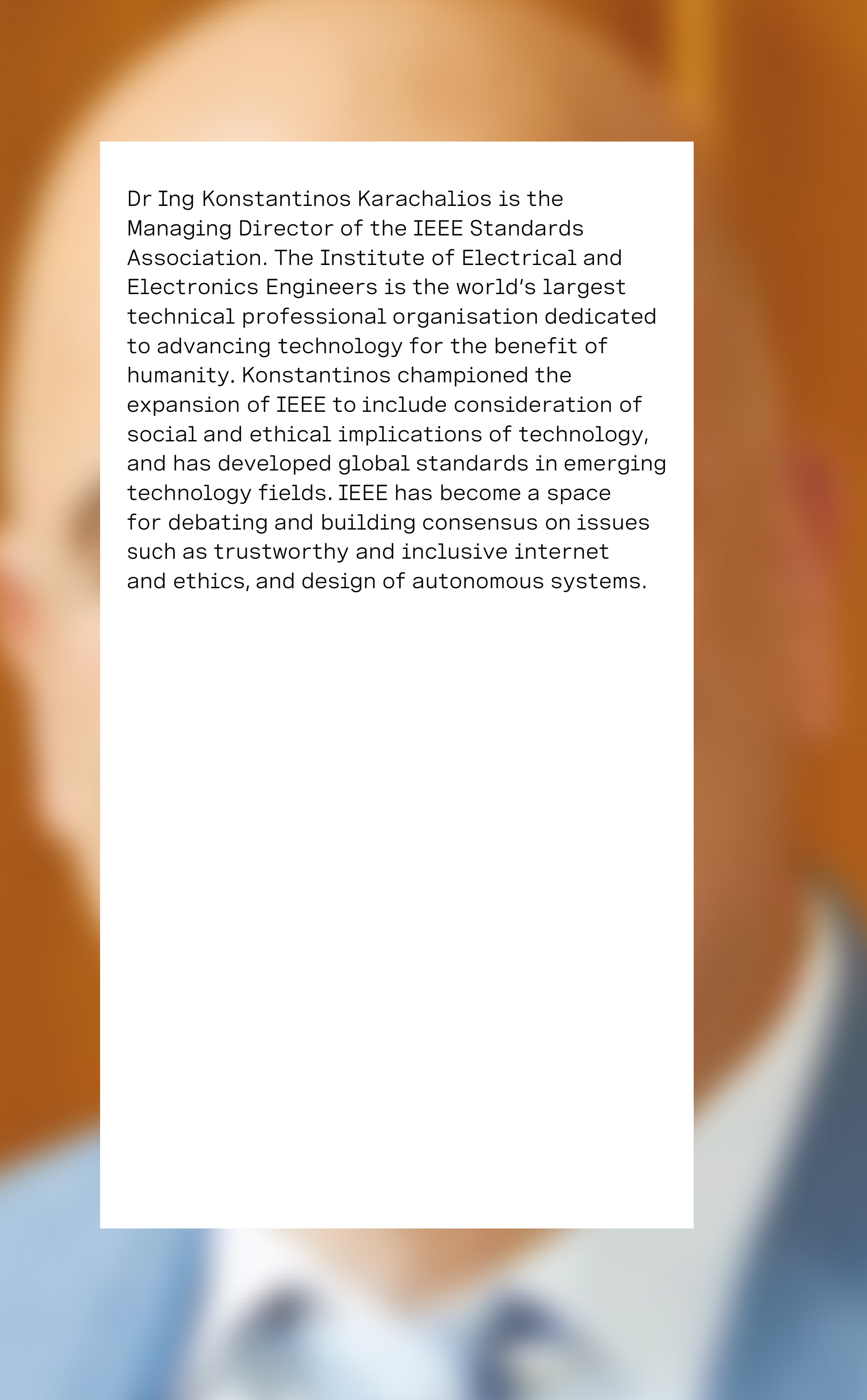
[3] Digital birth: welcome to the online world, Business Wire, 6 October 2010

[4] We read 150 privacy policies. They were an incomprehensible disaster, New York Times, 12 June 2019

[5] Whose rights are they anyway? Trends and highlights from Stream 1 of the DPC's public consultation on children's data protection rights, Irish Data Protection Commission, 9 September 2019

[6] Livingstone, S., Byrne, J. Parenting in the digital age: the challenges of parental responsibility in comparative perspective, Nordicom, 2018

[7] Data ownership, rights and controls: reaching a common understanding, British Academy, Royal Society, TechUK, 3 October 2018



Dr Ing Konstantinos Karachalios is the Managing Director of the IEEE Standards Association. The Institute of Electrical and Electronics Engineers is the world's largest technical professional organisation dedicated to advancing technology for the benefit of humanity. Konstantinos championed the expansion of IEEE to include consideration of social and ethical implications of technology, and has developed global standards in emerging technology fields. IEEE has become a space for debating and building consensus on issues such as trustworthy and inclusive internet and ethics, and design of autonomous systems.

Dr Ing Konstantinos Karachalios

The Five Singularities We Have Created and What They Mean for Our Children

I believe that in Europe, a thousand years after its burial by theocratic regimes and raw barbarism, the paradox of rediscovery of the scientific method as a search for truth, together with the social rise of a kind of middle class, helped to open the gates for a new era of enlightenment and political emancipation. Half a millennium after the so-called Renaissance, the 20th century tested all limits of humanity. We failed many of these tests, but miraculously, we survived. There was even a moment at the end of this century, when the triumph of a capitalistic regime, allegedly based on rationality and tolerating some varieties of political freedom, appeared to be so overwhelming that the "end of history" was proclaimed; the era of liberal democracies had become apparently irreversible.[1] Thirty years later, I find myself wondering whether we are truly progressing, equipped with tech gadgets of all sorts, toward a new age of enlightenment or regressing toward a new era of dark ages.[2]

Unfortunately, I am not overly optimistic. There is a school of thought around one hypothetical "singularity",[3] based on a messianic vision that computers will take control over humans and possibly protect us from our worst inclinations. However, I cannot warm-up to this idea, mainly because I fundamentally disagree with their concept of "human intelligence" as a mechanical, computer-like "function". There are good reasons to believe that the phenomenon of human intelligence has aspects that we are able to observe in action, but cannot explain with purely rational means.[4]

Moreover, there is no reason to spend any time on such speculations, because there are at least five other obvious singularities that are already ante- or even intra-portas. Three of them represent threats and two are possible remedies.

Probably the most acute threat-singularity emanates from the escalating nuclear weapons races, and the coupling of such uniquely lethal devices to more and more complex computer systems for their control. Knowing the number of times in the past seventy years that humanity survived incidents of incorrect computer hints to nuclear attacks, it is already a miracle that I am still alive and writing this essay. We should all send thanks to Lieutenant Colonel Stanislav Petrov who may have saved humanity single-handedly in one extremely critical situation, because in 1983 he was still able to say "[W]e are wiser than the computers. We created them" and ignore the false nuclear attack alarm in the middle of the night.[5] To this type of directly tech-induced threat, we could add engineered viruses that could swiftly eradicate humanity.

The second, extinction-level threat is of a geological dimension. Against the Western image of a passive-submissive "nature",[†] Gaia is hitting back, big time, and much faster than predicted by the most pessimistic scenarios. In the past few million years, the earth has never warmed up as quickly and to the level that our children's generation will most certainly experience, even if we start doing our best-of-the-best, immediately.

The third singularity is socio-political and is intimately associated to an epochal shift of the regime of power. We, adults, were born and grew up in an era where power was exercised mainly in a disciplinary manner, where the insignia of coercion were the walls (around schools, military barracks, factories, prisons). Now power is exercised more and more through a continuous, modulated control; through devices granting us access to the resources we need, while enabling a ubiquitous tracking and monitoring of our physical presence and activities. One remarkable result is that the physical "factory" is ceding its place to an "enterprise", which becomes more and more virtual.[6]

Regarding the relation between technique and power, Lord Anthony Giddens says that it is the mastering of the techniques of storage (food, weapons, information) and of "transportation" that gives rise to empires.[7] It seems now that the most precious goods to be stored and transported are information and knowledge, in particular information about ourselves and our behaviors that results in knowledge that helps anticipate our future desires and actions. Assuming this is an accurate assessment, who are the true emperors of our era and what have we, techno-scientists, done to bring them to power? It is a delusion to believe that our democratic systems can survive this classic master-slave configuration. The crisis of some flagship democracies is not just an unfortunate episode; rather, it is probably the prelude of worse that is coming.

The fact is that we are rapidly losing the power to reveal or conceal the aspects of our personality and personal life, or in other words, to choose our personas[‡] according to our interactions and their circumstances, as we have done since the dawn of humanity. After homo sapiens, a new human species is emerging, the homo transparensis. We are becoming totally transparent to people and mechanisms that are themselves obscure and not transparent, while forcing all others to accept their rules of the game. How dominant their position has already become is revealed by the fact that they state publicly and solemnly, almost without any protest or backlash, that they will decide how much "privacy" we deserve, or whether we should try at all to keep something secret (from them). They have become so self-confident, because we are subduing ourselves without physical coercion to their new power regime. A regime which disguises itself as a "service", at the same time as it takes control over our identities; manipulating our behavior through anticipation and co-opting

[†] Close your eyes, think "nature" and note what you do NOT see in the picture (for the solution wait until the end of this essay).

[‡] Persona is a Latin word, literally meaning 'theater mask'.

our desires, thus perverting our capacity to imagine our future.

While some may say that we deserve what we are getting, our kids definitely deserve better. The problem is that they are born into the new power regime and will perceive it as something "natural". They will find it difficult to realize that it is an artefact that we, their parents, produced within one generation. In addition, they are factually deprived of their most fundamental and encoded rights, by having all kinds of data about them gathered since birth and by being treated as consenting adults in the cyber-space. How are they supposed to have a chance in their struggle for dignity and political self-determination in a world where their desires, intentions, and acts are transparent from the moment of their birth, in a monstrous hyper-realization of Foucault's Panopticon? This will inevitably lead to a political submission and thus to a prolonged medieval age, where the new benevolent masters of the cloud[8] will dictate how much dignity, privacy, and wealth everybody else deserves as a function of one's willingness to serve the new regimes of power.

Interestingly, there is a common link among all mentioned singularities (including the one hypothetical and the previously mentioned three real singularities): they are all intimately related to developments in the sphere of science and technology (i.e., computing, combustion engines, nuclear science, and the Internet/Web). Whereas all these technologies are releasing new types of energy and possibilities, all have also exhibited critical downsides. Combined, these downsides may have a devastating effect on the souls of our children, through what Paul Virilio calls "negative horizons".[9] What could be a blessing turns into a problem, because techno-science has become a Deleuzian "machine de guerre": a system that does not recognize any constraints, other than its own temporary limitations, and thus imposes itself as a "fact", largely resistant to any attempt for control from "outside".[10] Heidegger, in his famous interview to Augstein, speaks even of "Technik" as a new sui generis ontology, largely escaping human control and one that will inevitably extinguish humanity.[11]

Even if we assume that Heidegger was exaggerating, the fact is that techno-science has been integrated by and is primarily serving another self-referential mega "machine de guerre", namely turbo-capitalism; the future of humanity being an "externality" to its single "currency" and purpose, namely exponential growth. How else can one explain the mind-boggling fact that extremely rich power brokers are vehemently obstructing any environmental protection measures and denying anthropogenic global warming?

This epochal confluence of human-made singular threats and the apparent massive failure of our generation to deal with them explains why our children are now openly revolting against the nihilism of the negative horizons we, their parents, are offering. They are also revolting against us because they do not trust us anymore. It is becoming a clash of generations, this time at a global level. This emerging global conflict between two generations marks an unexpected socio-political turn in human history. How can we be their guardians and mentors at an individual level if they believe we have been betraying them at a collective level? This is the fourth singularity, and I would say one that should give us hope, even if it is painful and humiliating to admit our failure as the current adult generation in power and custodians of the future of our kids. This pain explains partly the intensity of vitriolic hatred against the kids who dare to speak up.

The fifth singularity is the one announced by Buckminster-Fuller approximately fifty years ago, when he proclaimed the "technological ability to protect, nurture, support, and accommodate all growth needs of life." He concluded that precisely because of this technical progress, humanity was about to cross a singular boundary: "It no longer has to be you or me. Selfishness is unnecessary and hence-forth unrationalizable as mandated by survival. War is obsolete."[12]

What a vision! The problem is that it looks like we are going in the opposite direction, where technology is used primarily as a strategic tool in the service of power and dominance, at all levels. The current falling apart of this globalization era is probably due as much to trade and social tensions as to aspirations for global, perennial dominance, and military supremacy through technology.

So, is there anything we, scientists and technologists, can do as individuals and through our collective forms of self-organization to make Buckminster-Fuller's vision a reality? As an example, we could use our collective intelligence as well as our inclusive community building and convening capacities to contribute to blueprints and road maps of actions toward a sustainable planet: in particular to mitigate global warming as much as possible. We would do so by integrating technological expertise with policymaking and other experts, such as economists and climate scientists.

We could join forces to create a "[s]afe, secure and performant information and communications technology that fosters the fullest achievement of humanity's potential."[13] In particular, we should work together with those legislators and regulators who try to both enforce existing children's rights in online environments and create new rules where this might be necessary. We could offer our neutral and well-informed technical expertise when regulatory frameworks are being built, and support their implementation through appropriate technical tools, platforms, and standards.

At the same time, we should try as much as we can to reduce feeding the forces that work against our goals. To understand these forces, we must add a layer of self-reflection, individually and collectively, about what we are doing and how. Perhaps, we could ask the "why" questions too. We must challenge the self-serving perception of inherent innocence or benevolence of our acts. The time of innocence is over: it is time to really become adults, at an individual and collective level.

Several scientific and engineering professional associations have already begun to address ethical aspects of their profession and encourage their members to assume their share of responsibility for a human-centric design and use of the technologies and systems they produce. As an example from my direct field of experience, IEEE has recently revised its Code of Ethics to reflect the need to assume our share of responsibility, through complying with "ethical design and sustainable development practices" and by improving " the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems."[14] IEEE's Global Initiative on Ethics of A/IS[†], and the work inspired and produced by its global communities, such as Ethically Aligned

Design and the related series of standardization projects and certifications, are large-scale trailblazers in this direction.[15]

ACM also recently revised its Code of Ethics, which now includes environmental considerations as well as "promoting fundamental human rights and protecting each individual's right to autonomy."[16] It would be interesting to think through what the deeply manipulative and addictive computer programming by many online platforms practically means with regard to our children's rights to mental health and autonomy, and what may be the personal responsibility of the involved programmers and coders.

In spite of these encouraging signals, we are still in the timid beginnings. A much deeper and broader transformation is necessary. This means we should push our organizations as much as we can to assume their - often publicly declared, but not always executed - good intentions and ambitions, in the service of global public goods that would strongly push the needle in the right direction. Even the CEOs of some of the most notorious Wall Street corporations declared recently that their goal should no longer be to simply serve the short-term shareholder interests but also to pursue broader socio-economic ambitions. Let us not ironically shrug our shoulders, and take this instead as a sign of change that may be in the air. In addition, let us work within our organizations so that they start to not only explicitly embrace but also practically pursue higher global causes, e.g., what can a given knowledge-based organization do to join the fight against global warming? What can it do to respect and enforce our codified norms and rights online?

Finally, we must understand that we cannot do this alone. We have to ally ourselves with those political actors and other scientific disciplines that fight for a sustainable planet and for a new "Internet" in the service of democracy and enlightenment. In particular, we need to recognise that "children are children until maturity, not until they reach for a smartphone," as my friend Baroness Beeban Kidron says, and commit to the principle that the online world should be designed to account for children's rights and needs.

† Autonomous and Intelligent Systems

In the *Iliás* there is a remarkable episode about the fate of King Télephos, who was wounded by Achilles. His wound was not healing with time, and the oracle told him "ο τρώσας και ιάσεται", which can be translated as "the one who hurt you will heal you." Only if we, techno-scientists, wake up and divert techno-science from being a machine de guerre per se and in the service of another machine de guerre, only then will we stop infecting the wounds of humanity and be part of a healing process, of the driving forces toward a new age of enlightenment.[†]

[†] Answer to 'Close your eyes, think "nature" and note what you do NOT see in the picture': humans

[1] Fukuyama, F. The end of history? The National Interest No. 16, 1989

[2] Bridle, J. New dark age; technology and the end of the future, Verso, 2019

[3] Vinge, V. The coming technological singularity, Feedbooks, 1993

[4] Karachalios, K., and Ito, J., Human intelligence and autonomy in the era of 'extended intelligence'

[5] Stanislav Petrov, Soviet Officer who helped avert nuclear war, is dead at 77, New York Times, 18 September

[6] Gilles Deleuze has anticipated this development in a text published, see: Post scriptum sur les sociétés de contrôle, L'Autre Journal, Numéro 1, May 1990

[7] Giddens, A. The constitution of society: outline of the theory of structuration, Cambridge: Polity Press, 1984

[8] Note 2

[9] Virilio, P. L'Horizon négatif: essai de dromoscopie, éd. Galilée, 1985

[10] Deleuze, G., Guattari, F. Nomadology: The war machine, Semiotext(E), 1986

[11] Der Spiegel 23/1976

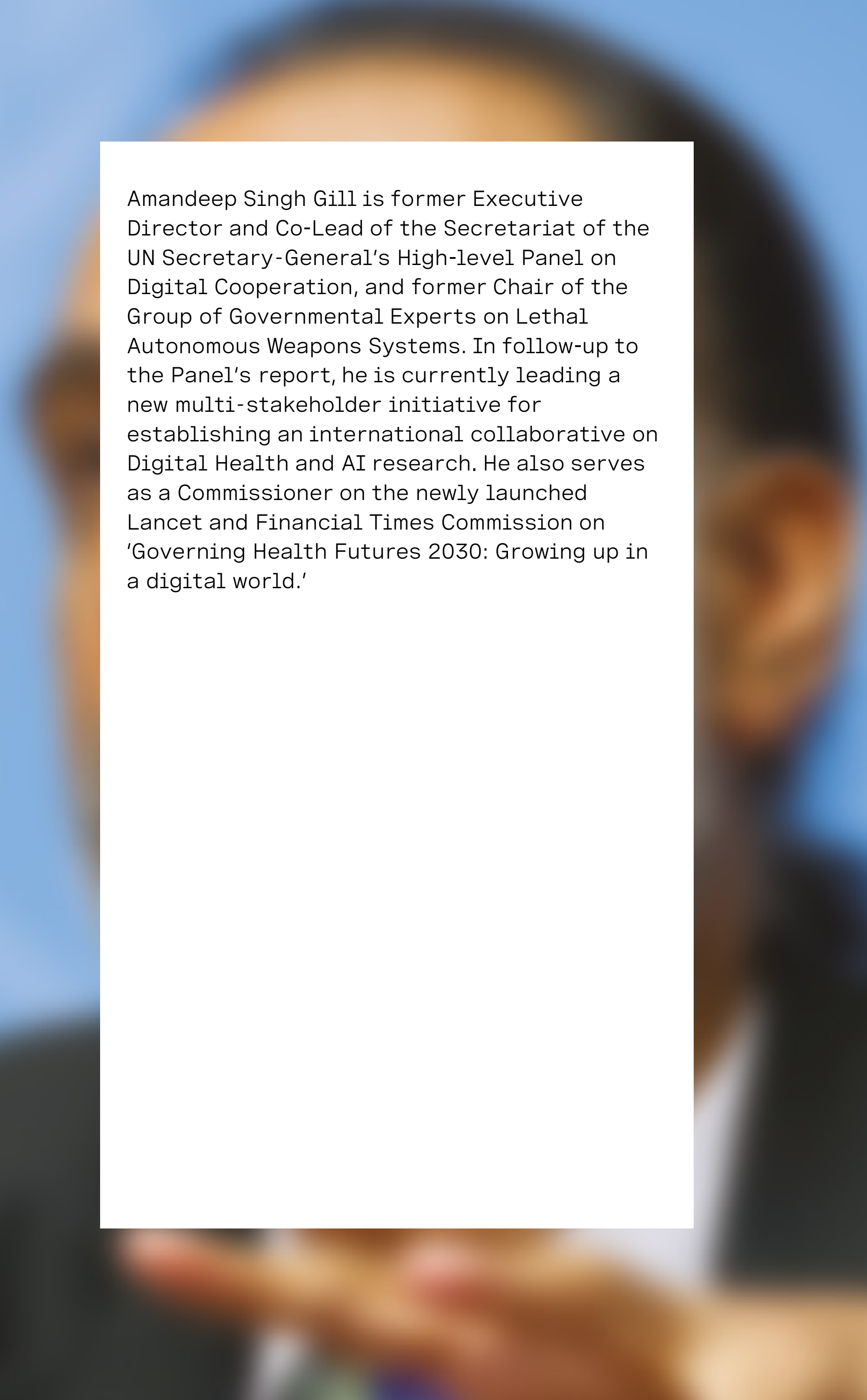
[12] Buckminster-Fuller, R. Critical Path, New York: St. Martin's Press, 1981

[13] Fish, R., Luiken, M., Meyer, B. IEEE and Sustainable Development, Presentation at IEEE Board of Directors meeting in Boston, USA, November 2019

[14] See IEEE Code of Ethics, in particular Clauses 1 and 5

[15] Ethics in Action, IEEE

[16] ACM Code of Ethics and Professional Conduct



Amandeep Singh Gill is former Executive Director and Co-Lead of the Secretariat of the UN Secretary-General's High-level Panel on Digital Cooperation, and former Chair of the Group of Governmental Experts on Lethal Autonomous Weapons Systems. In follow-up to the Panel's report, he is currently leading a new multi-stakeholder initiative for establishing an international collaborative on Digital Health and AI research. He also serves as a Commissioner on the newly launched Lancet and Financial Times Commission on 'Governing Health Futures 2030: Growing up in a digital world.'

Amandeep Singh Gill

Being a Child in the Digital Age

Today, children and adolescents under the age of 18 make up one third of all Internet users.[1] They are also the most connected age group: 71% of young people between the ages of 15 and 24 are online, compared to just 48% of the total population.[2] Children and young people are not only consumers of digital content but they also generate significant data through gaming apps and platforms such as Instagram and YouTube.

As children continue to go online at increasingly younger ages and have growing access to connected devices of their own, we have seen unforeseen consequences of use, ranging from children’s sexual exploitation and bullying online, to distraction at school and at home. There are new trends in abuse such as ‘on-demand’ and crowd-sourced production of sexually-explicit material, encrypted offender communities, as well as live-streaming, grooming and sextortion.[3] In some cases, children are victims as well as offenders.

One trend that worries me personally like no other is the impact of engaging with the world through screens, on children’s minds and bodies. There is more than anecdotal evidence that deep thinking and focus are being impacted as children spend less time reading books and wrestling ideas with peers and adults. There is also evidence that the delicate balance in education between head, hand and heart is being disturbed. Any number of physical education teachers will tell you that children have more difficulty catching balls today, there are growing sleep and posture-related health issues, and school counsellors struggle to keep up with children with emotional difficulties.

Human rights such as those enshrined in the Convention on the Rights of the Child (UNCRC) have been traditionally addressed to States, which have a duty under international law to uphold them, and protect children. The circle of impact upon private companies was limited. This has changed with digitalisation. Online platforms, developed privately, function now as global digital public infrastructure, and algorithms designed in one place can impact decisions and behaviour in other geographies. And unlike other industries, digital companies can impact the rights of millions at once. That they operate seamlessly across borders complicates governmental efforts to work with them, to protect the human rights of users within their jurisdiction.

Apart from issues around the protection and promotion of children's rights and privacy, there are issues of equal opportunity. In 2030, of the 8.55 billion global population, 39% (equivalent to 3.31 billion) will be young people under 25 years of age and 24% (2.03 billion) will be children under 15.[4] Almost one-third of children and young people will live in Africa. These digital natives could be a huge asset given the right educational and economic opportunities. However, if existing inequalities continue to fester and are allowed to intersect with new digital divides around access and agency, the asset of digital natives could turn into a liability. There is therefore an urgent need to promote lifelong learning alongside quality content and skills needed to thrive in a world of AI and data systems.

How can we manage the risks of digital technologies for children, and deploy them in a way that promotes their wellbeing? How can we make certain that children grow to be lifelong learners and have the skills needed to succeed in the digital economy? How can we ensure that childhood is not overwhelmed by digital devices and content; just as disease, poverty and exclusion overwhelmed the joys of childhood for millions in the past?

This is a formidable task. For one, it cannot be achieved by a single government or organisation alone. We would need an unprecedented level of collaboration across the public, private, tech and civil society sectors to get it done. Political will would need to be mobilised for this collaborative effort, which should go beyond the child online safety framework that has been at the center of efforts thus far.

Second, we need research and evidence-based consensus around key concerns. This should include new metrics and new ways of measuring children's wellbeing in the digital age, as well as policy research on how – and under what conditions – digitalisation would help children flourish.

Third, we need concrete guidance on how to safeguard children's rights under existing covenants and national laws in the course of digitalisation. We already have useful principles to help companies evaluate their responsibilities for protecting children.[5] The 5Rights Foundation has outlined further principles as a minimum requirement for children to enjoy a respectful and supportive relationship with the digital environment.[6] The UN Secretary-General's High-level Panel on Digital Cooperation noted some good practices on strict design and data consent standards for online services and apps used by children.[7] The Committee on the Rights of the Child is working on a General Comment on children's rights in relation to the digital environment.[8]

Finally, we need to empower the children themselves through education and respectful dialogue. I have experienced this power of agency first-hand when discussing digitalisation in school with children. A middle school student came up with an interesting distinction between watching a story online and reading about it. "When we read, we can stop and make our own story. When we watch a video, we are in someone else's story." Our schools need to develop imaginative programmes to develop digital literacy and agency going beyond the teaching of ICT skills.

We owe it to them. After all we put this technology in their hands without sufficient forethought.

[1] The state of the world’s children, UNICEF, 2017

[2] Ibid

[3] Global threat assessment 2018, WeProtect Global Alliance, 2018

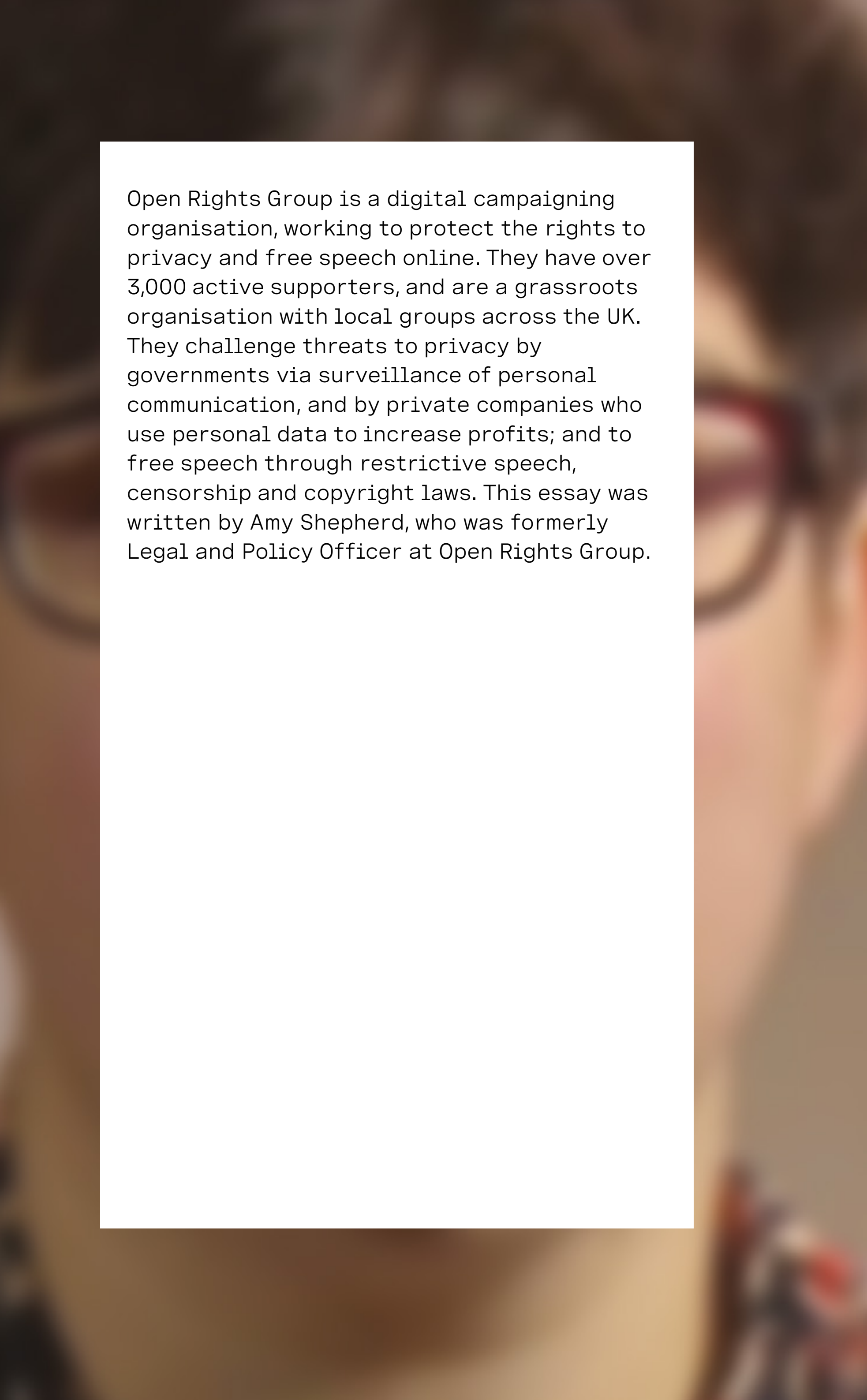
[4] Population Division, United Nations’ Department of Economic and Social Affairs, 2019

[5] Guiding principles for business and human rights: implementing the United Nations’ ”Protect, respect and remedy” framework, UN Global Compact, 2011

[6] The 5Rights framework, 5Rights Foundation

[7] The age of digital interdependence, UN Secretary-General’s High-level Panel on Digital Cooperation, 2019

[8] General Comment on children’s rights in relation to the digital environment, UN Committee on the Rights of the Child, 2019



Open Rights Group is a digital campaigning organisation, working to protect the rights to privacy and free speech online. They have over 3,000 active supporters, and are a grassroots organisation with local groups across the UK. They challenge threats to privacy by governments via surveillance of personal communication, and by private companies who use personal data to increase profits; and to free speech through restrictive speech, censorship and copyright laws. This essay was written by Amy Shepherd, who was formerly Legal and Policy Officer at Open Rights Group.

Amy Shepherd

Right Click for the Kids: Open Rights Group's Views on Building an Empowered Digital Childhood

Open Rights Group turned fourteen years old this year. That's old enough to have been recruited by Facebook to sell our private phone and web activity for their commercial profit,[1] to have been sucked into dark advertising webs on YouTube,[2] to have seen unwanted sexually explicit images or been sent unsolicited sexual messages via social messaging services,[3] and to have been put at risk of future identity fraud by our own parents through their over-sharing of school photos, birthday party invitations, personal achievements and cherished family moments.[4]

Today's connected world presents both incredible new opportunities and troubling new threats for children and young people in the UK. The Internet and digital tools can valuably enrich learning, play and social environments, but not all of the online world is child-friendly and not all children adapt and thrive amid the rapid pace of technological development.

The challenge for researchers, regulators, technologists and activists is to navigate through these tensions and build a digital society in which children can benefit from the many wonders of the Internet, be protected from its dangers and have their fundamental rights, including rights specifically afforded to them due to their status as children, fully respected and upheld. Indeed, without privacy and freedom of expression, children cannot have a full and rich online experience. The ultimate aim of legal and policy frameworks, both in the UK and worldwide, should be to prepare children gradually for adulthood as effective participants online with agency and confidence in their rights.

This is no easy task. And achieving it is made all the more challenging by the data-driven business model on which online platforms base their commercial operations.[5] In terms of advertising revenue, children's spending power is arguably even more valuable than adults',[6] and children's developmental vulnerabilities make them easy prey for corporations and advertisers seeking to capture their attention.[7] Online platforms are desperate to amass children's data, but systems that actively court child users whilst failing to respect their rights are exploitative. Fighting the model is an essential, though potentially daunting, criteria for change.

Responsible actors in the adult world have focused extensively on improving online privacy and data protection in recent years. The EU's General Data Protection Regulation (GDPR) took a seminal step towards curbing the ability of information-hungry platforms to choose, abuse and lose consumers' sensitive personal data. The e-Privacy Regulation, if it ever manages to get out of the starting blocks, offers a similarly powerful opportunity to extend individual protections to private e-communications and messaging. Yet although these pieces of legislation and others apply equally to children, their remit is often forgotten, or not wielded, when it comes to under-18s.

Children make up the majority of online users. They interact with almost all the same online services as adults, use the Internet for hours every day (it being embedded into everyday school life and social interaction) and leave trails of data around the web that are almost as messy as an average teenager's bedroom.[8] And yet this numerically and qualitatively significant group largely tend, in UK policymaking, to be subject to a demoting narrative that defines them as passive in the online space, needing 'protection from' rather than 'rights to'.[9]

Children are the source of much creativity and innovation. Their energy, ideas and capacity for challenging the status quo is everything that the Internet was founded on. They deserve to be equal participants in the vibrant society that digital technology affords, and to have their equally fundamental rights to privacy and data protection respected and upheld. Indeed, protecting children’s rights online can have a knock-on positive impact on adults’ online experience and engagement.

The Age Appropriate Design Code (under development by the ICO at the time of writing) presents a fresh and unique approach to upholding children’s rights online. In contrast to DCMS’s nebulously-constructed ‘duty of care’, it is positively steeped in the established language of international law and focuses on maximising both rights protection and agency for under-18 Internet users. This is critical. At Open Rights Group, we strongly support ambitions to create stronger default privacy settings and we work towards better provision of information to both child and adult Internet users about terms and conditions and privacy notices. We want to empower an online system that creates a realistic digital life for under-18s, not one that replaces it with the online experience of an adult. We encourage digital- and rights-based capacity-building for under-18s, so that children can become effective participants online and can increasingly understand and exercise their rights as they move into adulthood.

This graduated approach is especially important when considering the additional vulnerabilities and needs of children with special educational needs, disabilities and mental health issues, who may have impaired capacity to understand, consent and activate their rights. It might be argued that all children, and especially those with complex personal circumstances, should be able to depend on parents or other adults under whose care they reside to take good decisions about their access to online services, to set fair and sensible web use limits and to object from an informed ”grown-up” perspective to negative or nefarious data processing. But developing digital structures appropriate for children requires more than simple reliance on parental ability.

Systems that rely on parents controlling and consenting to their children’s online experience assume that all adults have a good grasp of privacy notices, that they are sensitive to the development needs of their children and can realistically assess the risks of their use of online services. Arguably, adult caregivers fail on all three of these areas continuously. Research has shown that adults do not understand how children use online services,[10] can overreact to misunderstood context[11] and are at risk of 'consent fatigue',[12] leading to clicking without thinking. Adults might also agree to data processing where children might object, since appreciations of privacy can differ drastically between parents and their children.[13]

If parents cannot be relied on, then who can? At Open Rights Group, we strongly encourage the Government to implement Article 80(2) GDPR into UK law: this would enable children, who are inherently less able to identify their rights, to have expert third parties represent them in areas of data protection that they are unlikely to be able to access by other means. To protect children's rights and wellbeing online, it's vital to hold data-using actors to account.

But even if fines are issued and data is deleted, even if useful progress – such as better information provision and consultation with children on the wording of terms and conditions and privacy notices – is achieved, this will mean very little unless there is proper, UK-wide investment in children's ability to be competent, confident online actors. This requires embedded national curriculum learning, starting from an early age and continuing throughout school years.

The problems for children engaging with privacy and data protection online begin not at opaque wording in privacy policies, but at the very existence of privacy policies. Research shows that younger people appear unaware of what privacy policies are or where to find them. With a challenge such as this, it does not matter how much work is put into a privacy policy to make it clear for multiple reading ages if a child does not know where to find a privacy policy, or even know that they should expect to see one on a service they visit. These are the sorts of issues that only education can address.

Children themselves are requesting more education on digital issues: consultations have repeatedly found teenagers, tweens and even the youngest of ages wanting to learn more about how the Internet and companies on the Internet work.[14] This wish should not be set aside. Placing greater burdens on data controllers to operate with regard to children is a laudable outcome. Investing in educating children to gain a better understanding than their parents about the Internet, the Internet economy, and their rights online has the potential to change society.

[1] Facebook pays teens to install VPN that spies on them, TechCrunch, 29 January 2019

[2] YouTube's child viewers may struggle to recognise adverts in videos from 'virtual play dates', The Conversation, 28 March 2019

[3] Livingstone, S., Haddon, L., Gorzig, A., Olafsson, K. Risks and safety on the internet: The perspective of European children, LSE, London: EU Kids Online, 2011

[4] 'Sharenting' puts young at risk of online fraud, BBC News, 21 May 2018

[5] This model of invasively tracking people by amassing vast quantities of data on their Internet viewing, inferred preferences and sensitive identity characteristics and then monetising their online activity through personalised advertising was eloquently summarised as a system of "surveillance capitalism" by Professor Shoshana Zuboff in her book with the same title, published in January 2019.

[6] Gen Z (people born between 1998 and 2008) account for $29 - $143 billion in direct spending and is on track to become the largest generation of consumers by 2020. See: The power of gen z influence: marketing to gen z, Millennial Marketing, January 2018. Also: 93% of parents say their children influence their spending: DeepFocus, Winter/spring 2015 cassandra report: gen z, 30 March 2015.

[7] Note 1; Note 2

[8] Note 3

[9] Whilst not discounting the real protection of children online that is essential for their wellbeing, it is noticeable that policy interventions largely fail to consider children as actors with independent agency online: consider the UK Digital Economy Act 2017 and DCMS Online Harms White Paper, 2019.

[10] Boyd, D., Marwick, A. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies, 10 September 2011

[11] Ibid

[12] Macenalte, M., Kosta, E. Consent for processing children's personal data in the EU: following in US footsteps?, 10 May 2017

[13] Research shows that children have an instinct towards their privacy, with younger children seeking a greater privacy than older. See: The i in online, Children and online privacy survey, 2011

[14] See Stoilova, M., Livingstone S., Nandagiri, R. Children's data and privacy online: Growing up in a digital age, LSE: London, 2019

Kathryn Montgomery, PhD. is Research Director and Senior Strategist for the CDD. In the early 90s, she and Jeff Chester co-founded the Center for Media Education (CME), where she served as President until 2003, and which was the predecessor organization to CDD. Dr. Montgomery has written and published extensively about the role of media in society, addressing a variety of topics, including youth engagement with digital media and contemporary advertising and marketing practices.

Jeff Chester is Executive Director of the Center for Digital Democracy (CDD), a Washington, DC non-profit organization. CDD is one of the leading U.S. NGOs advocating for citizens, consumers and other stakeholders on digital privacy and consumer protections online. A former investigative reporter, filmmaker and Jungian-oriented psychotherapist, Jeff Chester received his M.S.W. in Community Mental Health from U.C. Berkeley. He is the author of *Digital Destiny: New Media and the Future of Democracy* (The New Press, 2007), as well as articles in both the scholarly and popular press.

CDD is one of the leading U.S. NGOs advocating for citizens, consumers and other stakeholders on digital privacy and consumer protections online. Since its founding in 2001 (and prior to that through CME), CDD has been at the forefront of research, public education, and advocacy protecting consumers in the digital age.

Kathryn Montgomery and Jeff Chester

Creating a Quality Digital Media Culture in the Big Data Era

In September 2019, the U.S. Federal Trade Commission (FTC) and the New York Attorney General fined Google $170 million for the failure of its YouTube service to comply with the Children's Online Privacy Protection Act, commonly known as COPPA. We spearheaded the national campaign that led to passage of COPPA during the 1990s. The law requires commercial websites and other digital media that target children under 13 to limit the collection of personal information; mandates a mechanism for parental involvement; and places obligations on companies for minimizing the collection of data, and ensuring its security. In 2013, we successfully convinced the U.S. Federal Trade Commission (FTC) to update its COPPA regulations to address contemporary and emerging practices. The new rules include restrictions on the use of "cookies" and other "persistent identifiers" that enable behavioral targeting, personalized advertising, and location-based marketing.

In 2018, our coalition of privacy, consumer-protection, and child-advocacy groups filed a complaint with the FTC against Google. Its YouTube platform, which was launched in 2005, has quickly become the number one online destination for children in the U.S., and a boon to advertisers seeking to cash in on this market. Yet, as it unleashed a growing torrent of programming and marketing designed to appeal to kids, the tech giant has been disingenuously claiming that YouTube was intended only for those aged 13 and older. This cynical behavior sent a message that any powerful and well-connected corporation could ignore U.S. privacy law, even when that law was specifically designed to protect young people.

In its landmark settlement agreement with regulators, Google has now promised to make a number of changes to YouTube's business practices, which will affect both its U.S. and global operations. As of January 2020, YouTube no longer allows personalized, "behavioral" marketing on programming that targets children. In order to trigger these new digital marketing safeguards, Google requires video producers and distributers to self-identify that their content is aimed at kids. It has also committed to "use machine learning to find videos that clearly target young audiences, for example those that have an emphasis on kids characters, themes, toys, or games" to supplement the information received from YouTube content creators. Google has also announced that it will apply marketing and other safeguards currently in place on its YouTube Kids app to all child-directed content on its main YouTube platform. These policies include banning not only ads that feature "sexually suggestive, violent or dangerous content," but also all food and beverage advertising.

In addition to these internal policy changes on its main platform, the company has committed to make substantial investments in its YouTube Kids service. YouTube Kids was initially launched in 2015 as a separate app designed exclusively for young children. But the app never rivaled the main YouTube platform's hold on children, and was plagued with a number of problems (including exposing kids to indecent and other harmful content). Now, as a result of the FTC investigation, Google announced that it will bring "the YouTube Kids experience to the desktop," increase its promotion of the service to parents, and more effectively curate different programming that will appeal to more young people—with new tiers of content suitable for "Preschool (ages 4 & under); Younger (ages 5-7); and Older (ages 8-12)." Google has also created a $100 million fund for a three-year program that is designed for "the creation of thoughtful, original children's content on YouTube and YouTube globally.

It remains to be seen how well these promised changes will be implemented, and whether the quality of content for children on YouTube will improve. The FTC is also now in the process of conducting an unusual early review of the rules implementing COPPA, which Google and other digital media companies may see as an opportunity to significantly weaken how the law is implemented. For the growing number of commercial companies seeking to generate revenues from the expanding and highly lucrative children's digital media marketplace, privacy and data protection policies such as COPPA present an obstacle to the kind of friction-free online marketplace they have perfected.

The Google settlement comes at a time when the media system is at a critical crossroads. The digital media and advertising technology ("ad-tech") industry—led principally by platforms controlled by Google, Facebook and now Amazon—has fueled the development of a complex, far-reaching, global media, marketing, and sales apparatus. Today, digital marketing utilizes technologies that track and analyze our every move on every device, from home to school to work or store. Vast databases filled with personal details on our lives can be accessed in the "cloud" in seconds, and fed into a digital profile containing ever-more-detailed information about us. These profiles are continually updated and regularly sold or given to powerful "programmatic" advertising engines that enable marketers to buy and sell us in milliseconds. An expanding array of innovative techniques and applications use artificial intelligence, machine learning, neuromarketing, virtual reality, branded entertainment, influencer marketing and more to both predict and influence our behaviors—including whom we choose to vote for in elections. Our dependence on—or addiction to—the digital world ensures that a torrent of personal and other information continually flows into the databases of Google, Facebook, leading brands, device manufacturers, mobile app developers, marketing data clouds, and others.

Children and adolescents are at the epicenter of these developments. Their role as "early adopters" with deep connections to digital media from their youngest ages, combined with their spending power and their ability to influence family expenditures, has made them a key target for tech companies and brands. The children's digital marketplace is booming worldwide, fueled by an explosion of new technologies that are swiftly moving into every aspect of young people's daily experiences. While all of these innovations create opportunities for enhancing children's lives, they are also part of a powerful and growing Big Data system with far-reaching implications for safety, privacy, and health. For example, the internet-connected toy market is expected to reach $25 billion in the next five years, with more and more products designed to react to a child's behavior in real time and "grow" with them as they become older. Many of these new products have serious security flaws, including voice-recognition software that monitors not only the individual child user, but can also connect to playmates and others; this sensitive personal information can also be shared with third parties. "Smart speakers," such as Amazon's Alexa, and the emerging business based on "voice search" also gather extensive amounts of "home life data," based on family interactions and activities, raising serious privacy and security issues for children and their families. New streaming-video services, many which are targeting children, are engaged in the same kinds of data-gathering practices pioneered by online platforms and apps. Virtual reality and AI are among the latest tools used by the food industry to promote unhealthy products to young people across multiple digital platforms. And an explosion of new messaging apps and online video gaming platforms threaten to increase young people's exposure to sexual exploitation, violent and hateful content, and cyber bullying.

While policies such as COPPA and the EU's General Data Protection Regulation (GDPR) offer some privacy-connected safeguards for children, their protections are limited, particularly in the face of this rapidly emerging, next-generation, highly commercialized media culture, where young people will serve as a generation of digital "guinea pigs" to perfect an always-on, aware and interactive digital system whose principle goal is monetization and mass personalized influence.

We believe that it is time for civil society, child advocates, educators, consumer groups, industry, parents and policy makers should build on this work to forge an international movement on behalf of young people in the Big Data era. Children and teens must be guaranteed the right to grow up in a digital media environment that supports their healthy development, fosters personal and collective growth, promotes cooperation and harmony and strives to engender democratic values. Our collective efforts should build on several global initiatives currently underway, including the United Nation's current review of its Convention on the Rights of the Child, to incorporate policies addressing the rights children should receive in the digital era, and UNICEF's work promoting such issues as the internet's impact on their health and privacy. In the U.S., EU and elsewhere, we should work together to strengthen privacy and data protection legal frameworks for children. The GDPR should be better enforced when it comes to minors, and the U.S. should legislate an update of COPPA. Protections should also be extended beyond the youngest children to include adolescents as well, giving them greater control over how their information can be gathered and used. Regulatory policies must address the ways that digital marketing impacts the lives of youth, so that unfair practices—such as paid influencer marketing—are not permitted to target children directly.

Such an intervention is especially timely, especially as the technology industry finds itself under unprecedented public and government scrutiny worldwide. The controversy over how Facebook and Cambridge Analytica used data gathering, analytics, and targeting tools to spread misinformation and manipulate voters has spurred numerous hearings and legislative initiatives in Congress and in the European Union. Amid calls for "platform accountability" from civil rights organizations and other groups concerned about racial, economic and health justice, tech companies have been forced to make significant adjustments in their internal content moderation and advertising policies. There are ongoing investigations of Google, Facebook and Amazon by antitrust agencies in the U.S. and abroad. Federal and state privacy legislation, either enacted or proposed, as well as the 2018 implementation of the EU's landmark data protection law—are forcing companies and the digital industry to begin making some changes to their business practices, including those that impact children.

The tech industry is also experiencing pressures from within its own ranks, as leading advertisers have mobilized to institute new codes of conduct and other related "brand-safety" regimes, designed to ensure that their ads do not appear alongside hate speech, fake news and other inappropriate content. Facebook, Google and other major platforms and publishers are being required to revise their business practices to ensure the interests of their most important global marketing partners are taken into account. Advocates should take advantage of these developments to ensure that concerns about the ways marketers and platforms manipulate and otherwise potentially harm young people are part of the brand safety debate. Global marketers should be pressed to adopt new codes of conduct that require them to engage in more responsible practices when it comes to children.

As we move into the second decade of the 21st century, we must seize this unique historical moment to establish a quality digital media culture not only for today's children, but also for future generations of young people.

Elettra Ronchi, Andras Molnar and Lisa Robinson work at the Organisation for Economic Cooperation and Development in various capacities. Elettra Ronchi is a Senior Policy Analyst, and since 2015, has been Head of Unit in the Division for Digital Economy Policy. In this role, she coordinates work on privacy, risk management and data governance. She is currently leading the revision of the 2012 Recommendation on the Protection of Children Online, and the review of the implementation of the 2013 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Andras Molnar is a Policy Researcher, and has worked in the Division for Digital Economy Policy since 2018, where his work focuses on data governance, digital security and child online protection. Lisa Robinson is a consultant who specialises in children's rights and protection in the digital space. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the member countries of the OECD.

The OECD is a unique forum where 36 governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

Elettra Ronchi, Andras Molnar and Lisa Robinson

Addressing the Needs of Children in the Digital Environment

Policy interventions to ensure a trusted digital environment for children increasingly demand international collaboration and whole-government coordination across traditional policy fields. Recent events indicate that there is an urgent need for strong frameworks and guidelines to support all stakeholders involved to play their part in both protecting children from online risks, and ensuring that benefits can be realised.

Since 2008, following a call made at the Ministerial meeting on the Future of the Internet Economy in Seoul (South Korea),[1] the Organisation for Economic Cooperation and Development (OECD) has engaged governments and key stakeholders in anticipating change and implementing good practice and preventative solutions, rather than simply reacting to problems in this space.

Children spend more time online than ever before, using mobile devices (smartphones and tablets) with Internet connectivity to access the digital environment. This time spent online creates a number of real and important opportunities for children and young people, such as socialising with peers, expressing themselves through the creation of online content, and seeking information on just about any topic imaginable:

essentially allowing them to exercise a number of their rights, such as freedom of expression, and rights to information, leisure and participation.[2] Whilst it is important to ensure that such benefits can be realised, increased exposure to the digital environment also results in increased exposure to digital risks. Many digital risks are online versions of long known offline risks (for instance, bullying, racism, and sexual predation) and, just as is the case in everyday life, a zero-risk digital environment is unattainable. Nonetheless, setting conditions for a safer digital environment is feasible, and children must be provided with the (digital) skills and tools necessary to recognise and manage these risks, without unnecessarily limiting their online opportunities.

In 2012, OECD member countries adopted the 'Recommendation on the Protection of Children Online' ('the Recommendation').[3] The Recommendation aims to support governments in setting the conditions for the protection of children online through better evidence-based policymaking and enhanced coordination between all stakeholders. Consistent with the United Nations Convention on the Rights of the Child (UNCRC), it defines children as all persons below the age of eighteen years. While not legally binding, OECD Recommendations do carry a political commitment, which in other policy areas such as privacy have proved highly influential in setting international standards and helping governments to design national legislation.

Today however, the landscape that gave rise to the Recommendation has dramatically changed. Not only have advances in technology resulted in an almost constant capacity for children to be online through a wide range of mobile devices, the reasons why children go online have evolved. And this is no longer to simply undertake discrete tasks, such as for research or educational purposes, but for a wider range of reasons, including for entertainment, as well as communicating and socialising with peers. The previously identified risks have also evolved and new risks have emerged. At the same time, a changing commercial landscape has resulted in increased "datafication" and rendered children important commercial subjects, a fact which has significantly impacted on their right to privacy.[4]

Since 2017, the OECD has been examining whether the Recommendation remains relevant, through surveying OECD member countries; undertaking an extensive review of the legal and policy environment; and holding expert consultations. Given the brief nature of this contribution, it is not possible to cover the full breadth of issues which have been identified through this work. However, some concerns which have been identified as central are briefly expanded below. These are: (i) the centrality of protecting children's privacy and data; (ii) the need for proportional legislative and policy responses; and (iii) the role of online platforms and other digital service providers.

Privacy and datafication

The privacy space has significantly evolved since the adoption of the Recommendation in 2012. Today, children's personal information and their data is not merely the information that they knowingly share, but includes information that can be gleaned from their online actions, as well as from disclosures that friends and parents may make. These are sure to follow children into adulthood. The information that children share online has been identified as falling into categories of (i) data given – the data children themselves provide (i.e. name, date of birth, etc.); (ii) data traces – the data they have left online (i.e. through cookies, web beacons or device/browser fingerprinting, location data and other metadata); and (iii) inferred data – the data derived from analysing data given and data traces.[5] At the same time, data can be interpersonal, institutional and commercial. Whilst most children have an understanding of their private space, interpersonal context, and personal data given (albeit depending on age), a similar understanding is more limited as it relates to commercial use of data traces and inferred data.[6]

The use of children's data, particularly the commercial use of inferred data, is a central and key issue for policymakers. A number of potential risks flow from the use and misuse of children's data. They include: concerns that artificial intelligence algorithms may direct children towards harmful advertising content; that children's personal information could be shared, leading to inappropriate contact; that data may be collected unknowingly and without consent, through apps or ‘smart’ connected toys;[7] and that children’s data may be used to allow marketers to target them.[8]

Proportional legislative and policy responses

Legislative responses today are wide-ranging and largely made up of rules and norms addressing specific risks. Responsibility is siloed across government agencies and often uncoordinated, despite digital issues crossing traditional legislative boundaries. As an illustration, legal responses to sexting often fall to Justice Ministries, when the involvement of bodies responsible for health and education is also likely needed. Sexting is also an example of where responses exist in the absence of clear evidence of actual risk; and where isolated legislative actions have resulted in some countries unnecessarily criminalising children as their own pictures are considered as child sexual abuse. Here, it is seen that the narrow conceptualising of laws and frameworks can in fact prove both ineffective and often counter-productive, if not outright harmful.[9] Legislative and policy responses should be evidence based, and should appropriately address the needs of children online.

Role of online platforms and digital service providers

Concern regarding the impact of risks such as sexting, cyber-bullying, sextortion, and harmful online content has prompted calls to change legislation and put pressure on online service providers, platforms and social media sites to do more to protect children from data misuse and online abuse. In some countries steps have already been taken, for instance the introduction of the Age Appropriate Design Code in the UK which strengthens data protection rights for children; the 2017 decision in the United States to modify the Communication Decency Act by including liability for websites who facilitate child sex trafficking; and Germany’s 2017 law, which among other issues provides significant fines for online platforms that fail to remove hate speech. While multi-stakeholder dialogue and positive engagement with business is key to addressing a number of online concerns for children, requiring platforms to be more responsible and accountable may prove effective in promoting change.

Conclusion

Changes in technology have contributed to an evolving risk landscape which requires enhanced governmental action and international collaboration to ensure that children realise the benefits of the digital environment and are sufficiently protected from online risks. In light of these developments, this essay has examined three key issues:

> The advances of the technologies through which data can be collected, stored and used have resulted in new privacy risks that are highly complex. Today children's online activities are the focus of commercial interests and a multitude of monitoring and data-generating processes. There is a need to better recognise children as data subjects and content creators, and consequently how best to protect their privacy.
>
> The wide-ranging nature of legislative responses, the drawback of separating legislative responsibilities and the narrow conceptualising of laws and frameworks are major concerns. To address these issues, policy and legislative responses should be evidence-based and able to appropriately address the needs of children in the digital environment.
>
> Finally, positively engaging businesses and better capitalising on multi-stakeholder actions are key to addressing a number of concerns for children online.

[1] The Seoul Declaration for the future of the internet economy, Organisation for Economic Cooperation and Development, 2018

[2] Articles 12, 13, 17, and 31, UN Convention on the Rights of the Child, 20 November 1989

[3] Recommendation of the OECD Council on the protection of children online, Organisation for Economic Cooperation and Development, 2012

[4] Van der Hof, S., I agree... Or do I? A rights-based analysis of the law on consent in the digital world, Wisconsin International Law Journal, 2017

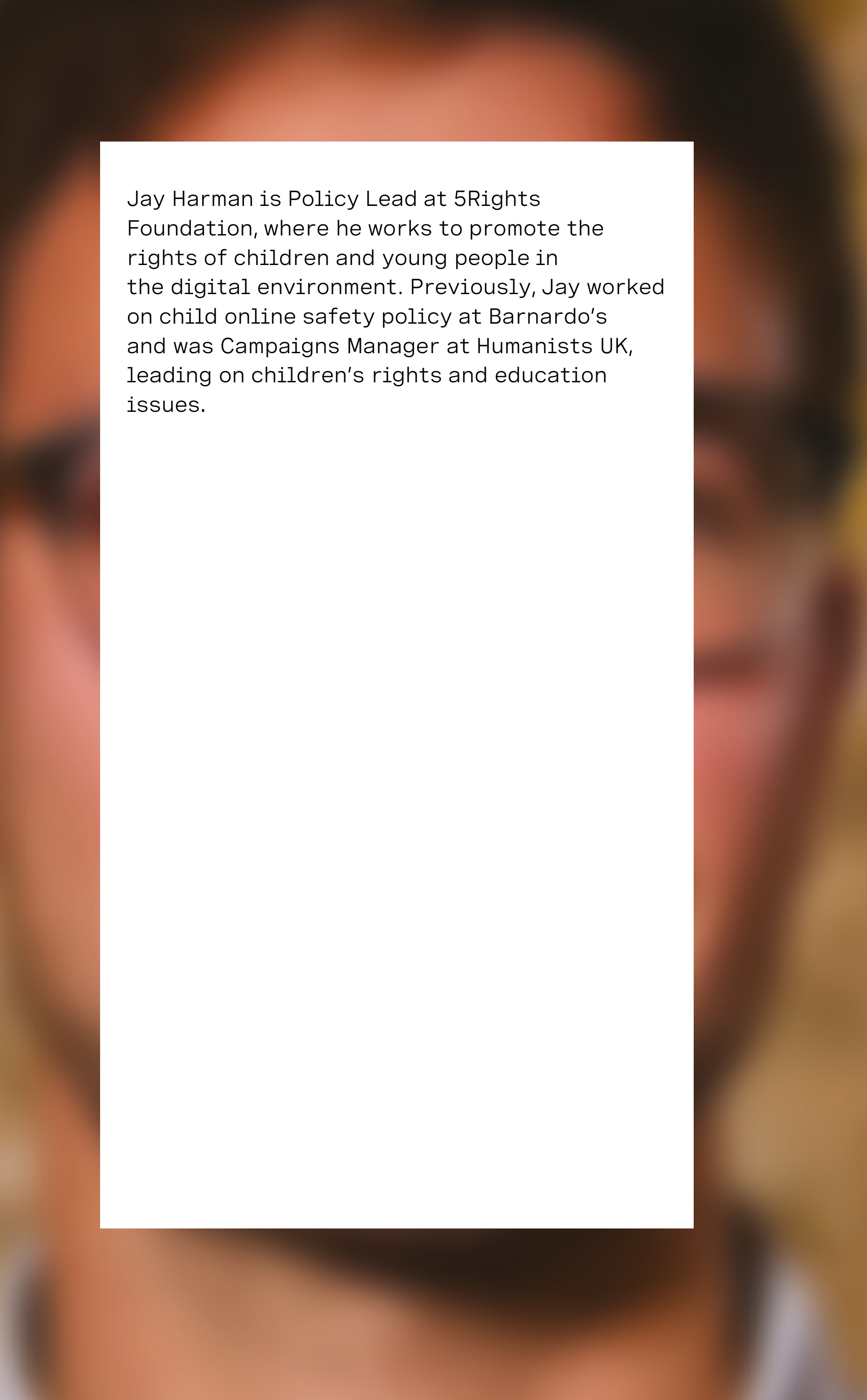
[5] Livingstone, S., Stoilova, M., Nandagiri, R. Conceptualising privacy online: what do, and what should, children understand? Parenting for a digital future, LSE: London, 2018

[6] Ibid

[7] Significant security flaws in smartwatches for children, Norwegian Consumer Council, 2017

[8] Note 4

[9] Byrne, J., Burton, P. Children as internet users: how can evidence better inform policy debate, 2017



Jay Harman is Policy Lead at 5Rights Foundation, where he works to promote the rights of children and young people in the digital environment. Previously, Jay worked on child online safety policy at Barnardo’s and was Campaigns Manager at Humanists UK, leading on children’s rights and education issues.

Jay Harman

The Enormous Potential of Technology - and the Absence of Children in the Design of the Digital World

> *Meanwhile, the poor Babel Fish, by effectively removing all barriers to communication between different races and cultures, has caused more and bloodier wars than anything else in the history of creation.*

In the digital age, we have never been more connected, and yet never more polarised. Free speech, too, is as untrammelled as it has ever been, but is often used to distort the truth and subvert our democracy, rather than promote the truth and strengthen democracy.

There are, therefore, two important lessons that we can draw from the plight of the Babel fish, the small creature described in *Hitchhiker's Guide to the Galaxy*, which when inserted into one's ear, allows them to understand any language spoken by any species from any planet. The first is the law of unintended consequences, and the second is the risk that, in the wrong hands, 'every virtue carried to the extreme becomes a vice'. These lessons are particularly relevant to the place of children in the digital environment.

The foundational, idealistic vision of the internet as intrinsically egalitarian demands that all users must be equal, and all users must be treated equally. While admirable in theory, this vision has led to children being treated as adult in the digital world, denied any meaningful recognition of their age or of the needs and vulnerabilities that come with it. "Equality", taken to its extreme and with little thought for the consequences, has effectively served to discriminate against children and to rob them of their childhood.

Elsewhere, the growing realisation of our surveilled existence, brought into sharp focus by a series of high-profile and catastrophic breaches of public trust, has led to a distorted pursuit of user privacy. Explaining away his company's pending implementation of end-to-end encryption, Mark Zuckerberg said: "Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things. When billions of people use a service to connect, some of them are going to misuse it for truly terrible things like child exploitation, terrorism, and extortion." For context, 16.8 million instances of child sexual exploitation or abuse were reported on Facebook's platforms in 2018 alone, only a tiny fraction of which would be captured if end-to-end encryption was implemented without the necessary protections in place. "Privacy", taken to its extreme and with little thought for the consequences, could come to protect paedophiles over children.

In a similar vein, the gold-standard for an integrated society is often held to be one in which "everyone is a potential friend". Social media companies have been particularly determined in their pursuit of this ideal. But as algorithms are repeatedly shown to serve up sexual predators to children (and vice versa) in the form of automated 'friend recommendations', it seems no one stopped to consider that a world in which *everyone* is a potential friend might not be a safe one for a child. "Connection", taken to its extreme and with little thought for the consequences, has served up children to strangers, and strangers to children.

The recommendation of *content* has caused problems, too. Recommendation algorithms exist to serve the right content to the right people at the right time. This ensures that the 'infinite library' is accessible and that the content we view is relevant and engaging. In 2017, however, a British schoolgirl called Molly Russell took her own life, and it was subsequently revealed that self-harm and suicide content was repeatedly and relentlessly recommended to her by the algorithms of Instagram and Pinterest. Re-appropriated to focus exclusively on boosting user engagement, these algorithms stopped serving Molly's interests and, instead, used her data to exploit her vulnerabilities. "Engagement", taken to its extreme and with little thought for the consequences, would sooner promote suicide to children than allow them to disengage.

And what of efforts to protect children online more generally? To date, online safety education has largely taken the form of 'stranger danger' messages intended to discourage children from using digital technology entirely, rather than encourage them to use it responsibly. The inexorable rise of parental control apps and student monitoring systems can also coddle rather than genuinely protect, denying children vital and formative opportunities to both encounter risk and learn how to manage it. "Online protection", taken to its extreme and with little thought for the consequences, can constrain children's flourishing rather than create the safe and supportive conditions on which their flourishing depends.

It's important to emphasise again that none of these things are problematic in-and-of themselves. Equality, privacy, connection, engaging content, and a parent's impulse to protect their child are all necessary for a thriving digital environment. The problems come when the blinkers are applied, and the needs of children are ignored (and, indeed, when we allow these virtues to be defined in ways that distort their true meaning, to serve ulterior and commercial interests).

The 'essay question' we were given for this book was to consider how we might balance privacy, freedom of expression, and security in making the digital world fit for children. Reading the essays that come before mine, I was struck by the significance of *this* group of people writing about children. An African Union Commissioner, a playwright, an applied mathematician, a NATO cyber security expert, and a UN Special Rapporteur. All of them, whatever their line of work or field of expertise, considering carefully the needs of children in the digital age.

This is not 'normal'. It may even be a first. And so, my answer to the 'essay question' is that the principal problem for children has not been a failure of 'balance'. The problem has been that children are rarely part of the equation at all. For all the proposals made in this book, the implicit consensus among its contributors is that the solution is one with which we are all familiar: the best interests of children should be a primary consideration in all matters that affect them.

It is dispiriting how regularly this fundamental principle gets cast aside. We must legislate to make sure that it cannot be.

Companies must be ready to account for the steps they have taken to protect and promote the best interests of children in the design of their services, and regulators must be resourced and empowered to instruct or sanction any companies that fall short. Above all, this means mandatory child impact assessments for any digital service, product, or feature that a child is likely to access. These assessments must be transparent, auditable, and carried out both in advance and at regular intervals. In sum, the message to industry should be crystal clear: if you fail to acknowledge honestly or respond appropriately to the impact of your business on children, there will be consequences.

I am encouraged that something like this has been proposed by the UK's Information Commissioner as part of her Age Appropriate Design Code, albeit in relation to data specifically. This principle also sits at the heart of the UK Government's plans for a 'duty of care'. We will have to wait for these to take effect before judging their impact, but I suspect they will confirm what we already know: the enormous potential of technology can only be realised when it is designed with children in mind.

In the digital age, how should we balance the freedom, security and privacy of children? Does an adult's right to freedom of expression trump a child's right to be protected from harmful material? When should a child's right to autonomy or freedom of association trump a parent's concern to know where they are? Can privacy protect children if it also protects those who wish to harm them? And, importantly, what responsibility should be bestowed on technology companies for striking this balance? How should they be held to account?

The answers to these fundamental questions will impact on the design of digital technology today, and on the tone of our digital future. They will also dictate the future of childhood itself.

In this collection of essays, global experts from a range of different fields set out their vision for a digital world that includes nearly a billion children and young people. The strength of their collective vision is less that the authors came to a consensus about everything, than that they came to a consensus about one thing. This generation of children are a "forgotten mass" upon whom we have, by not recognising their vulnerabilities and needs, allowed a social experiment at an unimaginable scale. An experiment in which we have failed to remember that childhood is the time in which everything you do, see, feel and imagine contributes to your makeup as an adult.

This volume starts an urgent, but little considered conversation. Its answers are neither definitive nor exhaustive, but we hope it will both encourage and equip regulators, policymakers, innovators, and developers to understand the impact that their decisions have on children and young people all over the world.

The discourse about children and the digital world is plagued by false binaries. They must pay for responsible corporate behaviour with their freedom, for access with their privacy, for personal security with 24/7 surveillance, and for services with their attention. These binaries protect the business interests of the data driven companies of Silicon Valley, but they do not adequately meet the needs of children and young people.

In this collection of essays, global experts from a range of different fields set out their vision for a digital world that includes nearly a billion children and young people.

5RIGHTS
FOUNDATION