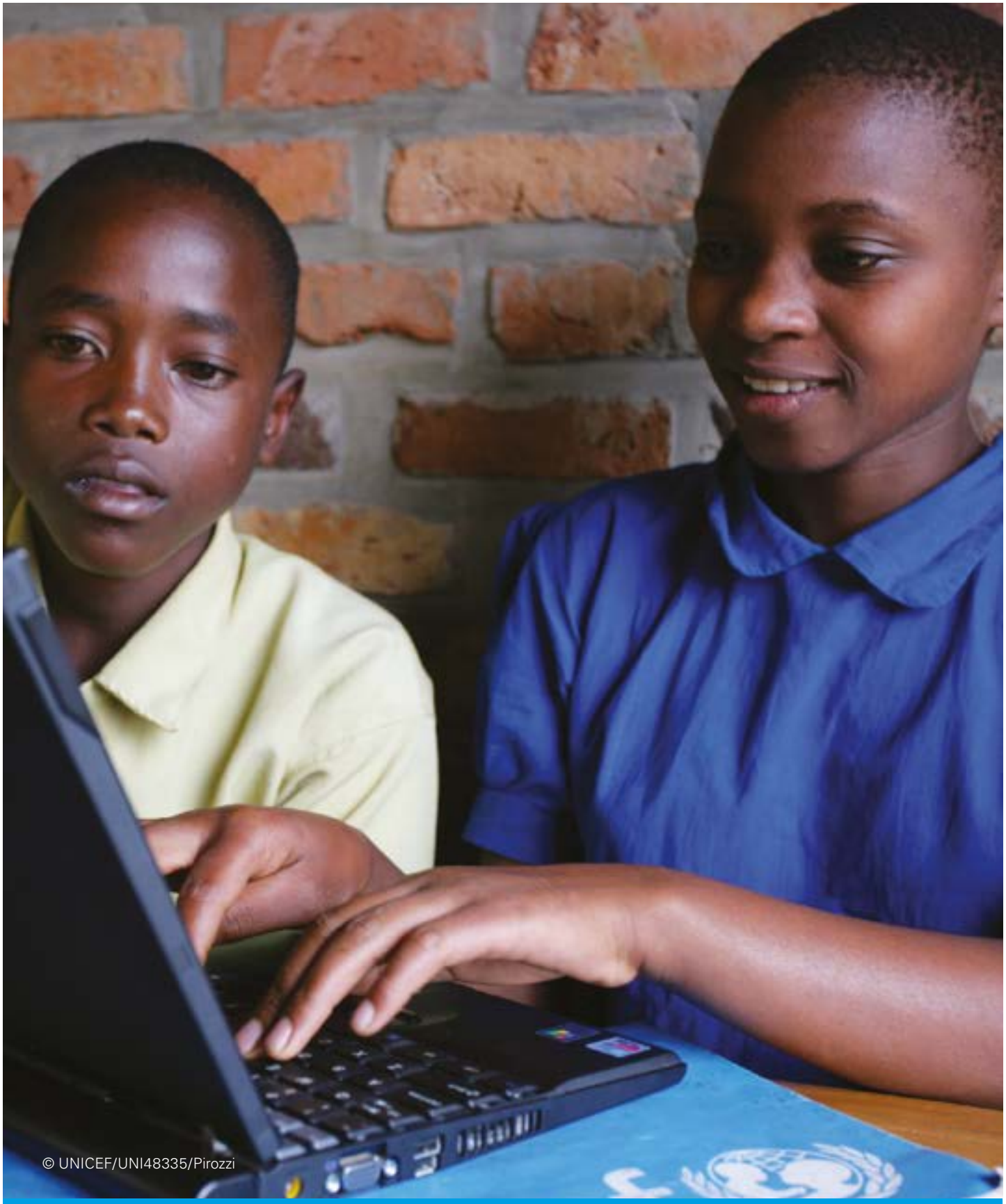

unicef

Children's Rights and the Internet

From Guidelines to Practice

Articles from the Guardian Sustainable Business Child Rights Hub

COPYRIGHT AND DISCLAIMER

This publication was developed by UNICEF in collaboration with Guardian Sustainable Business. It includes a selection of articles first published on theguardian.com from November 2015 to March 2016, which benefited from the expertise and testimonials of a wide range of companies and experts on children's rights and the Internet.

For more information, please visit
www.unicef.org/csr/childrensrightsandinternet.htm

UNICEF Contributors
UNICEF Child Rights and Business Unit:
Maria Alfaro, Saskia Baar, Emma Bergman, Kailtin Boyd, Amaya Gorostiaga, Eija Hietavuo, Robert McLean and Katherine Ortiz.

UNICEF Private Fundraising and Partnerships
Design Unit: Bruno Brocha and James Elrington

May 2016

FOREWORD

This publication includes a compilation of articles published on Guardian Sustainable Business about how different organizations, companies, and individuals are working to make the Internet and mobile technology safer for children, but also as a vehicle for children to learn, create and access information.

This series of articles and interviews elaborates on ways that the Child Online Protection Guidelines for Industry are being put into practice, highlighting the role of business, the potential for multi-stakeholder collaboration, and the various initiatives and partnerships underway to minimize online risks and harm, as well as to facilitate children's positive civic engagement through the online world.

In order to reap the benefits and reduce the risks of the rapidly evolving digital landscape, we need a coordinated global response that brings together governments, civil society, local communities, and companies.

We at UNICEF look forward to working with our partners in every sector to respect and support children's rights both offline and online, for today's children and for future generations.

Eija Hietavuo
CSR Manager
UNICEF Child Rights and Business Unit


© UNICEF/UNI118960/Tylle

CONTENTS

04
Introduction

06
Chapter 01 *Integrating child rights considerations into all appropriate corporate policies and management processes*

20
Chapter 02 *Developing standard processes to handle child sexual abuse material*

40
Chapter 03 *Creating a safer and age-appropriate online environment*

54
Chapter 04 *Educating children, parents and teachers about children's safety and their responsible use of ICTs*

69
Chapter 05 *Promoting digital technology as a mode for increasing civic engagement*

INTRODUCTION

During the past 25 years, new information and communication technologies have profoundly changed the ways in which children interact with and participate in the world around them. The proliferation of Internet access points, mobile technology and the growing array of Internet-enabled devices – combined with the immense resources to be found in cyberspace – provide unprecedented opportunities to learn, share and communicate.

The benefits of ICT usage include broader access to information about social services, educational resources and health information. As children and families use the Internet and mobile phones to seek information and assistance, and to report incidents of abuse, these technologies can help protect children from violence and exploitation. Information and communication technologies are also used to gather and transmit data by child protection service providers, facilitating, for example, birth registration, case management, family tracing, data collection and mapping of violence. Moreover, the Internet has increased access to information in all corners of the globe, offering children and young people the ability to research almost any subject of interest, access worldwide media, pursue vocational prospects and harness ideas for the future.

ICT usage empowers children to assert their rights and express their opinions, and it provides multiple ways to connect and communicate with their families and friends. In addition, information and communication technologies serve as a major mode of cultural exchange and a source of entertainment.

Despite the profound benefits of the Internet, children can also face a number of risks when using ICTs. Children can be exposed to inappropriate content for their age or to inappropriate contact, including from potential perpetrators of sexual abuse. They can suffer reputational damage associated with publishing sensitive personal information either online or through 'sexting', having failed to fully comprehend the implications for themselves and others of their long-term 'digital footprints'.

Children may be unaware of the short- and long-term consequences of engaging in risky or inappropriate behaviours that create negative repercussions for others and themselves. They also face risks related to online privacy in terms of data collection and usage and the collection of location information.

The Convention on the Rights of the Child, which is the most widely ratified international human rights treaty, sets out the civil, political, economic, social, and cultural rights of children.[2] It establishes that all children have a right to education; to leisure, play and culture; to obtain appropriate information; to freedom of thought and expression; to privacy and to express their views on matters that affect them in accordance with their evolving capacities. The Convention also protects children from all forms of violence, exploitation and abuse and discrimination of any kind and ensures that the child's best interest should be the primary consideration in any matters affecting them. Parents, caregivers, teachers and people in the community, including community leaders and a range of civil society actors, have the responsibility to nurture and support children in their passage to adulthood. Governments have the ultimate responsibility to ensure that parents, caregivers, teachers, community leaders and civil society actors may fulfil this role. Private sector actors, including the ICT industry, also have a key responsibility to fulfil children's rights.

Building on the United Nations Guiding Principles on Business and Human Rights,[3] the Children's Rights and Business Principles call on businesses to meet their responsibility to respect children's rights by avoiding any adverse impacts linked to their operations, products or services. The Principles also articulate the difference between respect – the minimum required of business to avoid causing harm to children – and support, for example, by taking voluntary actions that seek to advance the realization of children's rights.

When it comes to protecting children's rights online, businesses have to strike a careful balance between children's right to protection and their right to access to information and freedom of expression. Therefore companies must ensure that measures to protect children online are targeted and are not unduly restrictive, either for the child or other users. Moreover, there is growing consensus in relation to the importance of industry proactively promoting digital citizenship among children and developing products and platforms that facilitate children's positive use of ICTs.

Traditional distinctions between different parts of the telecommunications and mobile phone industries, and between Internet companies and broadcasters, are fast breaking down or becoming irrelevant. Convergence is drawing these previously disparate digital streams into a single current that is reaching billions of people in all parts of the world. Cooperation and partnership are the keys to establishing the foundations for safer and more secure use of the Internet and associated technologies. Government, the private sector, policymakers, educators, civil society, parents and caregivers each have a vital role in achieving this goal. Industry can act in five key areas as described in the following chapters. These five areas follow the same structure of the Industry Guidelines for Child Online Protection, calling on companies to take action to promote children's safety when using ICTs and to promote children's positive use of ICTs.

The text in this introduction and the introductory sections of each chapter of this publication are from the Guidelines for Industry on Child Online Protection, developed through a multi-stakeholder process led by UNICEF and the International Telecommunications Union. The Guidelines provide advice on how industry can work to help ensure children's safety when using the Internet or any of the associated technologies or devices that can connect to it, including mobile phones and game consoles. The Guidelines can be accessed at http://www.unicef.org/csr/.

2. "United Nations, Convention on the Rights of the Child, New York, 20 November 1989, www.ohchr.org/EN/ProfessionalInterest/ Pages/CRC.aspx. All but three countries – Somalia, South Sudan and the United States – have ratified the Convention on the Rights of the Child."

3. "For more information and to access the full United Nations Guiding Principles document, see www.business-humanrights. org/UNGuidingPrinciplesPortal/Home."

01 Chapter 01
Integrating child rights considerations into all appropriate corporate policies and management processes

INTRODUCTION

Integrating child rights considerations requires that companies take adequate measures to identify, prevent, mitigate and, where appropriate, remediate potential and actual adverse impacts on children's rights.

The United Nations Guiding Principles on Business and Human Rights call on all businesses to put in place appropriate policies and processes to meet their responsibility to respect human rights.

Businesses should pay special attention to children and youth as a vulnerable group in regards to data protection and freedom of expression. The United Nations General Assembly Resolution, "The right to privacy in the digital age" reaffirms the right to privacy and freedom of expression without being subjected to unlawful interference.[4,5] Additionally, the Human Rights Council Resolution on "The promotion, protection and enjoyment of human rights on the Internet", recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development and affirms the same rights people have offline must also be protected online[6] In States which lack adequate legal frameworks for the protection of children's rights to privacy and freedom of expression, companies should follow enhanced due diligence to ensure policies and practices are in line with international law.

As youth civic engagement continues to increase through online communications, companies have a responsibility to respect children's rights, even where domestic laws have not yet caught up with international standards.

Additionally, companies should have in place an operational-level grievance mechanism to provide a format for affected individuals to raise concerns of potential violations. Operational level mechanisms should be accessible to girls and boys, their families and those who represent their interests. Principle 31 of the Guiding Principles on Business and Human Rights clarifies that such mechanisms should be legitimate, accessible, predictable, equitable, transparent, rights-compatible, a source of continuous learning, and based on engagement and dialogue. Together with internal processes to address negative impacts, grievance mechanisms should ensure companies have frameworks in place to ensure children have suitable recourse when their rights have been threatened.

When companies take a compliance-based approach towards ICT safety that focuses on meeting national legislation, following international guidance when national legislation is not present, and the avoidance of adverse impacts on children's rights, companies proactively promote children's development and well-being through voluntary actions that advance children's rights to access information, freedom of expression, participation, education and culture.

4. United Nations General Assembly Resolution, "The right to privacy in the digital age", A/RES/68/167, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

5. United Nations Human Rights Council "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

6. United Nations Human Rights Council Resolution, "The promotion, protection and enjoyment of human rights on the Internet", A/HRC/20/L.13, http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

Child rights are universal, online and off

One in three of the next billion users of the internet will be under the age of 18, so now's the time to make children front and centre of its governance and the right to access, a new report states.

To those who fear that the web is beyond control, there's a message: there's more to hope for than to despair of. In their report, One in three: internet governance and children's rights, three experts in children's use of technology seek to pinpoint those rights to protection whilst ensuring that the benefits offered by internet and offline technology - to children in particular - are not eclipsed.

One of the authors, John Carr, makes it plain that protection cannot equal a clampdown on provision of, or participation in, online services and mobile technologies. "We don't refuse to teach children how to read because of the possibility they might come across an unsuitable book," he says, summing up the three 'Ps' that are outlined in the UN Convention on the Rights of the Child: the child rights to protection, provision and participation.

In the report's conclusions the authors make six recommendations to international internet governance organisations to ensure recognition of children's rights. They recommend that internet governance organisations recognise that around one in three internet users is under 18 years of age and that children's rights are central to any activities, policies and structures when internet governance processes are considered and set up. However, the authors counsel that care should be taken to promote the full range of child rights in the internet governance debate, beyond just protection.

The three authors call on all those playing a part in the internet to become involved - from international governance organisations and educators to welfare professionals and te private sector. They also state that children, according to their capacity, should be represented when internet governance processes are set. The representation could be through appropriate people, through research or through children's direct involvement. The recommendations state that involvement should be supported. Finally, the authors advise that mechanisms are put in place to represent and implement children's rights online and point out that an evidence base is required to support and track all the report's recommendations.

HOW TO DEFINE A CHILD?

Co-author Jasmina Byrne, who leads UNICEF's research on children and internet as well as family and parenting support, points out that even when a child takes on adult responsibilities for family needs, as a breadwinner or caregiver for example, they are considered children until they reach the age of 18.

"It is important to remember that child rights are universal and equally applicable everywhere in the world, irrespective of the age or gender of the child, whether they go to school or not, are rich or poor. And that should be the same when it comes to the internet. Why should we think that rights, when applied to the internet, are any different?" says Byrne.

"What we could do as parents or educators … is really to make sure that we build [children's] skills, capacities and their resilience, but also to improve our own relationships and communications with them – and trust – so that children will come and tell us when things happen," she says.

That trust could be invested in older siblings, friends or teachers, besides parents, she says, so that children report incidences of bullying or sexual harassment without feeling guilty or ostracised if they find themselves a victim.

UNICEF, in collaboration with the International Telecommunication Union (ITU), has published the Guidelines for Industry on Child Online Protection, which also sheds light on how ICT companies can play a role in areas such as educating customers to manage concerns on Internet usage; setting up mechanisms and educating parents to be involve.

It is understandable that in countries such as India or Africa providing clean water seems more pressing than children's rights to safe provision of the internet and technology, so co-author Sonia Livingstone feels the better-policed nations, where many of the biggest technology firms have their headquarters, should get involved in international governance and regulation.

"Getting decent sanitation is important, but it is also possible that having a phone in their hand can help [children] in locating resources or help to target material as well as information needs," says Livingstone, who, besides being a professor at the London School of Economics and Political Science, acts as an adviser for UNICEF, the European Parliament and the ITU.

One simple solution to ensure that decision-making and governing bodies take account of global children's interests would be the inclusion of at least one children's representative to speak on their behalf, since even the best intentioned organisations tend to ignore them as a vulnerable group, she feels, highlighting one of the key recommendations within the report.

Carr, who is one of the world's leading authorities on children and young people's use of the internet and associated new technologies, and who has advised the ITU, the European Union and several major high tech companies, says it's time to make companies more open to scrutiny and regulation in the matter of data privacy, which could be a big issue in years to come.

Any lack of action on the part of providers, regulators and international governance institutions when it comes to monitoring, regulating and empowering children in the use of technology might make tomorrow's adults feel that today's adults failed them, he says.

© UNICEF/UNI142000/Vishwanathan

How can children be protected online when the internet has been designed for adults?

Sonia Livingstone examines how policies and tools which evaluate digital rights and freedoms can be more inclusive of children.

There is growing momentum behind the idea that children's rights need renewed support and fresh thinking in today's digital age. How can children's right to privacy be respected when anything and everything seems to be online, permanently? How can they be protected, when the internet has been designed for adults and doesn't even know which of its users are children? How can they be free to explore, express themselves and participate when a risk-averse society wants to keep them in walled gardens or monitor their every message?

Right now, national and international organisations are commissioning new reports and spawning initiatives centred on the idea of digital rights. Parents and children themselves are increasingly anxious about the significance of the digital transformations they are living through: ever more of our time and money devoted to digital platforms; ever more of our once-public activities (think of learning, playing, even just chatting with friends) now mediated by transnational proprietary services whose terms and conditions few of us fully understand.

Is the result more opportunities or more risks? More expression or more exploitation? Most likely the answer is "both". But where do children fit in? Perhaps a focus on human rights is enough?

But where do children fit in? Perhaps a focus on human rights is enough? But children are often the digital pioneers – trying out new opportunities before most adults catch up. Arguably, they are the canaries in the coal mine, encountering the problems before child protection services have caught on. Certainly, they may not have developed the understanding – technical, legal, social – that is assumed (wisely or not) of adults.

So above children's heads, but supposedly with their best interests at heart, a struggle is being played out among educators, governments, industry and policymakers about just who is responsible for what in relation to children's rights in the digital age. And while many are stepping up to the plate, the digital landscape changes fast, with new players entering the field and old solutions becoming outdated.

For this piece, I was asked whether one particular initiative, an independent audit of digital rights, could be extended to include children's rights.Ranking Digital Rights is a non-profit initiative which launched its inauguralCorporate Accountability Index in November 2015. The index evaluated 16 top internet and telecommunication companies on 31 indicators "focused on corporate disclosure of policies and practices that affect users' freedom of expression and privacy." The purpose is to "encourage companies to develop, deliver and manage products and services in a manner consistent with international human rights norms" by ranking performance, identifying barriers to good practice, and keeping the public informed. And while the report tries to be encouraging, some of the findings are pretty damning of the big platforms.

UNICEF is the monitoring body for the internationally-ratified UN Convention on the Rights of the Child, which specifies children's fundamental rights to provision, participation and protection. In principle if not always in practice, the convention applies as much online as it does offline. UNICEF itself is developing a child rights self-impact assessment tool, for companies to self-assess their performance – mainly but not exclusively in relation to child online protection. Some companies argue that self-assessment is the way to go, enabling them to head off trouble by building in design solutions from the outset, but many public and civil society bodies prefer an independent and external audit of the big corporate players – especially for something as important as human rights.

Could that be done by the Ranking Digital Rights initiative? While conscientiously conducted, transparent in its methodology and generally respected, this non-profit is already at capacity. As its director Rebecca MacKinnon explained to me, it's currently worried about raising funds for the next audit of service provision for adults' freedom of expression and privacy. I say "for adults", because even though the audit has been concerned with human rights, it's more specialised than it might sound. Thus far, it seems there has been little or no thought to the specific requirements of child users. For example, evaluating companies in terms of their "user-friendly" terms and conditions or accessible forms of redress would look very different if we assume those users are adults only, or if it is recognised that they include children.

So if policies and tools implicitly assume users are adult, where does that leave children? Often in a different department or group of specialists, the companies audited by Ranking Digital Rights have, in parallel, invested in recent years in child online safety policies of one kind or another, coordinated for example by the UK Council for Child Internet Safety. Here too, real progress has been made, not least because it is in companies' interests to avoid the reputational damage of children being harmed through their services.

All these initiatives can only work if companies take them seriously and if independent bodies monitor progress over time, and with this proviso they are surely all to be welcomed. Those I spoke to for this article from CSR departments are clear – the more tools and indexes the better, to give them leverage within their company to support child rights better. But it seems that, at present, the digital landscape is being evaluated in terms of the efforts of companies and NGOs to defend adult freedoms online, on the one hand, and protecting children online, on the other.

The result is that such initiatives appear to be generating two disconnected forms of expertise, each separately evaluated. As a result, child freedoms online – particularly important for teenagers around the world – may be obscured.

Why technology companies should tackle their impact on children

By Viktor Nylund

The ICT sector has the potential to have a positive and negative impact on children. UNICEF is working with businesses to help them place children's rights at the heart of their operations.

Children represent one third of the world's population and in some countries, especially emerging markets, children and youth can make up almost half of the population. They are consumers, they are the children of employees and customers and they are young workers, future employees and business leaders. Today's children and youth have been born into a digital world; they are exposed to technology and innovation and are avid users of new information and communication technologies (ICTs).

Technological innovation has advanced in unprecedented ways over the past decade. Although access to information and communication technology is not equal across different countries, regions and socioeconomic groups, the landscape is changing rapidly. On the one hand the rise of social media and mobile technology can provide powerful networking platforms for peer to peer education and can empower young people to express their views and demand their rights. On the other hand digital technology creates security risks for children and young people: it can threaten their right to privacy; children and youth are reached with inappropriate content; and they are the victims of online exploitation, harassment and bullying.

The ICT sector has a wide range of potential positive and negative impact on children's rights and that is why this sector is of particular importance to UNICEF in an effort to consider the impact of business behaviour on children's rights and aim to harness the resources of this industry to promote the rights of children.

MOVING FROM REACTIVE TO PROACTIVE: HOW CAN ICT COMPANIES FURTHER SUPPORT AND RESPECT CHILDREN'S RIGHTS?

UNICEF has a long-standing experience engaging with companies to deliver results for children through a wide range of interactions including fundraising and programmatic collaboration. More recently, UNICEF is working with companies, including in the ICT sector to support them in advancing child rights throughout their business operations, value chain and spheres of influence in the workplace, marketplace and broader community.

Recognising a need for explicit guidance on what it means for business to fulfill their duties on children's rights, the UN Global Compact, Save the Children and UNICEF led a process that led to the release of the Children's Rights and Business Principles in March 2012. They articulate the responsibility of business to respect – doing the minimum required to avoid infringing on children's rights; and the commitment to support – taking voluntary actions that seek to advance the realisation of children's rights.

UNICEF has also recently produced a set of practical tools. These include guidance on developing relevant corporate policies that address children's rights; conducting impact assessments; integrating appropriate programmes and systems; and monitoring and reporting on children's rights.

WALKING THE TALK: HOW THE ICT SECTOR CAN TAKE ACTION

A number of ICT companies are focused on protecting young workers and combating child labour in the workplace. UNICEF and Telenor Group recently joined forces to combat child labour in Bangladesh by providing through a combination of activities targeting working children through social workers. Millicom is another example of an international telecom company wanting to better understand its impact on child rights and thereby made use of the Children's Rights Checklist developed by UNICEF to begin identifying how to address its impact on children.

Addressing issues in the marketplace, ICT companies are taking actions to address child online protection or to market products and services keeping in mind the best interests of the child. For instance, Vodafone devised a "top tips" pocket guide for parents, as part of its child safety customer education initiative. The guide provides recommendations on a number of areas including chat, games, premium rate services and how to address bullying.

Finally, ICT companies are addressing children's rights in the local communities where they operate, by scaling up programmatic collaboration in support of national development priorities. For example, Safaricom is working with UNICEF Kenya to apply its Short Message Service (SMS) services to send bulk SMS mailings on hand washing to their over 14 million subscriber base. Another mobile operator in Thailand, Digital Total Access Communications (DTAC), joined forces with UNICEF to launch the "best start" initiative, which will provide free mobile information services to promote the health of mothers and children.

Although the industry shows greater engagement by taking action in raising awareness on the optimal and safe use of new technologies, as well as building a protective environment for children, a number of challenges still need to be addressed.

Business has a contribution to make, but so does government, in regulating and promoting business actions to address their impacts on children's rights. In 2011, in response to a request from the UK Government, a report, Letting Children be Children, was published with recommendations, one of which stated that internet service providers (ISPs), public WIFI providers, retailers, device manufacturers and mobile internet services should make it easier for parents to block adult and age-restricted material from the internet. This process inspired the four main fixed-line ISPs (BT, Sky, TalkTalk and Virgin Media) to create an Open Internet Code of Practice.
Last but not least, consumers themselves have a role to play in demanding that companies take their responsibility towards children's rights as seriously as they take the making of financial gains for their shareholders.

Maximising opportunities and minimising risk: how will we protect children online?

Top industry experts gathered in London this month to discuss the roles and responsibilities of ICT companies in safeguarding children online.

Half the world's population now has a mobile subscription (pdf) – up from one in five 10 years ago – and there has been a rapid shift from fixed to mobile broadband. Many of those with access to the mobile internet will be children, and increasing numbers of them are in the developing world.

The mobile internet offers huge opportunities for children to learn, connect, share and express their opinions. So what specific actions can be taken to maximise these opportunities while minimising and tackling the risks of inappropriate content and contact, online harassment and abuse?

These topics were the subject of the Children's Rights and ICTs – tools of the trade workshop held in London by the UNICEF Children's rights and business (CRB) unit, in collaboration with GSMA, the global industry body for mobile operators. Representatives from a wide range of industry bodies and NGOs, including mobile operators, technology companies, children's' and human rights organisations, got together to discuss these issues and to hear some of the new ways to tackle them.

Andres Franco, deputy director, private sector engagement, UNICEF, started the day by talking about the wish and need to act to protect children online. "We are always asked: 'what can I do'?" We have to make [actions] relevant to companies around the world. We have to formulate concrete measurable plans at the national level."

Keynote speaker Mats Granryd, director general, GSMA, pointed out that the UN Convention on the Rights of the Child and 2g mobile internet were both around 25 years old. He looked forward to the truly connected society that 5g would offer, with the chance of better education and health treatment in even the most remote communities.

John Morrison, executive director, Institute of Human Rights and Business talked in his keynote speech about the complexities of ensuring privacy and security while at the same time protecting children's rights. "Child rights themselves include freedom of expression and the right t o participate in society," he said. "So we can't disconnect our children from ICT nor would any of us want to."

UNICEF has already developed a range of tools and guidance for businesses that will help them in fulfilling their corporate obligations to respect children's rights. At the event, the new tools developed together with the ICT sector were discussed.

Lego, for instance, embraces the Children's Rights and Business Principles (CRBPs) – a 10-article framework that sets out actions companies can take to respect and support children's rights and the UNICEF ITU Child Online Protection (COP) Guidelines for Industry. Lego has helped UNICEF develop a COP Guidelines' related company self-assessment tool, which the company piloted recently. Lego came up with 13 actions it needed to take in the area of online safety: "We need to make them formal global policies that apply everywhere – because all children matter," said Dieter Carstensen, head of digital child safety, Lego Group.

The global telecommunications and internet company Millicom has also used the CRBPs framework and helped UNICEF develop a mobile network operator (MNO)specific company self-assessment tool to help assess children's rights impacts across the MNO value chain in different countries. In one of the African countries where they operate, they discovered there were areas of child rights impacts that they hadn't considered, for instance the role of electronic waste in increasing the risk of child labour.

Other organisations have used different ways to create a safe online environment. Caroline Millin, Facebook safety policy programs manager, EMEA, for instance, talked about its social reporting tool which looks at ways of self-resolving issues such as bullying and the posting of inappropriate photographs. Ola-Jo Tandre, director of sustainability at mobile network operator Telenor, gave an example of their work with the Red Cross, using an anti-bullying chat room, through which children could offer each other peer-to-peer support.

Following these presentations, participants got together in one of three thematic working groups to talk about children and advertising, responsible gaming and apps, and online child sexual abuse materials. Discussions were lively and participants shared challenges, opportunities and good practice in these areas.

A significant focus of the day was on online child sexual abuse and the development of technological and other solutions to combat this. According to statistics from INHOPE – the international association of internet hotlines – the number of webpages that contained child sexual abuse material increased by 147% from 2012 to 2014.

By March 2015, more than 6,300 victims of child sexual abuse had been identified in the International Child Sexual Exploitation Image Database managed by Interpol. The UK internet hotline Internet Watch Foundation (IWF) works with partners to ensure that URLs containing criminal child abuse content are identified and taken down in the UK. Susie Hargreaves, chief executive of IWF, chairing the panel discussion on child sexual abuse online, said the organisation had taken action on 32,000 URLs in 2015.

Becky Foreman, head of UK government affairs, Microsoft, spoke about PhotoDNA,developed in partnership with Dartmouth College in the US, which identifies illegal child abuse images. It creates a digital "fingerprint" which is tamper-resistant, creating a "signature" which is still evident even when images have been slightly altered. PhotoDNA allows companies to compare images with the millions of other images of child sexual abuse material (CSAM) that have already been identified. "We use technology to find CSAM, and humans to check, review and remove the content," Foreman said.

Anne Larilahti, VP sustainability strategy at mobile network operator TeliaSonera, was clear about her company's limits. "If you are determined to view this material you can do it. But we can deter people who might watch it experimentally and can ensure our customers are not going to be faced by this material by accident," she said. Within TeliaSonera, the company realised that blocking employees' access to this content on their work-supplied computers or devices was not enough. Instead, they began proactively searching for it in their corporate networks. The company announced on their intranet that they were doing this. "There was no push-back," she said.

Samantha Woolf, global partnerships and development manager at INHOPE, spoke about her organisation's work involving 50 internet hotlines, in 45 countries around the world, to stop circulation of CSAM images.

INHOPE works with Interpol and national law enforcement agencies to support notice and take down of illegal images. This is done using a prominent CSAM reporting button on their site and has reduced takedown time to days and (in the UK) sometimes hours. Using image and video fingerprinting systems means they can identify images at content level, not just the URL. That is key to avoid duplication of effort and exposure to analysts of already-known content.

Methods of tackling child sexual exploitation online were further discussed in a working group, where prevention, protection and technical solutions were considered. Issues that arose included the differences between what is culturally and legally acceptable in individual countries. Educating children about online sexual exploitation was also considered key. Projects mentioned by participants indicated that parents were best for educating 8-12 year-olds, but teenagers took more notice of "webstars" online celebrities in their early 20s.

As noted earlier, GSMA and companies like Lego and Millicom are collaborating with UNICEF in developing practical tools for the ICT industry on safeguarding children. These tools are based on the Child Online Protection Guidelines for Industry and the CRBPs and they will be released in Q2 2016 following a global consultation.

HALF THE WORLD'S POPULATION NOW HAS A MOBILE SUBSCRIPTION UP FROM ONE IN FIVE 10 YEARS AGO

A DAY IN A LIFE

DIETER CARSTENSEN LEGO Group: Safeguarding children online gives us an opportunity

Meet Dieter Carstensen, head of digital child safety, the LEGO Group

Our company mission is to provide fun, creative and safe LEGO experiences, both physical and digital, and it is my role to look after our digital child safety agenda globally.

I define the policies and assist my LEGO colleagues to ensure that we always develop the best and safest possible online and digital experiences for children. Together with UNICEF, we have recently assessed our approach and efforts concerning digital child safety. The purpose is to see where and how we can improve across the digital platforms where children engage with LEGO. Collaborating with a trusted partner is essential, simply to ensure we do not rest on our laurels, and UNICEF's expertise and critical eye helps sharpen our work.

WHAT SUCCESS LOOKS LIKE FOR ME

Success in my work is when children and parents trust our online experiences and they can safely engage in fun and creative play. For us internally, it is when we perceive online child safety as an opportunity to innovate our experiences towards the better and not see it as a restriction.

WHAT MY PROFESSION WILL LOOK LIKE IN 10 YEAR'S TIME

I see children being able to access, produce and experience more digital content year after year, thus creating new ways of engaging with likeminded people or brands like the LEGO Group. Technological tools and platforms will enable users to personalise such engagements, including the rules, thereby becoming owners of their own destiny. Catering for different needs and preferences when developing digital experiences on such scale will be challenging, so it is important to define and apply a basic safety framework that works regardless of end-user choices. I see it as the responsibility of companies to ensure that children have a safe and rewarding experience, which will not diminish with time. Unfortunately, the opposite is probably more likely the case today.

MY VIEWS ON COLLABORATION

I am happy to say that protecting children online is an area where companies and other stakeholders really come together to identify risks or challenges and discuss the best approaches to solve these. We all work towards the same goal of digital child safety and with such a mindset we are able to progress. No single company or stakeholder owns all problems nor is it able to provide all the solutions. The level of knowledge sharing on this topic between companies, that otherwise compete, is quite impressive.

> **DESPITE THE PROFOUND BENEFITS OF THE INTERNET, CHILDREN CAN ALSO FACE A NUMBER OF RISKS WHEN USING ICTS.**

THE LEADING CHANGEMAKER

When we discuss public policy, children are very often addressed as recipients and not always as a rightful source of input and inspiration. Luckily, a growing body of research which includes children's voices exists, thus enabling discussions to include recommendations based on evidence of and from children. One major source of importance is the work undertaken by the multinational research network EU Kids Online. Their purpose is to enhance knowledge of European children's online opportunities, risks and safety. Although their focus is Europe, their global recognition and impact is beyond doubt. One can only hope such research efforts will continue and are replicated in other parts of the world.

THE VALUE OF PLAY

At the LEGO Group we believe that play is one of the most effective ways to engage children in learning, which I completely buy into. Adding playfulness in the way we approach curricula, or learn social emotional skills, can help both overcome interest and attention difficulties, as well as strengthen the bond between a parent and child. Everybody likes to play, we just don't always create the space and time for it. So more than specific apps or programs, I think the application of them is what makes a difference. Teaching children to code has been a hot topic for several years, and the way it is done - in groups where you learn to collaborate - and how it requires the use of creativity, logic and to delegate and solve challenges, is a brilliant way to help children acquire critical digital citizenship skills. In the LEGO Group, for instance, we work together with other parties to host challenging building events such as the First LEGO League and World Robot Olympiad.

Children's rights in the digital era: action must come from the top of business

By Vicky Prior

Safaricom's CEO Bob Collymore is calling on the private sector to embed child rights in business today, to help shape the world of tomorrow.

"We are not the sources of problems; we are the resources that are needed to solve them. We are not expenses; we are investments. We are not just young people; we are people and citizens of this world." This powerful statement by children at the UN Special Session on Children in 2002 called on governments, businesses and others to make a world fit for them. For Bob Collymore, CEO of Kenya's largest mobile operator Safaricom and a board member of the UN Global Compact, investing in and protecting young people is a priority. He has put child rights at the heart of Safaricom's business in recent years and is working hard to persuade his peers to do the same.

"We're a big company in Kenya and some responsibilities come with that. If we're to protect the future generation, we have to protect their rights as well," he explains. "We can't do it on our own, so partnerships and bringing the rest of the Kenyan private sector along with us is really important."

With smartphone connections in sub-Saharan Africa forecast to reach over half a billion by 2020 and technology playing an increasingly important role in addressing socio-economic challenges, Safaricom's focus on young people makes good sense – from both a business perspective and its potential impact on society.

As Collymore says, "Many kids in Kenya will probably not see a computer or laptop until adulthood so the major benefit of handheld devices is that it gives them access to the internet and access to knowledge. We're working with the government, for example, to provide free internet access to government primary schools. We think that's a significant piece – if we're to close the education disparity between a country like Kenya and the rest of the world, we need to give them that access."

Safaricom also offers parental controls so that parents can limit what their children see online and is currently developing child-friendly content to be pre-loaded on mobiles and TV set-top boxes in the next 12 months.

When UNICEF approached Collymore about the Children's Rights and Business Principles, he recognised how Safaricom could further shape the way it does business with young people in mind.

"We were doing things that were benefitting children but we didn't have a child rights policy in place. So I asked the team to put together a policy using the Children's Rights and Business Principles as the basis and we worked very closely with UNICEF. I think we were probably one of the first companies to have a specific policy that addresses children's rights." Safaricom also made sure that children and teenagers, including representatives of the Kenya National Children's Government were involved in the development of the policy.

"We also launched the policy with the young people so that they could tell the story from their perspective and it was not just adults prescribing a policy for them."

Safaricom then engaged child rights champions in each business function to implement the policy and advance children's rights across the organisation. The marketing team introduced equal pay for adults and children who feature in the company's advertisements, for example, and Safaricom's mobile medical camps now include children-only facilities.

Other company initiatives include on-site crèches for employees' children run by professional childcare workers and doctors; the company's hundreds of suppliers undertaking self-assessment to ensure children are not involved in the supply chain; and a child-friendly zone at the recent Safaricom International Jazz Festival.

Having put child rights on the radar, Collymore acknowledges the importance of measuring how the company performs against the policy. Safaricom plans to use the MO-CRIA – a new child rights impact self-assessment tool for mobile operators – that has been developed by UNICEF, GSMA, Millicom and other stakeholders. As only the second mobile operator worldwide to commit to conducting a child rights impact assessment, Safaricom aims to continue influencing other business leaders through its commitment to child rights.

"I don't think the private sector is doing enough yet with the protection of children's rights. So one of the things I've been doing is to pull my fellow CEOs on to the child rights agenda and explain to them why it is they need to get involved rather than leave it for rights groups and civil society to deal with."

Collymore emphasises this is not about short-term gains; Safaricom is in it for the long haul. "We believe that if you want to run a business that will be sustainable 50 or 60 years from now, we have to look after future generations and not just manage our business for today's benefits."

02 Chapter 02
Developing standard processes to handle child sexual abuse material

INTRODUCTION

The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography defines 'child pornography' as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

Of all child sexual abuse material analysed by the Internet Watch Foundation in 2013, 81 per cent of child victims appear to be 10 years of age or younger, and 51 per cent of the images depicted sexual activity between adults and children, including rape and torture.[7] These disturbing facts underscore the importance of collaborative action among industry, government, law enforcement and civil society to combat child sexual abuse material.[8]

While many governments are tackling the dissemination and distribution of child sexual abuse material by enacting legislation, pursuing and prosecuting abusers, raising awareness, and supporting children to recover from abuse or exploitation, many countries do not yet have adequate systems in place. Mechanisms are required in each country to enable the general public to report abusive and exploitative content of this nature. Industry, law enforcement, governments and civil society must work closely with each other to ensure that adequate legal frameworks in accordance with international standards are in place.

Such frameworks should criminalize all forms of child sexual abuse and exploitation, including through child abuse materials, and protect the children who are victims of such abuse or exploitation, and ensure that reporting, investigative and content removal processes work as efficiently as possible.

Responsible companies are taking a number of steps to help prevent their networks and services from being misused to disseminate child sexual abuse material. These include placing language in terms and conditions or codes of conduct that explicitly forbid such content,[10] developing robust notice and takedown processes; and working with and supporting national hotlines.

Additionally, some companies deploy technical measures to prevent the misuse of their services or networks for sharing known child sexual abuse material. For example, some Internet service providers are also blocking access to URLs confirmed by an appropriate authority as containing child sexual abuse material if the website is hosted in a country where processes are not in place to ensure it will be rapidly deleted. Others are deploying hashing technologies to automatically locate images of child sexual abuse that are already known to law enforcement/hotlines.

7. United Nations, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, article 2, New York, 25 May 2000, www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx.

8. Internet Watch Foundation, 'Annual & Charity Report 2013', LINX, UK, https://www.iwf.org.uk/accountability/annualreports/2013-annual-report

9. Industry should provide links to national hotlines from their websites. In places where a hotline is not yet established, industry could refer reporters to the International Association of Hotlines at www.inhope.org where any of the international hotlines can be selected to make a report.

10. It should be noted that inappropriate user conduct is not limited to child sexual abuse material and that any type of inappropriate behaviour or content should be handled accordingly by the company.

We must never forget that children in sexual abuse material online are real

Networks, large companies and small start-ups all have a responsibility to help clamp down on and report child sexual exploitation on the internet

Mick Moran has a clear, strong message: "People need to realise, these are kids being abused to produce this material. These are children, real children in these images."

As assistant director of Interpol's vulnerable communities unit, Moran is at the frontline of tackling child sexual abuse online. A member of An Garda Síochána, Ireland's national police service, Moran is currently on secondment. Interpol officers do not carry out investigations themselves; the organisation's role is in coordination, database-holding, training and support across international boundaries to identify criminals and crimes. "We are putting the child first," he says. "This issue has been made demonstrably better by the role we play."

Another point Moran is very clear about is that this is not "pornography". "Pornography is deemed to be benign, seen to be socially acceptable, and the people in pornography are consenting to the actions that are being carried out on them or by them. None of those are applicable to child "pornography". We use the terms child abuse or child sexual exploitation or child sexual abuse material to be quite descriptive of what we look at."

This stark division is underlined by the age of the victims. "The vast majority of the images we deal with are of children under 10," he says. "Some are pre-speech."

In the mid-1990s, when the general public started to get internet access, there was a lot of child abuse material online, he says, and people started coming across it by accident. The Interpol specialist group on crimes against children started to look at victim identification as a key issue, and that involved the exchange of intelligence between police forces facilitated by Interpol.

This led to the setting up of the International Child Sexual Exploitation Database (ICSE) in 2001. One of its main focuses is on victim identification using image comparison software and, to date, the ICSE has helped identify more than 8,300 victims around the world and more than 4,000 offenders.

"We introduced the concept of 'finding the child'. This is a real child [being abused]," he reiterates. "And if you can identify the child you have the opportunity to disclose on behalf of the child because we know the child has been abused. Offline sexual abuse is by nature secretive, and rarely disclosed by the victim, but with this material we knew the abuse had taken place."

The database also means that they can avoid duplication of effort. "We don't want two officers in two parts of the world trying to identify the same child without knowing [they are doing so]."

Targeting the victim also has another advantage. "If you target the victim in your investigation you will find the abuser because the vast majority of child sexual abuse takes place within the immediate family circle. So statistically, if you find the child you are going to find the perpetrator."

Partnerships – particularly with industry – are key to Interpol's work. "The internet is a network of networks," Moran says. "We could go a long way to reducing online exploitation of children if everyone who owned a network ensured that there were proper child sexual exploitation prevention mechanisms in place. Systems administrators will scan their networks for spam and malware so why not child abuse material?"

The bigger organisations, such as Google and Facebook, do this already, as do some of the private networks. Ericsson, for instance, scans their corporate network for child abuse material. They make their employees aware they are doing it, and tell their employees that if they are caught with this material on their computers or devices they will be reported to the police. "This is corporate best practice and I encourage all companies to do the same," says Moran.

However, smaller networks and developers do not always do so. "Your network will be abused by people with a sexual interest in children and children will take risks on your platform. Surely it makes sense for you to mitigate those risks using whatever methods you can," Moran continues. "Unfortunately the rush to market by start-ups leaves security as an afterthought. I would argue they should build safety and security into their products from the start."

The commercial sexual exploitation of children online has become less prominent in recent years. INHOPE hotlines, which enable the reporting of sites and images showing child abuse, law enforcement activity against organised crime, and a general reduction in spam have meant that many sites have been removed.

Credit card companies have also helped by refusing to allow their cards to be used on child sexual abuse sites. But new ways to pay, such as crypto currency and mobile payments, still present challenges.

Children having access to the internet gives them access to the world. It also gives the world access to children. "We as a society take a zero tolerance approach [to child sexual abuse] so there's no reason companies can't do the same," he concludes.

A DAY IN A LIFE

JENNY JONES
Sexual exploitation of children online: 'there will always be people who seek to misuse technology'

Meet Jenny Jones, director, public policy for GSMA, who works with mobile operators around the world to keep mobile services free from child sexual abuse content.

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.

Success, for me, is when we're all collectively asking 'what else should we be doing, how can we do this better?'

MY ROLE

I look after the GSMA's mYouth programme which focuses specifically on young people's use of mobile – promoting the many opportunities available to young people in today's digital society, but also working to proactively address potential risks. I also manage the GSMA Mobile Alliance Against Child Sexual Abuse Content which is made up of a group of mobile operators from around the world who are committed to working proactively to keep mobile services free from child sexual abuse content.

I am very committed to the idea that encouraging the safe and responsible usage of ICTs by young people, and preventing the misuse of ICTs by adults to exploit children, is only achievable when all stakeholders are engaged and playing their role. By all stakeholders, I mean industry, but also government and educators, law enforcement, child support services and specialist NGOs, as well as parents and carers.

MY IDEA OF SUCCESS

Success, for me, is when we're all leaning in and collectively asking "what else should we be doing, how can we do this better?" Globally, we are getting better at this kind of collaboration every year – so I guess that would be an example of what makes me happy.

How I imagine my profession in 10 year's time

I am, in many ways, very optimistic. Most parents in 10 years will have more or less grown up online – I think my generation is perhaps the last one to feel a distinction between our "real lives" and our "digital lives". So I like to think that the next generation of parents will feel more confident about engaging with their children's digital activities and guiding them on how to enjoy technology safely and responsibly.

> **SUCCESS, FOR ME, IS WHEN WE'RE ALL COLLECTIVELY ASKING WHAT ELSE SHOULD WE BE DOING, HOW CAN WE DO THIS BETTER?**

Equally, the internet has already proven its capacity to inform and engage people, both young and old, in ways that encourage us all to become active digital citizens using technology to change the world around us for the better. I think this trend will continue and become increasingly embedded in the next 10 years.

But of course, optimism must be tempered with pragmatism. When thinking of the sexual exploitation of children, we must assume that there will always be people who will seek to misuse technology. There will never be a moment when this problem is solved and anyone that signs up to contribute to this fight, must do so for the long haul. Technology will evolve, as will misuse of it – and we must continually update our response to combat misuse.

WHAT I THINK ABOUT COLLABORATION

Open dialogue is vital, as is accepting that no one party holds the key. We must work together to ensure that we're providing the best possible balance where children's rights appear to be in opposition – for example, between children's rights to privacy and information, and their right to be safeguarded – so that we can continue to promote opportunities and manage risks.

THE MAJOR PLAYERS

There are so many who are improving the lives of young people – including growing numbers of young people themselves! – and using technology as a tool. There is the mighty UNICEF, which uses the UN platform to advocate for children's rights in the widest sense, to small organisations like Worldreader who work with a very specific focus but with an overarching ambition of improving children's lives.

I'm also constantly humbled by colleagues working on the frontline in law enforcement and child protection services, including helplines and hotlines. They are fighting to uphold the rights of one child at a time, painstakingly and with great personal commitment, and collectively and gradually their work changes and informs how we all approach children's rights.

TOOLS AVAILABLE

There are so many great online tools and communities already in place for campaigning and raising awareness of issues. Organisations like Apps for Good are already going out there and encouraging young people to develop digital skills and use them to make the world a better place.

A DAY IN A LIFE

JOHN CARR

Ridding the internet of child pornography: 'Some of the work being done is hugely impressive.'

Meet John Carr, writer and consultant on children and young people's use of the internet and associated technologies.

John Carr is a leading expert on child online protection. He has advised the International Telecommunications Union (ITU), the European Union and several major high tech companies including Google and Vodaphone.

MY ROLE

My work now is all around strategic engagement in the realm of policy so it is often quite hard to see immediate benefits. Typically I am working with large institutions and companies trying to develop new ways to make things better for children in the online space. However, several years ago I was involved in a very practical project. We were working with severely disabled children. They had no ability to communicate verbally and could not write or draw anything. We adapted several digital devices. Working with highly skilled professionals, we taught the children how to use them to "talk" to their parents for the very first time in their lives. D-Day was a highly emotional experience. Many tears of joy were shed that day. It was semi-miraculous.

IN 10 YEAR'S TIME...

We will have resolved and settled the boundaries between voluntary self-regulation and state intervention in the digital sphere, at least in respect of companies' responsibilities to children. In terms of how companies and other stakeholders should work together to address challenges and opportunities, I think it should happen sincerely and on a playing field that is much more level than it is today.

THE LEADING CHANGEMAKERS OF TODAY

Some of the work that Google, Facebook and Microsoft have been doing of late in relation to ridding the internet of the evil of child pornography is hugely impressive. For example, Google deploys Microsoft's Photo DNA to detect still pictures of child sex abuse and they are developing a similar tool to facilitate the detection of child abuse videos. They have said – as with Microsoft's Photo DNA – that when it is ready for release it will be given away gratis. Also, in a growing number of countries (the UK was the first), they have introduced "splash pages" so anyone trying to use the search engine to seek our paedophilic content will get a warning that what they are doing is very likely to be illegal, then pointing them to sources of help if they wish to confront their sexual feelings about children.

WHY I REMAIN WARY

Not all children and parents are living in a society where civic institutions listen and respond or are interested in any kind of participation. The internet and its associated digital technologies do not guarantee any kind of progressive or democratic political change. On the contrary, there are lots of examples where digital technologies have been used to oppress citizens, not improve their lot.

“D-DAY WAS A HIGHLY EMOTIONAL EXPERIENCE. MANY TEARS OF JOY WERE SHED THAT DAY. IT WAS SEMI-MIRACULOUS.”

A DAY IN A LIFE

THOMAS MÜLLER
Online child abuse: 'If the internet was a city, we'd warn them about unsafe places'

Meet Thomas Müller, head of policy and research, Child Helpline International.

Thomas' department focuses entirely on collecting, analysing and raising awareness of the stories children tell when they contact child helplines. Listening to what they say can help

At Child Helpline International, everything we do is based on the Right to be Heard, which is enshrined in the United Nations Convention on the Rights of the Child. Child Helpline International is one of the world's largest collective impact organisations, a network of currently 183 child helplines from 142 countries. Collectively, child helplines respond to more than 15 million contacts every year from children and young people in any emergency situation, when no one else is there to listen or help.

MY ROLE

I lead the policy and research department, where we focus entirely on collecting, analysing and amplifying the stories children tell when they contact child helplines. I sit on a gold mine of information, which gives unique insights into the situations children find themselves in.

It is really quite sobering when you have a closer look at these stories. Every second, somewhere around the world, a child tries to contact a child helpline and every third of these contacts deals with issues related to violence, neglect and various forms of physical, emotional and sexual abuse. And many do mention the internet playing a central role in this.

WHAT MOTIVATES ME

Despite the huge number of contacts we receive, in many countries only very few children know that a child helpline exists while others do not have the means to get in contact. Others haven't yet found the courage to talk and some might not even know that what is happening to them is wrong.

For that reason, the work my department does is so fundamentally important. We use the information provided and pass it directly to those who can make decisions that strengthen support and protection for all children. I have seen the difference our work makes in the lives of children and have personally talked to many who said that if it wasn't for a child helpline they are not sure if they would still be alive. Of course, I sometimes feel angry and appalled by what we allow to happen to our children but I take a lot of motivation and energy out of the absolute conviction I have that my work benefits so many of them.

HOW I SEE MY PROFESSION IN 10 YEARS TIME

With the speed at which technologies develop, it is difficult to even predict the next two years and we have to acknowledge that there are, have been and always will be people who try to take advantage of children for their own interests and pleasure. Technology can be utilised to empower children and give them a voice, but it also plays a crucial role in child abuse. If we can collaborate more to tackle problems globally and raise more awareness, especially among children, the work we will do in 10 years will be more efficient, more successful and will protect many more.

> **IF I WAS A DEVELOPER, I WOULD PROBABLY TRY TO CREATE A STRONG PROTECTIVE WALL BETWEEN THE DARK WEB AND THE ONE THAT OUR CHILDREN USE EVERY DAY.**

MY VIEWS ON COLLABORATION

I am a huge believer in collaboration. Often companies are simply not aware of a certain problem and are happy to collaborate if the issue fits their strategy and they feel they can make a difference. Governments, law enforcement, INGOs and civil society also all play a role in this effort. Governments should reward corporate activities and investments that are beneficial for child online protection. Civil society should look for win-win collaborations with the private sector and not for a confrontational approach by naming and shaming. We all need to take on this challenge together.

WHY WE ALL NEED TO BE MORE PROACTIVE

Just like with all other forms of abuse though, online sexual exploitation or cyberbullying are not virtual but real events in a child's life. And like with all other forms of abuse, the majority of the perpetrators can be found within the closer and extended family, people with quick and easy access to the child. I know this because children tell us. So by simply providing parental advice and control tools we are not doing well enough in protecting children.

No one has a greater interest in children being safe online than children themselves. For me, they have to be the leading change makers and we all need to empower them by educating them and raising their awareness about online risks, their rights, ways to reportproblems and support available. We need to help them to protect themselves. Whenever child abuse material is out there on the net, it is very likely that it stays there forever, or at least as long as the internet is governed, regulated and managed as it is at the moment. So rather than being reactive, I think we should be proactive and prevent bad things from happening to children by making them safe and confident users of the web.

PROVIDING A CREATIVE SOLUTION

If the internet was a city, we would explain to children where to go and where not to go, that there are good and bad places, that there are safe and unsafe places, and that at times it can be very scary. We would hold their hands when crossing the streets, we would know which movies they watch when they go to the cinema and we would definitely have an eye on who they are talking to and what they are talking about. With the internet however we often just let them walk and find out for themselves. So I would love to provide a creative solution that takes on the role of the well-intended, protective parent for children online for example an avatar superhero that is a child's best friend as they start exploring the online environment.

I also personally find it quite frightening that there is such a place as the dark web. If I was a developer, I would probably try to create a strong protective wall between the dark web and the one that our children use every day.

The tools being used in Latin America and the Caribbean to protect children online

by Vikki Knowles

In Latin America and the Caribbean, few acts of violence or abuse against children are investigated but various innovative initiatives for support and guidance are being developed to change this.

Many children around the world use digital tools in their everyday lives. And the use of mobile phones continues to grow – with nearly two-thirds (65%) of children between the ages of 8 and 18 now using one. This connectivity is enriching young people's lives – but it also means increasing accessibility to the internet, which can compromise children's safety, both online and off.

While children have always been exposed to violence and abuse - and ICTs are not in and of themselves harmful, they have changed the opportunity, scale, scope, form and impact of violence against children.

In the online world, some of the risks children face include invasive forms of bullying and harassment; posting of highly personal information including sexualised images/ videos; new opportunities for adults to prey on the vulnerability of children for sexual solicitation ("online grooming"); child sexual abuse material and user-generated content.

And many more instances of violence against children go unheard. In Latin America and the Caribbean particularly, few acts of violence or abuse against children are investigated and in those that are, the perpetrators are rarely held accountable. Over 200,000 children contacted helplines in 2012 and 2013 in the region, according to Child Helpline International. In 19% of cases, children requested help in suspected cases of violence or abuse.

Research (pdf) from UNICEF shows that children move seamlessly between the online and offline world; the distinction between these environments has increasingly become meaningless. They are often first adopters of new technology and this makes them particularly vulnerable. So what role does technology play in protecting children online and off?

Prevention is key and starts in homes. In the same way that we prepare children to move independently in the real world we need to prepare them to meet the online world. Prevention is not prohibition, but we need to educate, dialogue with and orient children in order to create resilience against constantly evolving threats in online and offline environments.

Collaboration across sectors, with governments and through public-private partnerships, is also very important. On a global scale, one such example isWeProtect, a worldwide alliance led by the UK government and supported by 50 countries, 30 NGOs and 20 leading technology companies to tackle online child sexual abuse and exploitation.

SOME US TOOLS

In Latin American and the Caribbean, some multi-stakeholder, innovative solutions have been built around the use of technologies.

In major Brazilian cities, Proteja Brasilallows users to anonymously report cases of violence. The app uses location data to provide telephone numbers, addresses and best routes to access organisations that help protect children, such as police stations and protection counsels.

Another mobile app in Costa Rica, Empodérate, educates children on their rights and enables them to report abuse, request information and contact emergency services. There's also the Ananda alert which is Jamaica's version of the US Amber alert. This system is designed to work with public and private sectors, civil society and communities to help law enforcement quickly find missing children. It also allies with communication networks and media houses to publicise information on both missing and recovered children.

Meanwhile, ECPAT (End Child Prostitution, Child Pornography and the Trafficking of Children for Sexual Purposes) develops technical tools for police, immigration officials, and other NGOs to help battle sexual exploitation of children in the region. The NGO also researches the roots of the problem in order to design targeted interventions, and as a global network, supports collaborative action.

THE ROLE OF THE PRIVATE SECTOR

In the private sector, the GSMA – which represents the interests of mobile operators worldwide – has been working closely with UNICEF to promote the Child Online Protection (COP) guidelines within the entire mobile ecosystem.

The guidelines provide advice on how industry, educators and policymakers can ensure children's safety in the digital era. Partnering too with the International Centre for Missing and Exploited Children (ICMEC), Interpol, International Association of Internet Hotlines (INHOPE), and other corporate allies, they are supporting multi-stakeholder engagement and training – such as workshops and webinars – to provide practical support on implementing these guidelines throughout the region, in support of a more coherent and coordinated response.

"We have been travelling around different countries in Latin America to get policymakers, industry representatives and NGOs around the same table to talk about best practices, form alliances and agree on the next steps required in each country to best protect child rights," says Mauro Accurso, communications and sustainability manager for Latin America at the GSMA.

Technology companies in particular have an important responsibility in tackling this issue, as it is through their networks and services that child sexual abuse content is circulated. Creating and promoting hotlines ensures that offensive content is blocked and deleted faster. Countries like Peru and Colombia already have advanced blocking systems in place, and other countries are not far behind.

The GSMA's WeCare campaign supports initiatives that enable the mobile industry to protect children in countries across the region. "For example, Costa Rican mobile operators made the national child helpline toll free; it is a simple step but it makes a huge difference for abused children trying to reach the helpline," Accurso says.

In the digital realm and beyond, everyone has a role to play in protecting children - whether that's ensuring there's no child labour within the supply chain, or safeguarding the children that use a company's services. "If you take a mining company in Bolivia and a telecoms company in Costa Rica, they touch the lives of children in a different way," says Stefan Stefansson, regional chief of partnerships at UNICEF. "But the basic principles are the same, and we really want to promote the idea that everybody is responsible for protecting the lives of children."

There are three steps to this approach, Stefansson explains. The first is for companies to ensure that they don't have practices that harm children or violate their rights. "Then it's about looking at their environment, their customers, and looking at the families of their staff and expanding the circle a little bit." The third step is for them to advocate for children in general, to impact not only their business, but society as a whole. As the COP guidelines note: "the internet knows no boundaries, and our efforts to protect children must be ambitious and far-ranging."

Bitcoin and darknet are making it harder to track online child abuse

by Tim Smedley

Tracking payment with the help of PayPal and Visa has helped catch paedophiles but anonymous technologies make this harder. It's time financial institutions did more.

Dutch child rights organisation Terre des Hommes put a fake picture online in 2013 of a 10 year-old girl purporting to be available for sexual activity. Known as "operation Sweetie", potential abusers were asked to make a $20 (£14) online transfer.

In just 10 weeks, more than 1,000 paedophiles in 71 countries were caught by the sting. While few arrests were made because the operation could be deemed to be entrapment, the experiment showed how online payments could track paedophiles.

Tracking the flow of money in the industry is a critical tool in efforts to stop online child abuse, but is a tactic that is becoming increasingly hard due to anonymous currencies and less traceable parts of the internet.

Ten years ago, it was common for individuals to use credit cards to access graphic commercial child abuse websites. To tackle this, the Financial Coalition Against Child Pornography (FCACP) was set up in 2006 in the US. Spearheaded by non-profit the International Centre for Missing & Exploited Children (ICMEC), it brought together leading names in the financial industry including American Express, HSBC North America, MasterCard, Visa, Standard Chartered and PayPal – together making up 90% of the US payments industry.

"The approach was to follow the money on the merchant side of the transaction, not the consumer side", says Cathy Cummings, senior director of ICMEC. To track down sellers, FCACP members donated credit cards which law enforcement agencies used to purchase illegal material. Working with the credit card companies, they could identify the processors and the acquiring banks that had the child pornography merchants on their system.

THE RISE OF ANONYMOUS PAYMENTS

However, the problem hasn't gone away. The use of personal credit cards and bank accounts to pay for content is now rare, but the trade has simply moved to alternative digital currencies, such as Bitcoin, and other anonymous forms of payment.

According to figures reported by the European Coalition Against Sexual Exploitation of Children Online (EFC) a total of 5,236 URLs suspected of commercial child sexual exploitation were reported in 2013. While the EFC says data is still being collected, it says this number has been growing over the past three years.

This new world has made it harder to target abusers through their financial transactions and, say campaigners, puts an onus on the financial industry to do more. "The [child sexual abuse] industry is growing at a very fast pace and the technology that offenders are able to use is growing as fast", says Bharti Patel, chief executive of child exploitation charity ECPAT UK. "If there is a concern and a genuine interest in addressing this and protecting children, then all players need to ensure it is stopped."

The financial industry has faced criticism for its sale of prepaid credit cards, which sometimes don't require customer identification. While providers such as Visa Europe claim all their cards generate trackable data, others are not so stringent. According to John Carr, chair of the Children's Charities' Coalition on Internet Safety: "Some card suppliers do little to disguise their lack of interest in what you do with their cards once you have bought them."

While prepaid cards are at least regulated to some extent in the US and UK, alternative online currencies such as Bitcoin, and marketplaces on the darknet and Tor, are not.

According to Olivier Burgersdijk, head of strategy at the European Cybercrime Centre, Europol, there is not much the mainstream financial industry can currently do but he's hopeful that traceability will improve: "Bitcoin's underlying 'blockchain' technology records all transaction in a searchable and unalterable public ledger ... criminal transactions that are difficult to trace nowadays may be detected in the future as Bitcoin tracing technology develops."

There has been some success in following Bitcoin transactions, with an Italian police investigation into child abuse images seizing 14,000 Bitcoin wallets worth around €1m (£800,000) in 2015. But it's the tip of the iceberg. For Patel, it's "a cop out" to claim that alternative payments or technologies are too hard to trace and out of reach of the global financial industry: "The Modern Slavery Act in the UK clearly stipulates child sexual abuse and online grooming as part of the modern slavery definition. This must be seen as part of any business's responsibility to address ... Technology has moved fast, but have we kept up- to-date with that?" The abusers certainly have.

What more can the tech industry do to protect children's safety online?

by Vicky Knowles

Tools for tracking and reporting offensive images and video are being adopted but differing legislation between countries makes a joined-up approach difficult

The issue of child sexual abuse material (CSAM) is a global one. 1.8bn photos are uploaded onto the internet everyday, some 720,000 of which are illegal images of children, and technology is making it easier to access and distribute this material.

So what measures does the tech industry have in place to ensure children's safety online, and what is their future potential? The most cited example is Microsoft's Photo DNA, the use of which is now considered best practice in fighting child exploitation online. Photo DNA - which was originally intended for internet service providers - helps track images of child sexual abuse by using an algorithm to create a unique signature, or fingerprint. This allows the technology to reliably identify copies of the image even if photos are marginally changed.

Since 2012, Photo DNA has been available to law enforcement around the world. This has helped government agencies speed up their investigations, allowing them to quickly identify both the victims and criminals, as well as limiting officer exposure to the offending images. And it's now been implemented by Bing, SkyDrive, Facebook and chat network Kik. The US-based National Centre for Missing and Exploited Children (NCMEC) creates Photo DNA signatures of illegal child abuse images and shares these with US online service providers to help reduce the proliferation of child pornography online.

But social media companies have been criticised for not taking online safety seriously. In this open letter to Facebook from the NSPCC earlier in the year, it's clear that offending material is not taken down quickly enough.

Social media companies like Facebook also need to consider the right to freedom of expression. In the past, the context within which disturbing material is presented has been important - if users are raising awareness, it can be viewed with a warning screen, but if the content is shared and encouraging the behavior, it is taken down.

From this year, Microsoft has offered its software as a free cloud-based service, making it available to smaller companies and organisations. Previously, only businesses that had the money and expertise to host the software and keep it running were able to use it.

Are there any other costs associated with Photo DNA? The Internet Watch Foundation (IWF) charges members a subscription service of £1,000 - £75,000, depending on the size of the organisation. The fees enable companies to take advantage of services like takedown notices, a hash list and a URL list. It also allows organisations to link up with others globally that are working to protect children online.The IWF uses MD5 and SHA-1 along with Photo DNA, but these technologies fail to capture much of the content. According to a 2013 study, other software did not find 98.7% of matches identified by Photo DNA.

WHAT ABOUT VIDEO?

At the moment, Photo DNA hashing is limited to images only. If it is the go-to tool for tracking offensive images, is there an equivalent for combatting video material? Google has developed a Video ID tool for identifying child abuse videos, and the IWF says it's working closely with one of its members to develop video hashing software.

Video Fingerprinting Technology, by UK tech firm Friend MTS, is another example of such software. It works in a similar manner to photo hashing, generating unique fingerprints of video clips, allowing offensive material to be filtered and blocked quickly. Friend MTS donated the technology to the International Centre for Missing & Exploited Children (ICMEC) last year, and it's now used by commercial entities and law enforcement.

Friend MTS CEO Jonathan Friend says the role of technology in tackling CSAM is extremely valuable. "It's very important to be able to use technology to ensure that material is identified quickly." So, could the software potentially be used as widely as Photo DNA? "Absolutely."

THE MULTI-STAKEHOLDER APPROACH

But technology itself is still somewhat powerless without multi-stakeholder participation and cooperation. As Baroness Joanna Shields said at the #WeProtect Children Online Global Summit last December, perpetrators are always finding new ways to evade technological solutions with new tools, which is why cooperation "between industry, law enforcement, non-governmental organisations (NGOs) and government" is required.

There are already existing examples. Project VIC is a collaborative effort between ICMEC, law enforcement and industry, and uses both Photo DNA and Video Fingerprinting Technology to streamline their investigations. There are thousands of users in 26 countries including the US, a sample of whom reported that the participation in the project has resulted in 250 victims and over 125 offenders being identified.

With these technologies available for free, there's no reason they shouldn't be used widely. But legislation facilitates the use of technology to fight CSAM, and it differs from country to country. As Fernando Ruiz, head of operations at Europol's European Cybercrime Centre (EC3) notes, "…we need sophisticated international response to stop the abuse. To achieve this, all countries need first to build up their national response to this crime."

For example, artificially created images are an area of dispute - if it doesn't contain a real child, is it still CSAM? In the UK and Canada for example, it is. Meanwhile, in 2010, the ICMEC found (pdf) that only 45 of the 196 countries reviewed had sufficient legislation in tackling CSAM offences, with 89 having no legislation that specifically addressed child pornography at all. That said, most countries (pdf) have hotlines run by a non-governmental organisation for reporting the material, which in turn will inform the internet service providers concerned. In most countries, ISPs will take it down once being alerted to it.

Though technology only addresses the identification of existing material, representing only part of the problem, the investigation it may prompt can only be positive. Jacqueline Beauchere, chief online safety officer at Microsoft, says in a blog that developing technology for this purpose is increasingly necessary. "Industry needs to continue to innovate with new tools and techniques to disrupt the spread of CSAM."

© UNICEF/UNI157767/Mawa

A DAY IN A LIFE

KATIA DANTAS
Eradicating child abuse: 'stop seeking easy, quick-fix solutions'

Meet Katia Dantas, policy director, The International Centre for Missing and Exploited Children (ICMEC).

Katia works to protect children throughout Latin American and the Caribbean, with a particular focus on technology-facilitated child sexual abuse and exploitation

ICMEC is a non-governmental, non-profit organization working to make the world a safer place for all children by eradicating child abduction, sexual abuse and exploitation. It is headquartered in the United States, with regional representation in Brazil and Singapore.

Since its inception in 1998, ICMEC has trained over 7,500 law enforcement officers from more than 115 countries; worked with governments in more than 100 countries to refine or implement laws against child pornography; increased global participation in International Missing Children's Day; and created a 24-member Global Missing Children's Network.

MY ROLE

Since January 2011, I've been working as ICMEC's policy director for Latin America and Caribbean to identify gaps in legislation and policies related to missing and abducted children, as well as on technology-facilitated child sexual abuse and exploitation, assisting with finding solutions to enhance the protection of children throughout the Latin American and Caribbean region.

Aside from being an integral part of ICMEC's vision and mission, protecting children online is something I hold dear and near to my heart. One thing that particularly frustrates me is the demonization of technology or the search for simple one-size-fits-all solutions to child online protection. The internet, is a tool that has sadly been abused in some aspects, but banning technology is not the solution.

With that in mind, I've worked throughout the years to build upon ICMEC's expertise and its regional contacts to promote the creation of alliances to enhance child online protection in a comprehensive way, having recently launched the Latin America Coalition Against Technology-Facilitated Child Sexual Abuse (CLAC).

The ICMEC has also supported several other initiatives in the region, and recently partnered with Unicef LACRO on the development of a series of regional events to bring awareness to the risks and benefits of the digital era. For me, it is critical to seek the balance between seizing all the benefits technology brings us, with a safer and responsible use of those tools.

HOW I IMAGINE MY PROFESSION IN 10 YEAR'S TIME

Technology has been advancing in such a way that making any predictions on where we will be is extremely daunting. I still remember when the first mobile phone was launched and how huge and cumbersome it was to carry it around. The smartphones we carry everywhere today are far better and faster than any computer from 10 years ago. And the number of people, especially children, who utilize these technologies is already incredible and will only continue to grow.

Despite the gloomy scenario painted by the current risks children face online today, I believe the future holds a great deal of hope. I believe we will reach a point where digital literacy is more widespread and the current digital divide we see in so many places is reduced. That for me is a key component of child online protection. The more we learn about technology and the more we learn to respect each other online, the more children will be protected in the future.

MY VIEWS ON COLLABORATION

It is paramount that we stop seeking easy, quick-fix solutions. Increasing partnerships and convening stakeholders at the international, regional, and local levels is critical to find targeted and comprehensive solutions for such a complex issue.

One big barrier to effective coordination is the lack of harmonized legislation internationally and the lack of appropriate policies and responses in many countries (particularly developing countries) to properly deal with the use of technology to abuse children. ICMEC has been working on promoting more effective legislation across the world through research-based advocacy and capacity-building and we are glad to see others join our fight. We have seen efforts from big internet service providers (ISPs) in creating new security features and investigation tools, but there is still a lot other companies can do to protect children.

We still see some companies develop independent solutions for prevention and safety, which may lead to fragmented responses that reach just a few users. If other companies joined the existing global and regional coalitions (Financial Coalition Against Child Pornography, Latin America Coalition Against Technology-Facilitated Child Abuse, Technology Coalition and others) we could maximize the amount of resources as well as the impact on the final user.

WHO I CONSIDER A LEADER IN THIS AREA

ICMEC! Seriously speaking, it is humbling to see on a daily basis that we are not alone in advancing children's rights in a digital world. Being a complex issue, we need all hands on deck and as many champions as we can to further this cause.

We have been lucky to partner with amazing organizations that have made significant strides in this regard, such as Unicef, the International Association of Internet Hotlines, the Groupe Speciale Mobile Association, the International Telecommunication Union, the International Criminal Police Organization, particularly their regional offices in Buenos Aires and San Salvador, and so many others.

We are particularly glad to see the increased interest and advocacy of the British government towards a protected childhood online (#WeProtect) and to see so many key actors, such as the Office of the UN Special Representative on Violence Against Children – Marta Santos Pais – designating violence online as a key topic to be addressed in 2016.

Regionally, we have gladly seen momentum for child online protection and have welcomed the increased attention from regional bodies (such as the Organization of American States, and the Inter-American Institute of the Child) and great networks such as Red NATIC. It makes us very hopeful for a better future.

THE APPS OR PROGRAMS I THINK WOULD BE USEFUL

I think there are great apps and programs already in place. I would love to see a portal of the different initiatives that are available consolidated and translated into different languages and different realities. Most importantly, I hope to see the continued development of new programs, apps, and technologies that can be used as tools to raise awareness and protect children in an online environment.

A DAY IN A LIFE

AMY CROCKER
Preventing spread of child sexual abuse material online: 'we're not powerless'

Meet Amy Crocker, hotline development coordinator, INHOPE Foundation.

Amy supports the development of internet hotline initiatives, working with them to develop capacity and become members of the INHOPE network, which works to stop the (re)circulation of child sexual abuse material on the internet.

INHOPE is a member-led network of 51 internet reporting hotlines in 45 countries worldwide. Together with industry partners, INHOPE members take action to stop the (re) circulation of child sexual abuse material on the internet while providing actionable intelligence to law enforcement which may lead to the arrest of offenders as well as the identification and rescue of child victims. INHOPE also provides support through its charitable arm, the INHOPE Foundation to start up internet reporting hotline initiatives around the world.

MY ROLE

My main role is to support the development of internet hotline initiatives around the world, working with them to develop capacity and eventually become members of the INHOPE network. To do this, I work closely with and rely on everyone in the team at INHOPE as well as with INHOPE member hotlines to promote and share the specialised technology, training and cooperation that underpin and drive our organisation. I provide technical support and act as a bridge between organisations that want to set up a hotline (but often lack the funding, specialised knowledge, political support or even legislation to do so), and the people and organisations in our network that are best placed to help them.

WHAT MAKES ME HAPPY IN MY WORK

I'm happy when I see this direct support in action, and when the collective of organisations working in this field achieve genuine cross-fertilisation of ideas, processes and activities. And I don't mean this in an abstract way, rather, the work that INHOPE and its member hotlines do is contributing in diverse but concrete ways to the reduction of online victimisation and to the identification of the children depicted in this material every day around the world. Apart from the very serious nature of the topic we work on, it can sometimes be frustrating when this type of cooperation takes longer than expected to take shape. However, the positives of what has been achieved in recent years far outweigh the negatives. Success is as much about the journey as the destination!

IN 10 YEAR'S TIME...

If the last 10 years are anything to go by, the landscape and the way we operate will of course be very different in 2025.

INHOPE and its member hotlines will inevitably adapt to evolutions in the use and misuse of digital technology and the internet, and to changes in the legislation and governance environment that defines how they can operate. In the coming years, we also need legislation on this issue to move forward all around the world, and adapt faster to keep up with technology.

The average internet user in 2025 will be more tech-savvy and connected than today, and the effects of the amazing prevention and education work being done today will be seen in the way children and young people are taught to protect themselves online. But as connectivity and the sheer volume of content being shared increases, it will remain crucial to ensure that every internet user knows where and how to make a report in a safe, secure, transparent and accountable way.

However developed the technology and processes to respond to this and other online issues become, what I really hope for in the coming decade is an increase in society's understanding and acceptance of the prevalence and complexity of child sexual abuse as part of society, all around the world and regardless of culture.

Those in my field will continue to play a specific but important role in encouraging dialogue about online child sexual exploitation and abuse, and will continue to provide trusted reporting mechanisms around the world for the public to report their concerns.

Of course I would like to predict that the world of 2025 will be so evolved as to have no need for this field of work. However, while there is child sexual abuse material being produced and circulated online, INHOPE will continue to play its role in coordinated efforts to stop circulation and prevent re-victimisation.

MY VIEWS ON COLLABORATION

Multistakeholder cooperation is essential, and success will be when each actor has a clear but adaptable role within the response ecosystem. The many challenges and opportunities should not be placed into siloes. If an internet hotline organisation can support law enforcement and industry partners, or industry can help law enforcement solve a technical challenge , or if law enforcement can help internet companies respond to challenges posed by misuse of their services, then they should be able to do so. The good news is that all of this is already happening. Naturally, there is always more we can do. We must continue to work together to anticipate and interpret trends, keep on top of the technology curve, and educate policymakers and the public to these new challenges and their role in child online protection.

THE LEADING CHANGEMAKERS

Aside from the INHOPE member hotlines that are driving the agenda in their countries every single day, the leading changemakers for me are all of the individuals and organisations around the world striving to put and keep this issue on the agenda, developing technologies that respond to very real challenges, or going the extra mile to identify the real child behind every child sexual abuse image or video. INHOPE works closely with numerous partners such as GSMA, UNICEF and the ITU to promote child online protection, with a number of partners through the #WePROTECT initiative, with expert civil society organisations such as ECPAT International and the International Centre for Missing and Exploited Children, with a wide range of large and small technology companies, and with Interpol, Europol, the Virtual Global Taskforce and many national law enforcement agencies around the world.

WE ARE NOT POWERLESS

INHOPE works hard to increase visibility of the issue by supporting existing and start-up internet reporting hotlines that work with digital citizens and encourage civic participation. INHOPE and its member hotlines work closely with the safer internet community at large and within safer internet platforms. In the context of the European Union, for example, INHOPE has a long-lasting and flourishing partnership with its dynamic consortium partner Insafe.

If I can leave only one message with everyone, it is that they are not powerless in the face of online content that they suspect represents the sexual exploitation of a child. If they see it, they can regain control and report it to their national internet hotline for expert assessment. In the UK for example, the public can report to the Internet Watch Foundation. Links to all our members around the world are available on INHOPE's website.

03 Chapter 03
Creating a safer and age-appropriate online environment

INTRODUCTION

Very few things in life can be considered absolutely safe and risk free all of the time. Even in cities where the movement of traffic is highly regulated and closely controlled, accidents still happen. By the same token, cyberspace is not without risks, especially for children. Children can be thought of as receivers, participants and actors in their online environment. The risks that they face can be categorized into three areas:[11]

• Inappropriate content – Children may stumble upon questionable content while searching for something else by clicking a presumably innocuous link in an instant message, on a blog or when sharing files. Children may also seek out and share questionable material. What is considered harmful content varies from country to country, yet examples include content that promotes substance abuse, racial hatred, risk-taking behaviour or suicide, anorexia or violence

• Inappropriate conduct – Children and adults may use the Internet to harass or even exploit other people. Children may sometimes broadcast hurtful comments or embarrassing images or may steal content or infringe on copyrights

• Inappropriate contact – Both adults and young people can use the Internet to seek out children or other young people who are vulnerable. Frequently, their goal is to convince the target that they have developed a meaningful relationship, but the underlying purpose is manipulative. They may seek to persuade the child to perform sexual or other abusive acts online, using a webcam or other recording device, or they will try to arrange an in-person meeting and physical contact. This process is often referred to as 'grooming'

Online safety is a community challenge and an opportunity for industry, government and civil society to work together to establish safety principles and practices. Industry can offer an array of technical approaches, tools and services for parents and children. These can include offering tools to develop new age-verification systems or to place restrictions on children's consumption of content and services, or to restrict the people with whom children might have contact or the times at which they may go online.

Some programmes allow parents to monitor the texts and other communications that their children send and receive. If programmes of this type are to be used, it is important this is discussed openly with the child, otherwise such conduct can be perceived as 'spying' and may undermine trust within the family.

Acceptable use policies are one way that companies can establish what type of behaviour by both adults and children is encouraged, what types of activities are not acceptable, and the consequences of any breaches to these policies. Reporting mechanisms should be made available to users who have concerns about content and behaviour. Furthermore, reporting needs to be followed up appropriately, with timely provision of information about the status of the report. Although companies can vary their implementation of follow-up mechanisms on a case-by-case basis, it is essential to set a clear time frame for responses, communicate the decision made regarding the report, and offer a method for following up if the user is not satisfied with the response.

Online content and service providers can also describe the nature of content or services they are providing and the intended target age range. These descriptions should be aligned with pre-existing national and international standards, relevant regulations, and advice on marketing and advertising to children made available by the appropriate classification bodies. This process becomes more difficult, however, with the growing range of interactive services that enable publication of user-generated content, for example, via message boards, chat rooms and social networking services. When companies specifically target children, and when services are overwhelmingly aimed at younger audiences, the expectations in terms of content and security will be much higher.

Companies are also encouraged to adopt the highest privacy standards when it comes to collecting, processing and storing data from or about children as children may lack the maturity to appreciate the wider social and personal consequences of revealing or agreeing to share their personal information online, or to the use of their personal information for commercial purposes. Services directed at or likely to attract a main audience of children must consider the risks posed to them by access to, or collection and use of, personal information (including location information), and ensure those risks are properly addressed. In particular, companies should ensure the language and style of any materials or communications used to promote services, provide access to services, or by which personal information is accessed, collected and used, aid understanding and assist users in managing their privacy in clear and simple ways.

Collaborating to make the digital world a safer one for children

by Gerrit Berger

Cross-sector collaboration can empower young people to harness online opportunities and stay safe in the digital world

In recent years, the mushrooming of feature phones and affordable smartphones, coupled with flexible pre-paid schemes and growing broadband availability has resulted in millions of new internet users from developing and middle-income countries. This growth has, of course, gone hand-in-hand with major expansion by international companies in emerging markets. News in the financial sector has been full of reports of increased presence and investment in Africa and other regions by technology and telecommunications giants including Microsoft, Intel, IBM and Google.

For UNICEF, understanding this explosion has been paramount, as children and young people have been leading the uptake in access to digital. Since 2010, through the Voices of Youth Citizens initiative, UNICEF and its partners have been examining the opportunities and risks that the digital explosion presents for children's rights, and advocating for safe and responsible use.

One of the recurring realities in a number of countries is that not only are children and youth the greatest users of digital tools, in many cases they learn how to use them with very little support from parents or teachers. A study conducted by UNICEF Argentina showed that almost two-thirds of children surf the internet unsupervised, while a study exploring the digital habits of adolescents in Kenya found that only 15% of respondents had learnt to use the internet from their parents. In many cases parents, caregivers and teachers do not feel they are sufficiently equipped to provide guidance to their children as they discover the digital world.

11. Livingstone, S., and L. Haddon, 'EU Kids Online: Final report', EU Kids Online, London School of Economics and Political Science, London (EC Safer Internet Plus Programme Deliverable D6.5), June 2009, p. 10.

In this context it is clear that there is a very significant role that private sector can, and should, play in helping to raise awareness of safe and responsible use of digital tools, and to empower young users to negotiate the online world safely. This also presents exciting opportunities for collaboration between the private sector, child-rights organisations such as UNICEF, and governments, to use evidence to design outreach and campaigns based on a common understanding that with the right support structures in place, the benefits of the digital world outweigh the risks.

And there are already effective examples of this from around the world. In 2012, UNICEF South Africa partnered with Google South Africa and other governmental and non-governmental agencies to localise Google's online family safety centre to meet the country's realities.

More recently, UNICEF Argentina, in partnership with Fibertel corporation, Cablevision and NGO Chicos.net, launched an online portal, Compas para el uso de internet, with resources for teachers, parents, and children to equip them with tips and advice to maximise the online experience, and a game which helps children to evaluate their online behaviour.

In Ukraine, UNICEF has partnered with top digital agency Smartica/Skykillers and the country's largest social network, VKontakte, to design and implement a campaign aimed at the young users of the social network. An interactive application and video engages users and promotes critical thinking on issues of online reputation and personal safety. On a global level, through the Voices of Youth online community, UNICEF shares resources and tools to galvanise children and young people to promote digital citizenship among their peers, recognising the important role that children themselves can play in protecting themselves and their friends online.

As more and more young people connect online, we need to work together to ensure that not only are they aware of how to reduce their risk of harm online, they are fully empowered to take advantage of the opportunities that the digital world offers for their education, development and civic participation.

Drug dealers using Instagram and Tinder to find young customers

by Leah Borromeo

Now you can swipe right for #mephedrone as dealers branch out to social media sites popular with young people

Drug dealers are branching out to platforms and apps, popular with young people, such as Instagram, Tinder, Kik and shopping app Depop to sell their wares. These can be anything from prescription medication and research chemicals to recreational drugs.

The process is simple. On Instagram, using the social platform convention of hashtagging, a potential customer trawls through the app looking for phrases like #weed4sale or the names of the drugs themselves (#mdma, #mephedrone etc). The customer then contacts the owner of the account and the deal moves along through direct messages. In the case of Tinder, potential customers can swipe through profiles until they find a dealer and match with them.

Buyers can either meet face-to-face or pay online and have their purchases posted to them. While online payments such as bitcoin and pre-paid gift cards such as Vanilla Visa are encrypted, more traceable measures such as unattributed bank transfers and PayPal are also used. Online dealers mostly sell their drugs as "research" even though pills are put in bottles or blister packs and powders in capsules."Despite packaging them specifically for human consumption, vendors attempt plausible deniability when it comes to what they sell," says Moe, a former user who bought legal and illegal drugs online from the age of 16.

There are few firm statistics about who's buying drugs over social media but interviews I did suggests young people are a market. Despite the risks – which include getting scammed, getting caught and having no guarantee about strength or composition of drugs – Moe says the internet is popular among teens who have no personal connections to drug dealers and users. In particular, he says, research chemicals that are legal for medical or clinical trial purposes are being bought online by teenagers who don't otherwise have access to illegal drugs.

Not everyone who buys drugs online is doing it to get high. I have spoken to young people in the LGBTQ community who buy hormones for gender transitioning online because it bypasses restrictions and bureaucracy in the NHS.

"The system doesn't guarantee what trans people need, and illegal underground behaviour becomes the way to get it, which in turn sustains systemic problems," explains sociologist Bilal Zenab Ahmed.

WEEDING OUT OFFENDERS

As far as possible, social media providers act swiftly to block or restrict links that could lead to the sale or purchase of drugs, and repeat offenders are banned, but the onus is on platform users.

"Promoting the sale of, or selling marijuana and other drugs is against our community guidelines," says an Instagram spokesperson. "We encourage anyone who comes across violating content to report it via our built-in reporting tools."

Anonymous mobile chat app Kik says it doesn't "tolerate any illegal activity" and "cooperates with law enforcement requests when appropriate". It says it will shut the accounts of users when misuse comes to its attention.

Despite an explicit and extensive list of prohibited items, vendors on the popular buy-and-sell network Depop have still managed to list prescription drugs like ritalin or dexamphetamine, and unlicensed "smart drugs" like modafinil. Depop says it has a no-tolerance rule to restricted sales and reacts immediately when it identifies or is alerted to items or activities against its guidelines.

Tinder was contacted for comment but hasn't responded. The common thread is that these social platforms and websites rely on their millions of users to report inappropriate content. Even the police rely on reporting from the public, encouraging people to contact their local force or the cybercrime unit if they see suspicious behaviour on the internet.

Until image detection technology is sophisticated enough, vetting images before they are uploaded would be highly resource intensive and counterintuitive to a social platform selling itself on being instant or quick.

CRACKING DOWN ON ONLINE DEALING

After being in and out of the justice and rehab system for a number of years since the age of 17, Moe says that arrests for drugs bought online tend to happen separately to the initial transaction. "You get the drugs, then you do something stupid with the drugs on you, or you sell them in person," he says.

Cracking down on online drugs transactions has proved difficult. "The digital world has transformed the availability and threat of harmful drugs and we must adapt to these challenges," says a National Police Chiefs' Council spokesman. "Forces are committed to reducing the harm caused by drugs but cannot do this alone; prevention, education and health services all have a crucial role."

Karen Bradley, the UK's minister for preventing abuse, exploitation and crime, says government and law enforcement agencies take the unlawful advertising and sale of drugs on the internet seriously. She says: "We continue to work with internet providers to ensure they comply – this can include closure of UK-based websites where they are found to be committing offences."

The legislation used to protect children's privacy online: is it effective?

by Olivia McGill

The US Federal Trade Commission has handed out millions of dollars in fines to companies for collecting personal information without parent's consent, but critics say there is more to be done to keep children safe

The internet has brought unprecedented opportunities to connect, share, learn and express opinions on matters that affect peoples' lives. While the opportunities for children are not any different, the levels of safety and privacy for this age group need to be much tighter.

The Children's Online Privacy Protection Act 1998 (COPPA) was passed by the US Federal Trade Commission (FTC) to help protect children's privacy online. Under it, websites are required to use an approved service to verify parental consent if they engage with, or market to children under the age of 13.

The law also applies to websites or online services directed to a general audience that have knowledge they are collecting data from children and those running third-party services like an ad network or plug-in.
So how effective is the law and how does it impact business?

The FTC has handed out millions of dollars in COPPA fines to companies such as Yelp and Path for collecting personal information without parent's consent, but according to internet lawyer Richard Chapo, there is more it could do. "The FTC has been criticised repeatedly for not enforcing law," says Chapo. "It creates an unfair landscape for businesses. Those that comply end up spending a lot of money on the compliance process as well as forgoing quite a few revenue channels compared to those that do not," he said.

"The FTC averages at about two cases a year where it enforces the law, which is a mockery compared to the hundreds and thousands of websites and apps that have no COPPA compliance."

FTC EXPANDS DATA PROTECTION

However, the FTC recently ruffled some industry feathers by targeting mobile app developers LAI Systems LLC and Retro Dreamer for allegedly collecting unique data linked to children for the purpose of advertising. The allegations, which the app developers agreed to pay a combined $360,000 (£252,000) to resolve, mark the first time that the commission has based an enforcement action solely on a company's collection and use of "persistent identifiers", a category of data that was added to the COPPA rule's definition of personal information in 2013. Persistent identifiers are bits of code such as cookies that can be used to identify a person over time across different websites and apps.

Overall, the prosecutions that have occurred mostly focus on domestic companies but because COPPA extends to foreign websites and online services that collect information from children in the US, it has also sent warnings overseas.

In 2014 the FTC issued a public warning letter to Chinese app developer BabyBus regarding potential violations of COPPA. It made a clear case that BabyBus needed to comply with COPPA because it sells apps through the iTunes and Android app stores which target US consumers. Subsequently all BabyBus apps were pulled by Google from the Android store.

The company responded to the FTC's letter with a statement on its website saying it intended to bring its apps into compliance with US law.

DEVASTATING RESULTS

"In these cases the FTC will seek judicial injunctions barring foreign offending companies from accessing consumer markets in the US. It will also likely seek a "till tap" order requiring all companies based in the US that are handling any part of the monetary transaction to transfer the revenues to the FTC instead of the international entity in question. Both are devastating results for the corporate entity," said Chapo.

Traditionally, most companies focus on COPPA compliance over any laws in the EU member states because enforcement actions in the EU have been considered a remote risk. However, this may soon change. Article 8 of the new General Data Protection Regulation, drafted in January, describes a COPPA-like compliance process but the triggering age for compliance will be "under 16" instead of 13.

This higher age limit could radically alter the children's privacy landscape online as there are millions of teens between the ages of 13 and 16 on social networking sites.

The new law could further complicate business as it allows EU member states to designate an age between 13 and 16 for their specific jurisdictions.

"For compliance for businesses this is a nightmare," said Chapo. "Within the 28 member states you will have a variety of ages. Unless there is a technology solution that will be able to handle the verifiable process for each stage, small companies will have to go for a higher age."

Another reason companies struggle with compliance is due to the process of notifying parents and obtaining Verifiable Parental Consent (VPC) - known as "safe harbor" - before the child or parent loses interest, as well as the limited technologies approved by the FTC that help firms to secure this permission.

Dylan Collins, CEO of UK company SuperAwesome, a kid-safe ad platform, believes it's unrealistic that VPC can be obtained in every scenario and has found a way round it. "When we set up SuperAwesome one of the big problems was how to do COPPA compliant kid-safe advertising," said Collins. "The COPPA compliance sector is not just about how you do VPC; it's not practical to do that for everything, the advertising market wouldn't work if it was.

We built an FTC safe harbor-certified marketing platform that delivers advertising on a content basis rather than a profile basis . Our technology gives advertisers compliance because they are not capturing data from children."

While children's privacy laws are being rolled out or tightened around the world, there is a huge area around child online protection that is still not being addressed. To fill the gap, UNICEF, together with the UN's International Telecommunication Union (ITU), wrote a set of guidelines for industry that integrate child rights, policies on child sexual abuse material and education on children's safety and their responsible use of the internet (the Child Online Protection Guidelines for Industry).

"COPPA is strictly for commercial sites," said Marsali Hancock, CEO of iKeepSafe, a safe harbor-approved certifier that tracks internet-connected devices' effects on children.

"They don't deal with anything outside of how you gather and share data with advertisers and if you have permission or not. They don't assess whether content is age appropriate either and there is nothing about educating teachers, parents and children about their responsible use of ICT."

Hancock recommends the Child Online Protection Guidelines for Industry work in parallel with COPPA so child protection and privacy are addressed equally.

Linked to bullying and even murder, can anonymous apps like Kik ever be safe?

by Nicole Kobie

Questions over whether the benefits of anonymous apps – such as giving children a space to explore sensitive issues – can outweigh the risks they pose.

Nicole Madison Lovell, a 13-year-old school girl from Virginia, chatted with an 18-year-old man over anonymous messaging app Kik before he allegedly killed her in January. Since then the app – which boasts some 240 million registered users and requires no phone number or name – has been the subject of scrutiny.

In response, Kik has handed over data to the murder investigation, updated its guide for parents, and asked the Apple Store to boost its age rating from nine to 12, with company representatives stressing teens between 13 and 18 should get parental permission to install the app. Kik is, of course, not the only anonymous app hit with safety scares. Yik Yak, which allows people within a particular radius to create posts anonymously and upvote or downvote other posts, has faced controversy for hosting racial abuse and violent threats. Secret, an app where users can share their secrets anonymously, has also faced scrutiny over cyberbullying and security. These might be more extreme cases, but can these anonymous apps ever be truly safe?

Stephen Balkam, founder of the Family Online Safety Institute, can see their value for teens looking to express themselves or explore sensitive areas such as sexuality.

While Sonia Livingstone, a professor in media and communications at the London School of Economics, says that anonymity doesn't inherently encourage negative outcomes. "It encourages intimacy and honesty as well as manipulation and nastiness," she says.

DEALING WITH ABUSE

However, the design of some apps make them worse than others, according to Balkam. Yik Yak's geolocation tool, for example, particularly concerns him because it limits user interactions with others within a 1.5 mile radius. This has the potential to create an online world for rumours and hate which can then spread offline in small communities.

Balkam believes in-line messaging, where users get prompts asking their age or pointing out features and security settings while they use the app, can help improve safety. He says reporting mechanisms and blocking tools should be easy to find, and that a team should be in place responding to those reports so they're not just landing in a neglected mailbox.

Kik's built-in help chat bot gives no help to questions about bullying or reporting users, instead offering random facts and jokes, but the app does feature a spam reporting tool that lets users send snippets of chat history as evidence for Kik's staff to review and then ban users if appropriate. Yik Yak has a reporting tool that flags posts as spam, offensive, or targeting someone; posts that get enough complaints are sent to a human moderation team. Human moderation is key according to Livingstone, but she says that it's an expense some app companies might be unwilling to pay.

DATA MINING

The anonymity of apps doesn't mean that user data is not being sought. Kik and Yik Yak are free and let users hide behind a made-up name inside the app, but both ask for real names and email addresses when signing up. User data can be used to target tailored ads. While heavy investment has meant Yik Yak has yet to seek ways to make money, Kik has started taking some advertising.

The data-mining business model behind free apps needs to change in order to improve safety, says ethical developer Aral Balkan. When apps and other free online services depend on data to make money, Balkan says they're designed to motivate as much use of a service as possible, and this means they encourage behaviours that are addictive – and not always positive.

"Some of that is confrontational, so it's against their interest to reduce conflict," he argues, pointing to Twitter as an example. When users get upset or pick fights with each other, they use the service more, says Balkan, and the company can gather more data.

For Balkan, creating a safe, welcoming community on an app would have to start from an entirely different business model such as paying outright for apps or finding a new way to fund them – anything that prevents a dependance on users trading their data.

There is of course another response to building better online communities: be nicer. Balkam says there's a growing notion of using positive behaviours to counteract negativity.

"We're just trying to steer kids towards that," he says, citing an example from the US. "There's an amazing story of a high school kid who, for a year, posted anonymously just wonderful things about every single member of his year and kept it a secret until graduation day and then he revealed himself. That was an incredible use of anonymity on social networks. If we can encourage those stories, that would be brilliant."

Surveillance state: fingerprinting pupils raises safety and privacy concerns

by Nicole Kobie

More than a million students have handed over fingerprints to enhance security and easy admin but how safe is the data and what is it being used for?

School lunch lines in the UK can be fraught: students receiving free lunches may not want their peers to know, lost payment cards mean some go without, and code-based payments leave children at risk of "shoulder surfing", where others spot their number and use it to buy their own meal.

Fingerprint scanners are being presented as one solution for doing away with this stress. They can be linked to online payments, making busy lunchtimes easier and faster, plus it will save schools from printing ID cards.

A typical secondary school in the UK can end up producing more than 400 new payment cards every year to account for lost, damaged and new intake ones, says Nigel Walker, managing director of biometrics company BioStore. "Biometrics can't be lost or forgotten, stolen or used by someone else. "When students and staff identify themselves on the system, you can be sure it's them. This improves a school's safety in terms of access, security and accountability."

The Department for Education doesn't track how many schools use biometric systems, but in 2014, campaigning group Big Brother Watch estimated that more than a million secondary schoolchildren had handed over their fingerprints.

In these hi-tech schools, biometrics – in particular fingerprints but also palm prints – can be used for entering and exiting the main school building as well as classrooms and buses, taking attendance, and accessing lockers, computers, library books and printers. Add in other new technologies such as wearables, and civil rights campaigners fear the result is that surveillance is quietly being normalised in children from a young age.

NORMALISING SURVEILLANCE

The Protections of Freedoms Act 2012 states that schoolchildren cannot have their fingerprints taken without written parental consent. Until then even the youngest of students may have had their biometric data captured. "There is no need to retrospectively gain this consent so many children are having their data processed without their, or their parents', consent," says Emmeline Taylor, author of Surveillance Schools.

Daniel Nesbitt, research director at Big Brother Watch, says that parents and children must understand what is going to happen with the information, how it will be used and where it will be stored. "Without this information, they can't give informed consent," he says.

"The immediate issue is that children may be monitored across a range of areas – potentially including what they are eating to which library books they take out – and this could normalise the idea of surveillance or being tracked from an early age," Nesbitt adds.

Taylor agrees: "Those that experience surveillance in a school are semi-captive, and the fact that the same individuals inhabit the same space on a daily basis means that surveillance forms part of their lived environment, as commonplace and mundane as the blackboard at the front of the classroom."

KEEPING DATA SAFE

Others wary of using biometrics in schools point to the challenges around security. "The risks include the data being leaked, hacked or misused by the school," says Pam Cowburn, communications director for the Open Rights Group. "Schools need to think about how data is collected, stored and used. Who can access it? What could happen if it were leaked?"

Some companies say encryption helps make these systems safe. With itsPalmSecure biometrics system, Japanese company Fujitsu, collects an image of the entire hand, encrypting the data. "Each sensor provides a unique encryption algorithm, so even if you stole the encrypted templates, the information would be useless," says Kent Schrock, marketing executive at Fujitsu. BioStore, meanwhile, holds student scans in a dedicated, encrypted database, promising to delete it – not just overwrite it – when it is no longer in use.

Such encryption is advised by the Information Commissioner's Office, but understanding the finer points of information security may be beyond school staff and parents, putting the onus on companies to keep data safe.
Fear of falling behind

Proponents argue that biometric systems can keep school buildings secure, help battle truancy and even encourage healthy eating. However, Taylor says she has seen little evidence of this and is concerned schools will feel under pressure to adopt the technology.

"As some schools introduce tracking devices to supposedly increase efficiencies, safeguard students and respond to issues such as truancy and obesity, other schools quickly follow suit through fear of otherwise being regarded as negligent of their responsibilities," says Taylor. "The only beneficiaries are the companies selling the equipment. Once these systems are viewed as necessary, then any cost, whether financial or social, becomes worth the trade. It is an ingenious strategy to turn limited public funds into private profits."

Is the Internet of Things putting your child's privacy at risk?

by Becky Slack

From Hello Barbie to hacked baby monitors, privacy legislation can't keep up with the increasingly Wi-Fi enabled world

Back in an era that this author fondly remembers, Barbie was a simple doll with moveable parts and long blonde hair ripe for plaiting (and chopping, in more mischievous moments). Today, she is much more sophisticated. Hello Barbie, the world's first Wi-Fi-enabled Barbie doll, for example, uses voice recognition software and artificial intelligence to bring her to life.

Just as we are connecting everyday objects, such as cameras, heating systems and fridge freezers to the internet, we are also connecting dolls, toys and other items that are accessed by children.

While this has many benefits for imagination, creativity and play, they also bring a number of risks – not least those associated with children's privacy.

Indeed, there have been multiple reports of baby monitors being hacked and of cyber attacks on toy software that has led to sensitive data – including photos of children – being stolen. Hong Kong toymaker, VTech is one recent example of this, while Hello Barbie herself has been at the centre of controversy over whether or not she can also be hacked (ToyTalk and Mattel say not).
So when it comes to the Internet of Things (IoT), what are the potential risks for child protection, and what needs to be put in place to mitigate against these?

According to the Federal Trade Commission (FTC) in America, the IoT presents a variety of potential security risks that could be exploited to harm consumers, including children. These include enabling unauthorised access and misuse of personal information (such as photos of children or recordings of conversations); facilitating attacks on other systems (by being able to access banking details, passwords etc.); and creating risks to personal safety (in extreme cases, grooming).

In a more general sense, research (pdf) by the UK Council for Child Internet Safety has found that 12% of children have experienced data misuse such as identity theft or somebody using their personal information in a way they didn't like. It all sounds pretty scary – so does that mean legislation is the answer?

Currently there is no specific legislation in place for the Internet of Things. The concept is so new and the technology changes so rapidly that the law has thus far found it impossible to keep up. That situation is unlikely to change any time soon.

There is only one example of case law and that relates to an American case involving TRENDnet, which provides internet-connected cameras for purposes ranging from home security to baby monitoring. Despite claiming its products were secure, the FTC found that hackers were able to access live feeds from consumers' security cameras and conduct "unauthorised surveillance of infants sleeping in their cribs, young children playing and adults engaging in typical daily activities." Under the terms of the settlement agreed with the FTC, TrendNet cannot misrepresent its software as "secure" and must get an independent assessment of its security programs once a year for 20 years.

Elsewhere, rules regarding IoT are established within the context of current laws, such as the Children's Online Privacy Protection Act in the US. Meanwhile, in the UK, the Office of the Information Commissioner recently provided guidance on wearable devices and stipulated there should be no data collected that breaches the Data Protection Act, but so far no specific recommendations or rules have been made that relate to child protection and the IoT.

While we wait for government to decide what is the most appropriate way forward with regards to IoT and child protection, there are ways in which product designers and companies can work more effectively to minimise risks. One such area is "security by design" whereby companies build security into their devices from the outset, says Tony Neate, chief executive of Get Safe Online. "They have to look at passwords, or even better – biometrics – building it in from the beginning rather than adding it on at the end", he says.

Tony Anscombe, senior security evangelist at AVG, agrees: "We're in a transitioning phase here. Some people may have fitness trackers, but if in five years' time we are all suddenly going to be carrying three or four of these devices, the industry needs to come together to develop clear defined standards as to how they inter-operate and how to provide security for end users," he says, adding how this is particularly important for those devices accessed by children.

Data minimisation is another area for developers to consider. This refers to the concept that companies should limit the amount and type of data they collect and retain, and should dispose of it once they no longer need it. In the case of children, this data could involve recordings of conversations between friends, photos and personal information about likes and dislikes.

"[Companies] can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect," advises the FTC (pdf). "If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data."

Communications with consumers, be it security instructions, privacy agreements or consents around data use, should all be in "simple language and understandable by everyone – ideally on one side of A4 paper", says Anscombe.

The government also has a responsibility to ensure the public understands the risks, particularly as the IoT and connected devices become more prevalent. In many of the security breaches reported thus far, the situation has involved a degree of ignorance as to what constitutes online safety.

For instance, one of the families whose baby monitor was hacked only had a password on the monitor itself and not one on the Wi-Fi.

"When I talk to parents about online safety, they often say to me that their son or daughter knows much more about computers than they do. But do the children know more about life than the parent? A boy or girl may appear to be located safe upstairs in their bedroom, but for all the parent knows they could be accessing the darker side of the web in its various forms", says Neate. It is very important that parents are provided with clear guidelines as to what data is collected and/or stored, and how to remain secure right from the outset. This could include instructions on packaging, video tutorials orQR codes on devices that take consumers through to more information.

For now, governments around the world appear to prefer a broad-based approach to privacy legislation, rather than IoT specific rules. However, this is a brave new world we are entering, and as the number of connected devices increases so too will the number of children being exposed to risks.

Would you use a GPS device to track your child?

by Nicole Kobie

Tracking children with GPS-enabled devices in becoming practical and affordable, but child rights and privacy campaigners are worried.

Losing track of a child is a terrifying prospect. The recent emergence of GPS devices that can report on youngsters' whereabouts, coupled with the falling prices of gadgets, seem to offer parents a tech solution.

Swedish firm Trax, for example, has designed a GPS tracker, on sale for $249 (£170), that issues alerts when children step outside of pre-set "geo-fences" and allows parents to follow their children from their smartphone or computer in real time. French company Weenect has also created a GPS tracker for children, and for €99 it includes an SOS button that allows distressed kids to call their parents. The device can send notifications when children reach a set destination and allows parents to review where their child has been throughout the day.

Any parent who's frantically searched for a lost child will likely see the appeal. Weenect founder Adrian Harmel expects to see "considerable growth" on the 10,000 trackers the company sold last year. But he says children aren't in fact the biggest focus for his GPS trackers. Currently, 60% of the company's total sales are for devices to track pets, 30% are for child trackers and the remaining 10% are for its Weenect Silver device, a tracker designed for elderly.

FREEDOM FROM TRACKING

However appealing such technologies may seem at first, they could have negative effects on the very children they aim to protect.

"It is understandable that parents want to do anything they can to keep their children safe but they need to ask themselves whether tracking technology is really necessary and whether it will actually protect their children," said Pam Cowburn, communications director of the Open Rights Group. "Parents need to teach their children to be independent and to be able to cope with risks and dangers."

These trackers, she says, could limit children's privacy and personal freedom, while encouraging them to accept surveillance. "There will undoubtedly be an impact on children's behaviour and development if they think that they are constantly monitored by their parents and teachers.

"A big concern is that it becomes normal for children to be tracked all of the time.Children have a right to privacy as much as anyone else. They need private spaces to be able to play and grow without feeling they are constantly watched."

Harmel believes the trackers should not be seen as spying devices. He says the purpose is to give children independence while reassuring parents at the same time: "Let's say you're stressed as a parent, what is better for your kid: to not let them do anything on their own, or to let them get a bit of autonomy thanks to a tracker?"

Harmel stresses such technology requires good communication, advising parents to carefully explain the purpose of the tracker and make sure children are aware it's not a "superhero" and they still need to be careful when out and about.

REAL-LIFE PARENTING

These gadgets can never be a replacement for parental attention, says Barbara Wallner, head of customer experience at Trax. "Trax provides an additional security aid for parents and pet owners, a little bit of extra piece of mind when their loved ones are away," she says. "But it can never replace proper care."

A spokesperson from the NSPCC warned that tracking technology could lull some parents into a false sense of security, particularly when it comes to crimes such as kidnapping or abuse. "There is no reason to think this will keep the child safe from determined offenders, who will simply throw the device away. It is also important to remember that most abuse is perpetrated by offenders who are either part of the family, or known and trusted by it."

"As children grow older and develop in maturity it's important they get the freedom to go out on their own or with friends. It's just a natural part of developing independence and, like every part of growing up, it can be a challenging hurdle for a parent to overcome," added the NSPCC spokesperson.

No technology can completely protect any child, and talking to them about dangers and teaching responsibility are necessary whether using trackers or not. Ultimately, trusting children to make the right decisions and giving them the freedom to do so is big part of growing up. This should not be lost sight of by parents, who may turn to tracking technology as a crutch to get over the difficulty of letting go.

From Liverpool FC to Google: business joins in pledge to promote safer internet

by Will Gardner, Susie Hargreaves and David Wright

From Premier League football clubs to search engines, organisations can leverage their reach to address digital safety challenges.

The world has changed dramatically in the 13 years since the annual Safer Internet Day (SID) was launched. Thirteen years ago, YouTube didn't exist. Now more than half of children use the video sharing website every day, according to a recent report from Childwise. And children spend more time on the internet than they do watching TV. As we become more reliant on digital technology, keeping children safe online becomes ever more pressing. Today's SID – marked in more than 100 countries and organised in the UK by the UK Safer Internet Centre (UKSIC) – is an opportunity for everyone, from families to law enforcement and businesses to policymakers, to play their part for a better internet.

High-profile supporters include the BBC, BT, Disney, Facebook, Google, Instagram, Microsoft, Nickelodeon, Twitter, Vodafone, and the UK government, as well as police services and schools. All are involved in delivering a range of activities.

Microsoft, for example, is doing a SID takeover on its search engine Bing, and will serve specially created resources when anything internet safety related is searched. Snapchat has created a filter for SID that can be applied to photos taken using the app, while Vodafone is supporting with its special emoji keyboard, featuring a #SID2016 heart shaped emoji intended to be shared in solidarity against cyberbullying.

The company is also working with YouTubers to create awareness raising videos and for each view, like and direct share a video receives, the Vodafone Foundation will donate £1 up to a maximum of £100,000 to child rights charities.

But it's not just the responsibility of big tech companies to ensure they are educating and supporting people in the safe and positive use of technology. Other businesses can also make a difference by through customers and staff. Football teams, for example. Premier League clubs Everton, Liverpool, Manchester United and Arsenal are hosting education sessions for hundreds of local schoolchildren, as well as getting players involved in promoting the safe and positive use of technology as part of their youth outreach programmes.

Other organisations bring unparalleled reach on SID, with the Post Office playing SID safety messages through TV screens in its network of stores on the day and Nickelodeon creating anti-bullying videos for TV, its website and its YouTube channel.

While the day provides a focus for raising awareness of internet safety issues and an opportunity for companies to create some good PR stories, many of these partnerships are continuous throughout the year. The UK Safer Internet Centre sits alongside representatives from corporates, NGO, government, and police on the executive board of the UK Council for Child Internet Safety, as well as being represented on safety councils for Facebook, Twitter, Snapchat, Ask.fm and more.

Keeping children safe online is challenging – cyberbullying is increasing and young people are facing increasing pressures online that can have long-lasting impacts on their wellbeing.

The ongoing threat from the proliferation of child sexual abuse images remains at the top of the agenda for many companies as they strive to use cutting-edge technical solutions to solve issues that can have huge consequences for the lives of some of the most vulnerable children both here in the UK and worldwide.

The challenges are complex, and there's no magic bullet to create a better internet but if all organisations step up to the challenge and play their part, we can all make a big difference.

What are four of the top social media networks doing to protect children?

Marc Ambasna-Jones

With reports of cyberbullying on the rise, a guide to what Facebook, Twitter, Snapchat and Instagram are doing, and whether it's enough.

According to recent report from NSPCC, ChildLine conducted 35,000 counselling sessions for low self-esteem between April 2014 and March 2015. The report blames "a constant onslaught from cyber-bullying, social media and the desire to copy celebrities," as key reasons.

Julia Fossi, senior analyst for online safety at NSPCC says that while most platforms are taking steps to improve safety, social networks must be held more accountable for the content they host.

She says that social sites, which often use tracking technology for adverts and marketing could use a similar technology "to identify potential bullying issues and help determine what an effective intervention would look like." With reports of cyberbullying on the rise and girls more likely to be affected, Will Gardner, CEO, Childnet International says that the area is "challenging" but agrees that sites must continue innovating with technology to tackle the issue.

Here, we look at what four of the biggest social media networks are currently doing.

FACEBOOK

Facebook's rules states under-13s can't sign up, but research from EU Kids Online and the LSE found half of 11 to 12-year-olds are on Facebook. .

Announcing the recent formation of the Online Civil Courage Initiative – a partnership between Facebook and NGOs to fund counter speech campaigns against terrorism and bullying – Facebook COO Sheryl Sandberg said that, "hate speech has no place in our society — not even on the internet". Facebook polices the content on its own site on a report by report basis, relying on users to report posts to its "around the clock" global support teams.

While Facebook claims it has improved its reporting transparency with a user dashboard that lets users know how their complaint is being dealt with, there is no available open data on how many reports are resolved satisfactorily and how many abusive users and pages are removed.

The network does have a family safety centre with information aimed at teens and parents, and encourages users to block or unfriend anyone who is abusive.

TWITTER

In a leaked memo in February last year, former Twitter CEO Dick Costolo claimed that Twitter "sucks at dealing with abuse and trolls".

Since then, the company says it has streamlined the process of reporting harassment and has made improvements around reporting other content issues including impersonation and the sharing of private and confidential information.

Crucially the site has updated its enforcement procedures too, claiming to use both an automated and human response to conduct investigations and follow appropriate actions swiftly. The site says it will take action against abusers depending on severity, ranging from requiring specific tweets to be deleted to permanently suspending accounts. Like Facebook, there is no public data showing the effectiveness of its policies and reporting.

Last year Twitter launched a safety centre where users can learn about staying safe online, with sections created especially for teens, parents and educators. It also recently announced a partnership with mental health charity Cycle Against Suicide to promote online safety.

SNAPCHAT

A report from last year's Safer Internet Day found that Snapchat is the third most popular messaging or social media app among the 11 to 16 age group (behind Facebook and YouTube).

The app has community guidelines which outline what users shouldn't send others, including harassment, threats and nudity, and as with other sites and apps, users can block people and report abuse.

It has a safety centre with safety tips and advice, produced in partnership with experts from iKeepSafe, UK Safer Internet Centre and ConnectSafely. And in November, the app partnered with Vodafone to raise awareness of cyberbullying by offering users emojis designed to be shared as an act against online abuse. Still, according to the NSPCC's Net Aware guide, "64% of the young children we asked think Snapchat can be risky".

INSTAGRAM

Owned by Facebook since 2012, Instagram has community guidelines and tips for parents that address questions such as, "who can see my teen's photos?". Like Facebook, users have to be aged 13 or over, though it's easy to lie about your age and sign up. Instagram encourages users to report those underage via an online form or through in-app reporting. This reporting also applies to abusive content, impersonation and hate accounts.

The company claims it monitors reports 24/7 to investigate abuse, shut down accounts and report to relevant authorities. Again there are no public stats to enable an accurate measure of effectiveness.

The ability to follow accounts of people you don't know and access unsuitable material has been highlighted by the NSPCC, although the charity says most content is deemed low risk.

04 Chapter 04
Educating children, parents and teachers about children's safety and their responsible use of ICTs

INTRODUCTION

Technical measures can be an important part of ensuring that children are protected from the potential risks they face online, but these are only one element of the equation.

Parental control tools and awareness raising and education are also key components that will help empower and inform children of various age groups, as well as parents, caregivers and educators. Although companies have an important role in ensuring that children use ICTs in the most responsible and safest possible way, this responsibility is shared with parents, schools, and children.

Many companies are investing in educational programmes designed to enable users to make informed decisions about content and services. Companies are assisting parents, caregivers and teachers in guiding children and adolescents towards safer, more responsible and appropriate online and mobile phone experiences. This includes signposting age-sensitive content and ensuring that information on items such as content prices, subscription terms and how to cancel subscriptions, is clearly communicated.

It is also important to provide information directly to children on safer ICT use and positive and responsible behaviour. Beyond raising awareness about safety, companies can facilitate positive experiences by developing content for children about being respectful, kind and open-minded when using ICTs and keeping an eye out for friends. They can provide information about actions to take if they have negative experiences such as online bullying or grooming, making it easier to report such incidents and providing a function to opt out of receiving anonymous messages.

Parents sometimes have less understanding and knowledge of the Internet and mobile devices than children. Moreover, the convergence of mobile devices and Internet services makes parental oversight more difficult. Industry can work in collaboration with government and educators to strengthen parents' abilities to support their children to behave as responsible digital citizens. The aim is not to transfer responsibility for children's ICT use to parents alone, but to recognize that parents are in a better position to decide what is appropriate for their children and should be aware of all risks in order to better protect their children and empower them to take action.

Information can be transmitted online and offline through multiple media channels, taking into consideration that some parents do not use Internet services. Collaborating with school districts to provide curricula on online safety and responsible ICT use for children and educational materials for parents is important. Examples include explaining the types of services and options available for monitoring activities, actions to take if a child is experiencing online bullying or grooming, how to avoid spam and manage privacy settings, and how to talk with boys and girls of different age groups about sensitive issues. Communication is a two-way process, and many companies provide options for customers to contact them to report issues or discuss concerns.

As content and services grow ever richer, all users will continue to benefit from advice and reminders about the nature of a particular service and how to enjoy it safely.

The businesses going above and beyond to protect children online

In the fast-moving digital world, how are technology companies educating children, parents and teachers about safety and privacy?

On 9 February 2016, millions of people worldwide celebrated Safer Internet Day (#SID2016). It was an opportunity for schools, charities and other organisations to run digital safety events but also for technology companies to showcase their child online protection initiatives.

Protecting young people should be a priority for digital businesses, say the Guidelines for Industry on Child Online Protection (pdf), which were developed by UNICEF and the International Telecommunication Union (ITU) and include advice on educating children, parents and teachers about online safety and responsible use of ICT.

While there has been criticism that some businesses do not take online safety seriously enough, other companies are going above and beyond to help families manage digital risks. As internet safety expert John Carr, who has advised the ITU and the EU, says, "Working through governments and inter-governmental agencies like the UN is, of course, extremely important but it can sometimes take years to see any results. Companies can change things now and thankfully many of them are ready to step up."

"If we are going to solve tomorrow's global challenges, we must come together today to inspire young people everywhere with the promise of technology," said Microsoft CEO Satya Nadella in 2015. Safety and security is central to that promise and Microsoft has created a broad range of resources for young people, parents, carers and teachers on topics such as bullying, sexting and hate speech online. Its YouthSpark programme is also helping more than 300 million young people around the world to improve their digital skills.

"It may sound like a cliché but the multi-stakeholder approach is the only way to achieve meaningful results in the long run," says Mauro Accurso of mobile industry body the GSMA, which is currently working with UNICEF to promote digital safety across Latin America. "Government, industry and civil society need to work hand in hand on matters relating to child online protection if we are going to make a difference."

As Lisa Felton, head of consumer policy and content standards at Vodafone Group, points out, "Young people see the internet as an essential part of their lives and do not necessarily see a separation of being 'online' or 'offline'. However, we need to ensure they are aware that their online activity and behaviour may have particular risks and consequences, and support education and awareness initiatives so they have the resilience and confidence for the internet to be a positive experience."

Resources developed by Vodafone, such as Digital Parenting, are helping millions of families in the UK, Greece, Qatar and other countries. And, following a Vodafone survey of 5,000 teenagers in 11 countries which revealed that one in five teens had been bullied online, the company launched its #BeStrong anti-bullying campaign in 2015.

At Telefónica, the Familia Digital platform provides technology news, FAQs, videos, games and surveys to help parents, guardians and educators stay up-to-date. The resources are available in various countries including Spain, El Salvador and Guatemala. According to Telefónica's sustainability innovation manager María José Cantarino de Frías, "The platform is also a place to share experiences and testimonials and help overcome the challenges and difficulties people might face due to technological change and the constant appearance of new applications and services."

Child online protection is also a priority for leading social media companies and search engines. Last year, Twitter launched a new safety centre and ASKfm revamped its safety resources, for example. As well as developing innovative safe search tools, Google's recent education work includes supporting an online safety campaign in Kenya and working with Parent Zone to tour UK primary schools.

As more people go online and on mobiles, technology companies share the responsibility for educating children, parents and teachers about the safe, responsible and positive use of ICT.

"The tech industry has brought us remarkable devices, platforms and apps to connect the world. It is incumbent on them to also provide the tools, rules and educational efforts to empower parents to confidently navigate the online world with their kids," says Stephen Balkam, founder and CEO of the Family Online Safety Institute.

Many businesses are taking this task seriously. More than 20 technology companies including Dropbox and Tumblr make up the Thorn Tech Task Force, for example, and a number of businesses pledged to tackle online child sexual exploitation at the #WeProtect Children Online Global Summit last November. As UNICEF deputy executive director Fatoumata Ndiaye commented ahead of the summit, "... protecting children online is an urgent global priority".

For children everywhere, #SID2016 is not just something that trends in February; its mission is relevant – indeed, vital – all year round. With the continued support of the technology industry, young people could be even safer in their digital spaces every single day.


© UNICEF/UNI149128/Schermbrucker

Parents, is it OK to spy on your child's online search history?

by Bella Kvist

Microsoft's Windows 10 and other parental control software face criticism for harming teens' exploration of sensitive topics such as sexuality

Can giving parents detailed activity reports of their child's online search terms be harmful to young people looking for information on sensitive topics such as religion,sexuality, gender or domestic abuse?

When Microsoft this summer launched its new Windows 10 feature that lets parents see what their children get up to online, this was one of the criticisms it encountered. Microsoft has since welcomed feedback and promised an update, with more appropriate default settings for teenagers. However, it is not the only service provider offering this level of parental control. Most security software companies today sell "family" products, many including reports, notifications and video supervision. But is it right to spy on your child?

The UN convention on the rights of the child stipulates that children have a right to privacy and a right to information. They also have a right to protection from all types of violence and exploitation – and there lies the rub.

With a young generation more internet-savvy than their parents, ensuring online safety for minors surfing an ever-expanding web becomes a hard task. Today's parents don't have an older generation to turn to for tech advice, so many turn to parental control software instead. Recent research [pdf] commissioned for Norton by Symantec, a provider of antivirus and security software, shows that 46% of British parents worry that they don't know what their children are doing online.

Nick Shaw, Norton's general manager of Europe, the Middle East and Africa, is one of those worrying parents. Perhaps predictably, he uses parental control software, including reports.

"I'm not looking at what they're doing day to day, I'm just checking to make sure that they're safe," he says. He emphasises that he uses Norton's family feature alongside face-to-face discussions with his children, and encourages other parents to do the same.

Raj Samani, chief technology officer at Intel Security, previously McAfee, applies a family protection pack with informed consent and says his children approve of his monitoring because he is transparent about the reasons for it.

"My daughter tried to communicate with somebody and I got the notification. And actually what she was doing was unsafe so I ended up having a conversation with her, explaining the concept of anonymity."

Shaw and Samani both have children aged 11-16, the age that 61% of British parents believe is when their children are most vulnerable online. Shaw says parents' product demands depend on their child's age: parents of young children often want to monitor screen time, whereas those with teenagers raise concerns about social media. "We build a tool that allows parents flexibility to do what they want," says Shaw.

Samani says parents and children do need to have a discussion about the when monitoring should stop: "To me I think it comes down to a point where have you got that level of understanding and maturity."

Cyber security consultant Dr Jessica Barker questions whether parental monitoring is fair on children, and says it can intrude into their privacy. Referencing research by Professor Sonia Livingstone on internet governance and children's rights, she goes so far as to say it can be harmful.

"If [children] feel they are being monitored that undermines any kind of relationship of trust. They might be using the internet in a healthy way to get information and support, and feel that they are not able to do that because they are being monitored."

She brings up the issue of teenagers wanting to explore their gender or sexuality in private. If parents have a problem with that, or even use filters blocking LGBT sites, that could cut off access to something hugely helpful, a service previous generations didn't have.

One young man, who wants to remain anonymous, said that his homosexuality was outed to his unsupportive parents by parental control software.

"They didn't say they had seen what I had looked at but they hinted very strongly at it in conversation," he said, adding that he soon learned how to work around his parent's system.

Barker says: "There's certainly evidence that suggests that teenagers who know they are being monitored at home will look at a friend's device. And then they don't have someone to talk to about it."

So do software companies consider these issues when creating their services?

"Absolutely," says Samani. "We'll always recommend that the reporting and the communication for children should be used as a vehicle to begin or continue that dialogue with children.

Shaw says Norton "looks at every aspect when designing a tool", but adds that the primary focus is protecting the child. "At the end of the day it's a tool … How people use the tool is up to them."

When it comes to balancing privacy and protection the key concepts that emerge are education, conversation, consent and the fact that the internet offers lots of opportunities for children – positive and negative. As for how far parental control should go, our anonymous gay man sums it up well: "Computers shouldn't do the parenting."

"WHAT SHE WAS DOING WAS UNSAFE SO I ENDED UP HAVING A CONVERSATION WITH HER, EXPLAINING THE CONCEPT OF ANONYMITY"

Essena O'Neill: Can kids spot covert marketing by social media stars?

Brands are using young influencers with big online followings to market their products, but real life and paid-for endorsement can sometimes become blurred.

Australian model and teenage social media star Essena O'Neill hit the headlines earlier this month when she decided to quit social media, claiming it wasn't "real life". Explaining the images she uploaded to social media portrayed as spontaneous life snaps, she spoke of lengthy staged photoshoots and sponsored clothing, claiming she could could be paid up to AUD$2,000 (£955) for each post.

In a recent survey of 16- 19-year-olds, participants said most of their online time was spent using websites and apps such as YouTube, Instagram and Facebook. Brands are following them there and partnering with teenagers who have big online followings to whom they can market their products and services. The problems arise when these commercial partnerships aren't transparent.

RULES ON SOCIAL MEDIA MARKETING ARE "FUZZY"

In the UK Advertising Standards Authority (ASA) regulates sponsored content. Last week, the ASA banned a video on the Instagram account of Made in Chelsea reality TV star Millie Mackintosh because it hadn't made clear it was an advertisement for a Britvic beverage.

The image caption featured the brand name and the hashtag #sp, which was meant to indicate sponsored content. However, the ASA ruled that it "was not a sufficiently accurate label" and that consumers needed to be aware that they were viewing marketing content prior to engaging with it.

"There is a common misconception that this space is not regulated but it is," says Richard Lindsay, director of legal and public affairs at the Institute of Practitioners in Advertising. "Advertising needs to be obviously identifiable as such, in other words advertising has to be transparent, and if it's not people get their fingers burnt."

The ASA's sister body, the Committees of Advertising Practice, offers guidance around non-broadcast advertising and urges brands and partners to be transparent about their association. Its director, Shahriar Coupal, says: "It's simply not fair if we're being advertised to and are not made aware of that fact."

Jed Hallam, head of digital strategy at global media and marketing services company Mindshare, explains that there is a difference between so-called "paid" and "earned" media.

For example, paid media would mean paying for an influencer's time and audience reach for a specific project, whereas earned media refers to giving an influencer a product or service and hoping they promote it in return.

"Usually it's a kind of you scratch our back, we scratch your back type of situation, but it always goes unsaid, so that's what makes it a really grey area," says Hallam, adding that Mindshare mainly deals with paid media.

Either way, he says it is important to remain clear. "If you don't know you're being sold to and you have even a glimmer of doubt that you are, then that is going to create a backlash from the audience," he says.

Nathan McDonald is co-founder and global managing partner of social media agency We Are Social, which matches commercial clients with online influencers. McDonald says the rules can seem "fuzzy" and that transparency, credibility and trust – as well as matching the right brand with the right online influencer – is key to getting it right.He also says that his agency wouldn't ask someone to say or promote something that they didn't believe in.

McDonald thinks authenticity will continue to remain key to social media marketing success, especially with the advent of live streaming services such as Periscope and Meerkat. He explains that with live streaming "there is no editing, there is no second take ... it's just as it's happening and I think that's really interesting for brands to be involved with".

EQUIPPING YOUNG PEOPLE WITH A "BULLSHIT METER"

Dr Pamela Rutledge, director at the Media Psychology Research Center in California, says that people, and especially young people, can often feel like they have real relationships with those they follow online, which is why it's so important that the line between real life and paid-for endorsement isn't blurred.
Rutledge says the fact that social media showcases so many different ways of being is "a real positive" but argues that education is critical.

"Just because [young people] can use apps and text like the wind doesn't mean they understand the implications of the media environment, privacy, and potential manipulation," she says.

"Just as we've argued for media literacy in terms of image, such as Photoshopped magazine covers, we need to be aware of lack of authenticity in endorsements. The only way to protect young people is to teach them the critical thinking skills and judgment, and to push for increasing transparency.

"We want to do everything possible to make sure kids are armed with, for lack of better words, a bullshit meter. The illusion of familiarity that comes with social media makes that critical."

But Rutledge also emphasises that product placements and endorsements are nothing new and that it is important not to just view teenagers as victims.

"To me there would have been nothing wrong with her [Essena] saying 'Look at this great outfit, I got this from this great company, they are supporting me to show it to you but I really love it'," says Rutledge.

She believes there is a huge opportunity for companies to embrace this authenticity and ultimately come across as good guys.

> **"THERE'S NO SHAME IN PROMOTING; THERE'S JUST SHAME IN TRICKING."**

A DAY IN A LIFE

JACQUELINE BEAUCHERE
Protecting children online: 'we need to empower young people to be their best digital selves'

Meet Jacqueline Beauchere, chief online safety officer, Microsoft. Jacqueline implements Microsoft's online safety strategy which involves internal policy creation, influence over consumer safety features on products and services and awareness-raising for parents, children and educators.

I have three main sets of responsibilities which are all aspects of Microsoft's online safety strategy. They include internal policy creation and implementation; influence over consumer safety features and functionality in our products and services; and communications to and engagement with a variety of external audiences, including awareness-raising and educational efforts for parents, children, educators and others.

WHAT MY WORK INVOLVES

With such a broad mandate, there are a number of child online safety-related projects underway at any one time. Recently, we released an internal guidebook to enable international personnel to work with local governments and others in a given geography to create national initiatives for child online protection. The guidebook provides a framework for reviewing and conducting research; raising public awareness of online risks to children; promoting in-school education about digital literacy and digital civility; enacting, strengthening and enforcing child protection laws, and collaborating with technology companies and civil society.

We've also released some new educational resources about two key issues: teaching kids how to identify misinformation and hate speech (pdf) online and addressing online harassment and cyberbullying (pdf). These are the newest additions to a long list of informational and educational materials we've created over the last decade-plus, including protecting young children online (pdf), protecting "tweens" and teens (pdf), and starting online safety conversations (pdf) with children. All our materials can be found on the Microsoft YouthSpark Hub, and on our resources pages.

WHAT I ENJOY IN MY WORK

I find it incredibly rewarding when I get to interact with young people directly about their online habits and practices. There's nothing better than when, after a brief awareness-raising, information session, or focus group, young people commit to being better "digital citizens," agree to take steps to safeguard their personal information online, or stand up for their friends and classmates in uncomfortable situations.

> **THERE'S NOTHING BETTER THAN WHEN, AFTER A BRIEF AWARENESS-RAISING, INFORMATION SESSION, OR FOCUS GROUP, YOUNG PEOPLE COMMIT TO BEING BETTER "DIGITAL CITIZENS**

WHY IT'S SO IMPORTANT

Microsoft invests in child online protection because we believe we have a responsibility to our customers, their families and the public at large. We work to earn customer trust and confidence in technology and online services, so our global society and digital economy can continue to thrive. Success comes from ridding our services of illegal content; educating parents, teachers, coaches and counsellors about protecting themselves, their children, students and families from online risks, and working with governments to ensure the proper laws are in place to help children thrive, grow and embrace what is truly the transformational power of technology.

HOW I IMAGINE MY PROFESSION IN 10 YEAR'S TIME

Technology, risks, laws, and individual preferences all will have evolved over the next decade. Yet, in some ways they will all largely stay the same. Inherently human desires to learn, grow, play, communicate and socialize will persist, but how those interactions materialize may be quite different. Just as we've seen a fairly dramatic migration of these activities to the digital space over the last decade, we could easily see a further step-change 10 years from now. In addition, by 2026, even the most remote corners of the world will likely be online, bringing both benefits and risks to an even larger number of global digital citizens, namely youth. In anticipation, we have an opportunity to inform and educate young and older future-users alike; to encourage them to exercise safe online habits and practices, and to empower them to always be their best digital selves.

A SHARED RESPONSIBILITY

Protecting children online is a shared responsibility among parents, teachers, school officials and other trusted adults in a child's life, as well as government, the technology industry and civil society. Each of us has a role. For instance, parents can lead by example when it comes to safe, responsible and appropriate use of technology and online services. They can watch for signs of inappropriate use among young people and encourage empathy in online environments. Meanwhile, educators can teach digital literacy, civility and etiquette, and they can invest in their own professional development to try to keep up with kids online. The technology industry can embrace "safety by design" in products and services, encourage civil behaviour among customers, and endeavour to educate consumers about the forever-changing online risk landscape. Governments can ensure appropriate laws are in place, enforce those laws, and grow public-private partnerships. Children and young people also have a role to play, including living the "golden rule" online and off, and respecting use rules and codes of conduct in various online formats.

THE MAJOR PLAYERS

There are so many individuals, companies, governments and organisations doing so many innovative and interesting things, and I'm honoured to work with several of them. I am part of the WePROTECT Children Online International Advisory Board, INHOPE's Advisory Board, and the board of directors of the Cyber Security Alliance, the Technology Coalition and the Family Online Safety Institute. All of these organisations—and many more—are innovating and working to keep children safe online and, thereby, at least indirectly helping them to succeed in our 21st century digital world.

Better child online protection desperately needed in India - Telenor is stepping up

Lack of digital literacy and online safety measures in India mean children are exposed to a greater risk of cyberbullying and sexual exploitation. The CEO of Telenor India speaks out on measures they're taking to protect them

Today's children can't imagine life without a social networking profile, sharing photographs online or gaming with their friends. In India over 30 million children have a mobile phone and an estimated 134 million are expected to come online by 2017.

While the internet provides opportunities for India's youth to learn and share, the lack of digital literacy and online safety measures mean children are exposed to a greater risk of cyberbullying, identity theft and sexual exploitation.

In 2013, the Delhi High Court noted that India is behind the times on online protection of children. Three years on, changes in child online safety-related policies and implementation of digital literacy programs in schools have moved forward very slowly. While policymakers are quite active in this area, the discussion is centered more around cybercrime than child protection and initiatives seem fragmented. But while progress may be slow in general, one of the country's international mobile internet providers, Telenor, is committed to lead by example in the area of child online safety and digital literacy.

DIGITAL LITERACY DEFICIT

"We did a global study on child online safety in 2012 and out of 12 countries we found children in India are in the highest risk category due to a combination of increased access enabled by affordable internet and smartphones, and low resilience with parents and children lacking the knowledge of how to safeguard themselves against different cyber threats," says Sharad Mehrotra, CEO of Telenor India.

"We responded by launching our Webwise programme, which educates children on how to protect themselves online. We started it in 2014 and we have 17 volunteers who visited 170 schools so far and 35,000 students have benefited from the workshops on cyberbullying and the role of parents in child online safety."

PARENTAL RESPONSIBILITY

The lack of education on the risks of going online is widespread, particularly in rural areas where, according to Mehrotra, children as young as six are browsing the internet with no parental guidance or supervision. According to a survey conducted in 2014 by the Associated Chambers of Commerce of India (Assocham), most underage kids on Facebook first got help from their parents to create their accounts. The survey said 75% of the parents of 8-13 year-olds on Facebook are aware of their child signing up for the site and many "initially knowingly allow their children to lie about their age".

To help parents understand the complexities of going online, Telenor produced a guide book that gives direction to parents on how and why they should talk to their kids about the internet and the importance of creating strong passwords, privacy settings and parental controls. "As parents, even if we are not tech-savvy, it is our responsibility to talk to children about their internet habits so they feel comfortable to talk to us if they foresee someone trying to harm them," says Mehrotra. "We need to monitor their activity and have rules around their internet use."

IMPROVING EFFORTS

Improving child protection online is desperately needed in India, but so is having the right protocol to deal with a crime if it does occur. To help address this, Telenor is looking to team up with Child Helpline India to build capacity of its staff to know what to do if a child becomes a victim online.

"Results from the workshops suggested at least every second child had experienced some sort of cyber-harm," says Mehrotra. "About half of them had received demeaning or indecent messages, some had been humiliated by public upload of their photos or had rumours spread about them online.

"We are working with staff to understand what kind of scenarios can come up and how to deal with them," says Mehrotra. "There is a big capacity building element. Staff haven't dealt with this type of problem before. We are putting together a panel of experts to train them to counsel children and to link it to services for their long term care and rehabilitation."

ABUSE FILTERS

Telenor Group collaborated with the European Commission's CEO Coalition and Interpol to become the first mobile operator in the world to introduce safety and child sexual abuse filters for mobile phones in all markets they operate in.

"The filters mean any site that is related to known child sexual abuse content is automatically blocked in India," says Mehrotra. "The message that comes up when a site is blocked contains the number for Child Helpline India. To help sign-post people to this service, we have actually integrated the helpline number in phone SIMs for easy access. There is no way a child can miss it when they look at their phone."

In order for children and young people to actively participate in the world today, it is critical they are able to take full advantage of ICTs and proactively manage any risks they encounter online. Telenor and its partners are making sure child online safety moves up the agenda so that children and young people in the third largest telecom market in the world can enjoy the internet safely.

05 Chapter 05
Promoting digital technology as a mode for increasing civic engagement

INTRODUCTION

The Convention on the Rights of the Child, in article 13, states that "the child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice." Companies can fulfil their respect for children's civil and political rights by ensuring that technology, legislation and policies developed to protect children from online harm do not have the unintended consequences of supressing their right to participation and expression or preventing them from accessing information that is important to their well-being.

At the same time, businesses can also support children's rights by offering mechanisms and tools to facilitate youth participation. They can emphasize the Internet's capacity to facilitate positive engagement in broader civic life, drive social progress, and influence the sustainability and resiliency of communities, for example, by participating in social and environmental campaigns and holding those in charge accountable. With the right tools and information, children and young people are better placed to access opportunities for health care, education and employment, and to voice their opinions and needs in schools, communities and countries. They can access information about their rights and make demands for information, whether in terms of the right to information on matters that affect them, such as their sexual health, or political and government accountability.

Companies can also invest in the creation of online experiences that are appropriate for children and families. They can support the development of technology and content that encourage and enable children and young people to learn, innovate and create solutions.

Companies can, in addition, proactively support children's rights by working to close the digital divide. Children's participation requires digital literacy – the ability to understand and participate in the digital world. Without this ability, citizens will not be able to participate in many of the social functions that have become 'digitized', including but not limited to filing taxes, supporting political candidates, signing online petitions, registering a birth, or simply accessing commercial, health, educational or cultural information. The gap between citizens who are able to access these forums and those who cannot due to a lack of Internet access or digital literacy will continue to widen – placing the latter groups at a significant disadvantage. Companies can support multimedia initiatives to provide the digital skills that children need to be confident, connected and actively involved citizens.

COMPANIES CAN ALSO INVEST IN THE CREATION OF ONLINE EXPERIENCES THAT ARE APPROPRIATE FOR CHILDREN AND FAMILIES.

A DAY IN A LIFE

KARLA MARIA RIVAS DE REYES Digital education in El Salvador: 'we're giving hope to a hard working country'

Meet Karla Maria Rivas de Reyes, CSR and communications director for Tigo/Millicom in El Salvador, who helps telecommunications company, Tigo, support public schools by providing them with connectivity, equipment, leadership training and workshops

Part of the Millicom Group, TIGO is a brand that delivers affordable, available and accessible digital products in an easy-to-use, customer-focused way. Our vision is to empower all to advance in life and find joy. With presence in the emerging markets of Africa and Latin America, we believe in change, in making people's lives easier and better through technology.

Tigo began operations in El Salvador in 1992 and is today the biggest telecommunications operator and cable company in the country.

TIGO'S IMPACT

At Tigo El Salvador, our largest social investment program focuses on digital education, where we support public schools by providing them with connectivity, equipment, leadership training, and educational technology workshops for students, parents and teachers. The impact goes far beyond giving away computers. We are seeing lives change in the surrounding communities, where children have opportunities for success their parents did not have.

MY HAPPINESS AND MY FEARS

When we open a new digital learning centre, the kids can't wait to get inside. They run inside and say "this is mine" (referring to a computer). Watching them look at the screen as if they were in Disneyland … that makes me really happy.

Success to me means that every Salvadoran knows what it is to "get connected" and "to chat", is able to use their mobile phone to pay bills, save money and be safe by doing it from home. It is great to work for a company that helps make that happen.

It bothers me to know that children fight every day against fear of gangs, while walking to and from school. Gangs limit their growth and keep them prisoners in their own homes.

Accessibility gives information, information gives knowledge and knowledge gives opportunities to escape poverty. So accessibility is key for us to reduce violence and move forward.

HOW I IMAGINE MY PROFESSION IN 10 YEAR'S TIME

In 10 years everything will be digital. We can't even imagine how different life will be. As my profession is communications and corporate responsibility, I think it will be a big challenge to promote digital inclusion and work so that the digital gap does not grow, and on the contrary, ease opportunities and accessibility for all.

> **IT BOTHERS ME TO KNOW THAT CHILDREN FIGHT EVERY DAY AGAINST FEAR OF GANGS, WHILE WALKING TO AND FROM SCHOOL**

WHAT I THINK ABOUT COLLABORATION

It's all about engagement, transparency and being open-minded. It sounds simple but can be surprisingly difficult when people are used to distrusting each other's motives. All participants should focus on common goals and cause. When it comes to child safety online, we all share the objective of empowering children to reap the benefits of digital inclusion in a safe way. What each stakeholder is able to do about it will differ and how each stakeholder will benefit from the outcome may be different. But ultimately we are together empowering a new generation.

In many areas of corporate responsibility we will have more to gain by working together with our competitors than each in our corner. Child online protection is no different. This is why in El Salvador we asked UNICEF to help us pull together all of the mobile operators in the country to sign a joint pledge to work together.

MY THOUGHTS ON THE LEADING CHANGEMAKER

UNICEF works for a world in which every child has a fair chance in life. UNICEF recognises that having access to the digital world is a right, and provides a lot of helpful guidance to different stakeholders on what they can do to better protect children online. With a presence around the world and working closely with both governments and the private sector, I think it is the best institution to lead the change and bring together the right allies.

MY NEW IDEAS

Often, people live far from voting centres. An app which allows people to vote electronically would be great. It would allow you to have real time results, increase people's participation and decrease risk of electoral fraud. A similar app could exist for kids, allowing them to give their vote or views on decisions adults make that affect them. As connectivity is all around, democracy prevails.

An interesting program would be to create digital public playing centres, establishing them in the middle of the city, crowded places where kids, no matter of their economic status, could go and just play with technology. Parents would have an area too, to play and learn about child online protection tips.

Brave new world: how are children in developing countries protected online

Technology is transforming the lives of children and young people all over the world but stakeholders need to work together to ensure the benefits outweigh the risks

In Diriamba, Nicaragua, an eight-year-old boy reads stories on a donated laptop. Teenagers in Kampala, Uganda, use a mobile app to speak out about social issues. And in the Mandalay region of Myanmar, tablets help students to complete their secondary education.

Around one in three internet users is under 18 (pdf) and millions more will soon be connected. With the United Nations calling for universal internet access in the least developed countries by 2020, closing the digital divide is a global priority.

But how can the socio-economic benefits of connectivity for children in developing countries be balanced with the risks of misuse? And who can help the next generation to enjoy technology and not fall prey to its darker side?

SAME RISKS, ADDITIONAL BARRIERS

Access to the internet and mobile devices empowers young people in areas like education and civic engagement but it also poses challenges to their wellbeing, wherever they are in the world. Unsuitable content, privacy breaches, sexual exploitation, bullying, radicalisation the risks children face online know no boundaries.

Historic digital inequality means that young people in developing countries – many of whom have bypassed computers and gone straight to mobile – could be especially vulnerable. Without the right digital skills, children might fail to recognise inappropriate content, conduct or contact. If their parents are not technology-literate or their teachers have no ICT qualifications, their support network is limited.

One thing is clear: closing the connectivity gap is not just a case of improving availability, affordability and reliability; it is about embedding technical skills, raising literacy levels (both online and off) and increasing resilience across entire communities.

LEGISLATION MUST CONSIDER CHILDREN'S RIGHTS

Although in many countries, basic legal frameworks are lacking, online safety is making its way up the political agenda in some developing nations such as Namibia. Micaela Marques de Sousa, UNICEF representative in Namibia says, "We are witnessing a major drive of reforming legislation to ensure child online protection as a result of an innovative partnership with the UK government.

"UNICEF's strategic work with the government of Namibia, including the ministries of information, gender, justice as well as the private sector, will ensure that by the end of this year, we have laws that will criminalise child pornography in all its forms. This will bring Namibia's legislation in line with the highest international standards governing child online protection. We hope that this progressive legislation will serve as a role model for the region and beyond," she added.

Namibia may be a role model but with technology evolving at such great speed, child protection laws and regulations often cannot keep up. As Milka Pietikainen, vice president of corporate responsibility at telecommunications and media company Millicom, says, "The main challenge is that the speed of development of new online services and solutions outpaces legislative developments, so laws may always be lagging behind. There are, however, some key areas where it is very important to have the legislation in place to protect children, in particular in criminalising child sexual abuse content."

Where illegal content is concerned, global initiatives like INHOPE, which works with law enforcement agencies to combat online child sexual exploitation, have a positive impact. In other areas, local context cannot be ignored. Family structure, gender roles and cultural norms must be considered when developing governance frameworks.

While teenagers in the UK can easily access information about sex and relationships online, it might not be deemed appropriate elsewhere, for example. Despite many arguing that the internet should not be censored, in some countries there might be pressure to block culturally-sensitive online content on issues such as sexual orientation and female empowerment.

In the race to protect children online, there is concern that their rights are not always considered; that a lockdown approach could limit the benefits of technology and prevent freedom of expression. With this in mind, UNICEF and the London School of Economics/EU Kids Online are investigating children's rights in the digital age and a recent paper for the Global Commission on Internet Governance included several recommendations.

MULTI-STAKEHOLDER APPROACH

Network providers, app developers and other technology companies also play an important role. As the Guidelines for Industry on Child Online Protection state, "... businesses have to strike a careful balance between children's right to protection and their right to access to information and freedom of expression."

Mobile operator Telenor Group believes that a supportive ecosystem can help to address digital risks and increase children's resilience. It runs a number of child protection programmes, including CyberSAFE in Schools in Malaysia, and also supports global initiatives such as the Mobile Alliance Against Child Sexual Abuse Content.

Telenor's head of social responsibility, Ola Jo Tandre notes, "In most cases, I believe it is possible to achieve better protection and greater resilience among young people without going down the route of changing the legal frameworks. I would like to see more research into what children see as the real threats, better awareness among children, parents and teachers of how to tackle those threats, and more institutional capacity to help children recover from negative experiences."

Child safety online is also a priority for Millicom. In Paraguay, for example, its Tigo business works with UNICEF to provide education materials and tools (pdf). Millicom's Pietikainen acknowledges, however, that there is no one-size-fits-all solution.

"Children come online as they come into the world: naturally curious and innocent and, as offline, they need guidance from adults on how to navigate and behave," she explains. "In Europe, parents are being informed with magazines and online resources. These models work to a large extent in our Latin American markets but they do not necessarily work in environments like Africa where many parents do not have fully internet-enabled devices, devices are shared, or services are pre-paid. We need to think of completely new ways of raising awareness."

Empowering the digital citizens of the future

From the homes and classrooms of Diriamba, Kampala and Mandalay to the congress centre in Davos, connectivity is a hot topic. The Fourth Industrial Revolution is here, claimed politicians and business leaders at the World Economic Forum, with new technologies "blurring the boundaries between people, the internet and the physical world."

For young people, the transformative potential of the internet and mobile devices is enormous but the safety challenges must be addressed. As we head towards 2020, governments, businesses, NGOs, educators, parents and other stakeholders must continue working together to help children everywhere become resilient and responsible digital citizens.

A DAY IN A LIFE

CARLA LICCIARDELLO
A safe and trustworthy cyber-space: 'together we have come a long way'

Meet Carla Licciardello, child online protection focal point, International Telecommunication Union (ITU). Carla works for ITU, an agency of the United Nations, to engage partners from all sectors of the global community in a dialogue to tackle child online safety and foster digital literacy among future generations

ITU is the United Nations agency for information and communication technologies – ICTs. We allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies interconnect seamlessly, and strive to improve access to ICTs to underserved communities worldwide. ITU is committed to connect all people around the world – wherever they live and whatever their means.

ITU'S VISION

The power to unleash the true potential of ICT lies in the hands of children and young people. ICTs are an excellent tool for children's development, providing them the opportunity to learn, create, and engage in innovative problem solving – and the "democratisation" of ICTs means that this is becoming more prevalent.

Despite the profound benefits that ICTs can offer, children and young people are facing new and significant risks. Children can be exposed to inappropriate content or contact, such as potential sexual predators. They can suffer reputation damage through the publishing of sensitive personal information, either online or through "sexting", having failed to grasp the long-term implications of their digital footprints. Children may engage in risky or inappropriate behaviour that creates negative repercussions for themselves and possibly others.

ITU has made this a priority issue, and launched the Child Online Protection (COP) initiative in 2008. The COP initiative engages partners from all sectors of the global community in an international dialogue to tackle child online safety, and to create an empowering online experience for children. COP brings together partners from all stakeholder groups to protect children online through forums such as the Working Group on Child Online Protection as well as through our global reach as a United Nations agency. Together we have come a long way: child online safety is now high on the political agenda for many countries, and has become a top priority for a wide variety of stakeholders, including businesses and financial institutions. Our common goal of ensuring trust in cyberspace cannot be achieved by stakeholders working in isolation. In an increasingly networked world, which knows no borders, it is vitally important that various efforts are well aligned towards the common goal of a safe and trustworthy cyberspace.

FUTURE-GAZING

In 10 years, I believe the internet – which is still in its infancy – will blossom further. Trends in the digital environment point to more wireless connectivity at exponentially higher speeds and the transfer of vast amounts of data on the go. This will mean picking up on our achievements today to ensure that our networks are fail safe and future generations will be able to surf cyberspace in a secure environment.

As we continue to work towards enabling the use of ICTs in both developing and least developed countries – where the remaining billion internet users will primarily come from – we must leverage widespread access to ICTs to enable social development and environmental protection, generate wealth, and deliver health care and education to children around the world.

We must also recognise that we can never achieve the full potential offered by ICTs, if children, wherever they live, do not have trust in their usage. We can only ensure this trust by working together with stakeholders from all nations, as new challenges arise and new tools and coordination mechanisms will need to be developed and shared.

THE VITAL ROLE OF COLLABORATION

In order to reduce the risks of the digital revolution while enabling more children and young people to reap its benefits, governments, civil society, local communities, international organisations and the private sector must come together with a common purpose. The technology industry has a critical role to play in establishing foundations for a safer and more secure use of internet-based services and other technologies.

For example, public and private partnerships are key to building a coordinated national, regional and international response to the problem of online child sexual abuse, while ensuring information sharing among different stakeholders. Industry, law enforcement agencies, governments and civil society must work closely with each other to ensure that adequate legal frameworks in accordance with international standards are in place. Such frameworks should criminalise all forms of child sexual abuse and exploitation; protect children who are victims of such abuse or exploitation; and ensure that reporting, investigative and content removal processes work as efficiently as possible.

THE LEADING CHANGEMAKER

The UN plays an important role as a global convener and facilitator for stakeholders to come together to discuss, identify and implement solutions towards building a universally available, open, secure and trustworthy internet.

THERE'S MORE TO BE DONE

I believe we need to stimulate the production of creative and educational online content for children as well as promoting positive online experiences for young children. Technical measures can be an important part of ensuring children are protected from potential risks , but these are only one element of the equation. Parental control tools, awareness raising and education are also key components that will help empower and inform children of various age groups, as well as parents, caregivers and educators.

Stakeholders can proactively support children's rights by working to close the digital divide. Children's participation requires digital literacy – the ability to understand and participate in the digital world. Without this ability, citizens will not be able to participate in many of the social functions that have become digitised. Therefore, it's crucial to develop programmes that support multimedia initiatives to provide children – particularly those in rural and underserved areas – with the digital skills they need to be confident, connected and actively engaged citizens, and enable them to fully participate in the digital world safely.

We must also develop online platforms that promote children's right to express themselves; facilitate participation in public life; and encourage collaboration, entrepreneurship and civic participation. Finally, it's important to design programmes in collaboration with local civil society and government to expand universal and equitable access to information and communication technologies, platforms and devices – and the underlying infrastructure to support them.

Investing in girls to promote gender equality and unlock potential

by Nokuthula Prusent

The Techno Girls programme in South Africa, is paving the way for young girls to engage in careers in technology, engineering, maths and science

Experience. Learn. Grow. This is the motto of the Techno Girls programme in South Africa, which through direct job exposure, is paving the way for young girls to engage in careers in technology, engineering, maths and science. Started as a supplement to the Girls and Boys Education Movement (GEM/BEM), which aims to help boys and girls complete schooling, the Techno Girls project was launched by UNICEF in partnership with the South African department of education in an effort to empower girls from disadvantaged communities. The programme is a response to some of the challenges posed by the legacy of apartheid, which contributes to the increasing socio-economic disparities that exist between men and women and relegates vulnerable children to the fringes of society.

Previous studies have revealed that girls underperform boys in the subjects of math, science and technology, which causes them to lose interest in these subjects as they go through school. This directly results in fewer females participating in the job sectors where the most growth is occurring, leaving them with fewer options for generating income.

Research shows that a shortage of professionals with skills in engineering, sciences, financial management, and information technology are an impediment to economic growth in both public and private sectors. In a country like South Africa, where more than half of the population are women, gender bias can further inhibit social and economic development.

Youth mentorships that lead to job placement have become a major focus of the South African government as part of an initiative to halve poverty and unemployment by 2014. With the overarching goal of making underprivileged girls more employable, Techno Girls engages schools and corporations to generate girls' interest in the technical fields where they are so under-represented.

The partnerships unlock young women's hidden potential and give them the confidence to pursue careers in fields currently dominated by men.

During the holiday season, the programme carefully matches school girls from Grades 9-12 with their career of choice where they are assigned mentors who guide them in the roles, responsibilities and risks of the profession. In addition to participating in job tasks at the workplace, the girls can witness real life applications of technical subjects outside the classroom. Its focus is not so much on giving girls access to technology, but to provide exposure to the world of work which in turn grants them the opportunity to engage with technology. The end result is that girls going through the Techno Girl curriculum feel motivated by what they have seen and experienced, turning that motivation into focus on their schoolwork.

For the girls in the programme, the job shadowing presents a unique opportunity to connect and build relationships with occupational role-models in influential positions, which instils in them a sense of obligation to do their best at achieving life goals. In the long-term, participating organisations also benefit from the partnership as they gain access to a pool of women that they've helped mould to fill job gaps, increase gender representation and ultimately create human capital to enhance economic growth.

The impact of the programme since its inception in 2002 has been positive with as many as 20,000 girls enrolled in corporate mentorships. Through the programme, girls have received scholarships, sponsorships, and preference in their chosen professions to make the dreams they thought impossible, a reality. Techno Girls is also in the process of revamping its project to include girls who have completed the curriculum, or Alumnae, and are currently enrolled in university. Continued investment in the girls ensures that the networks they are building and their drive stay with them long after they leave school.

Is technology in the classroom good for children?

by David Nield

Blamed for a decline in maths test results, handwriting ability and attention spans, critics say technology in education often misses the mark

Technology is an increasingly important part of today's classrooms. Globally £19bn is expected to be spent on educational technology by 2019, according to analysts Gartner, and UK schools spend £900m annually. But is it helping provide children with the skills they need for the jobs of the future or disconnecting them from the world around them?

A recent report from the Organisation for Economic Co-operation and Development suggests there could be a detrimental effect, finding that computers in classrooms are being linked with a decline in test results for maths, science and reading.

Elsewhere, iPads are being blamed for a decline in handwriting ability; technology terms like "broadband" are ousting words associated with nature, such as "acorn", from the Oxford Junior Dictionary; and some claim attention spans are being eroded by constant smartphone use.

TECHNOLOGY IS NOT THE PROBLEM

For Andrew Manches, chancellor's fellow at Edinburgh University's School of Education, it's the way technology is used in the classroom that should be under most scrutiny.

"'New' computing skills ... aren't so different to traditional skills," he suggests. "An ability to think logically, the ability to communicate ideas at different levels. I personally believe that the most important skill for children today is being flexible ... The world is becoming harder to predict." Used in innovative ways, with the right teacher training and infrastructure support, Manches says technology can open up new ways of learning and bolster core skills. However, applied in the wrong way, such as using tablets to play rote learning maths games, and it can have a detrimental impact. Learning apps are often like "chocolate coated broccoli", says Manches, based on dull and unhelpful learning approaches disguised with whizzy sound and colour effects.

Chris Davies, vice president of Kellogg College, says technology is changing children's abilities in "quite haphazard" ways. He too is concerned about how technology is being applied in lessons and how the trend of providing iPads in classrooms can undermine some skills: "Writing on screen keyboards is much harder and does not in general support the production of extended writing."

Davies says a number of schools are exploring the use of Google Docs to encourage skills considered valuable for the workplace, such as collaboration. But he questions whether this supports the development of other writing skills such as reviewing and redrafting cohesive texts.

GETTING THE BALANCE RIGHT

There are schools at that are shunning technology completely to refocus on practical skills and cultivating creativity. One of these, Silicon Valley's Waldorf School of the Peninsula, claims that despite its no-tech approach students pick up digital skills quickly and that many of its graduates go on to careers in the computer industry. Meanwhile campaigns such as the Wildlife Trusts' Every Child Wild initiative aim to reconnect children with nature amidst a daily diet of touchscreens, social media and computer use.

"This isn't about saying that children should never use the technologies available to them," says Lucy McRobert, campaign manager for the Wildlife Trusts. "Rather, by allowing them to spend time regularly in wild places, we can help them be healthier and happier, they'll do better at school and concentrate harder, they'll have more confidence and be more physically fit."

For many in the education profession it's about keeping a savviness and understanding of new technology in balance with core life skills that are always going to be useful no matter how rapidly tools and methods change. "The more that young children are exposed to technologies of learning which substitute for and short-circuit their sequential problem-solving and learning experiences, the more these latter abilities will be compromised, quite possibly in damaging way," says psychologist and childhood learning campaigner Dr Richard House.

PROTECTING THE SKILLS FUTURE EMPLOYERS WILL ALWAYS DEMAND

We may lament the way a reliance on gadgetry is eroding handwriting and spelling skills, but House says it's qualities such as creativity that businesses really want from their future employees — and these are the skills that should be most fiercely protected.

It comes back to the way technology is integrated into the classroom. Lee Parkinson, a primary school teacher who trains other teachers in the use of ICT, says modern-day gadgets should only be used to "go beyond what can be done on paper".

"When technology is used to its potential and with purpose in the classroom, it can provide children with a range of skills that I feel would benefit them in the world they are growing up into," he says, citing the ability to create rich content such as images, video and interactive presentations, share information globally and communicate with other people.

Jim Taylor, author of Raising Generation Tech: Prepare Your Children for a Media-Fuelled World, agrees that the use of technology in the classroom should be a tool, not an approach to education.

"On the plus side, they are learning important tech skills such as keyboarding, coding, and how to use the internet to gather information. On the minus side, there is evidence that they aren't learning the emotional and social skills that are so important for success in work and life," he says. According to Taylor: "What will make children successful in their careers is their ability to think originally, creatively, and expansively".

Will smart toys make parents lazy?

by Mark Harris

Pitched as the next must-have developmental tools, critics worry about hi-tech Barbie dolls and bears eroding parent-child interaction

The digital revolution means that modern toy shops contain more computing power than a space shuttle. Interactive and connected toys promise to bring your child's favourite characters to life, promote coding skills, and even diagnose medical conditions.

Hello Barbie is a $75 (£53) doll that can chat with children for hours on end; Kibo is a robot that toddlers program using coloured cubes; and Spanish researchers are developing hi-tech building blocks that can automatically detect neurological disorders.

But are smart toys really the next must-have developmental tools, or just digital babysitters that could leave children snuggling up at night with corporate marketers and malicious hackers?

"Young children are born into a digital world that we as their parents and educators were not," says Chip Donohue, director of the Technology in Early Childhood Center at the Erikson Institute in Chicago. "Play evolves, and modern technology can help a child feel more empowered, capable and competent."

Take toys designed to stimulate computational thinking: logical skills and practices considered essential for solving complex problems. Veronica Lin tested several such toys while studying human-computer interaction at Wellesley College, Massachusetts. She watched 38 children aged from five to nine as they played with the Kibo robot and littleBits, a modular robotics system.

"Digitally-enhanced objects appeared to elicit more smiles and laughs for all users, and led to higher levels of excitement," she concludes in her paper. "Both toys allow children to engage effectively in collaboration, and children were noticeably more engaged when playing with [their] digital aspects."

Smart toys might even help catch medical problems before they are obvious, thinks Maria Luisa Martin-Ruiz, an electronics engineer at the University of Madrid. "Early and effective identification of children at risk for developmental disorders remains a [unresolved] task," she says. Her team's solution is "smart cubes" packed with sensors that can measure their position and motion.

Children as young as one would then be allowed to simply play with the cubes, with researchers analysing the data in the hope of detecting problems with the child's motor skills, timing, balance or spatial awareness.

While the smart cubes are still being developed, toys that are nearly as impressive are already on the shelves. Hello Barbie can listen to a child's questions and respond with one of 8,000 perky phrases, while the Fisher-Price Smart Toy bear learns how your child plays and recommends new activities. Both use domestic Wi-Fi links to connect the toy to servers online.

"The advantage of the cloud is that you can do learning across platforms ... What one robot [toy] learns, it can share with all the others," says Ken Goldberg, a professor of robotics and automation at the University of California, Berkeley. "But opening up a channel between the outside world and your robot does make it vulnerable. When you're dealing with a kid, you can imagine a very diabolical scenario like Chucky."

Hello Barbie and Smart Toy have both had privacy scares, with security firms highlighting vulnerabilities that had to be patched, like a computer update. "A lot of people were excited to claim that they had 'hacked Barbie'," says Martin Reddy, chief technical officer of ToyTalk, the company behind Hello Barbie's interactive features. "But no one has actually demonstrated that. No one has eavesdropped on any kid talking to Barbie, and no one has made the doll say anything different from the phrases she is programmed to say."

In fact, smart toys generally have more protections built in than smartphone digital assistants like Siri, Cortana or Amazon Echo. This is because services designed for children in the US have to comply with the Children's Online Privacy Protection Rule, or COPPA. This regulation controls the use of data collected from anyone under 13, including personal information and audio files, and forbids services from sharing it with other companies or using it for marketing without explicit parental consent.

"Hello Barbie doesn't ask for your name, age or gender," says Reddy. "We don't want more personal information, [as] it just makes our lives more complicated. We only want data for speech recognition purposes to help it work beautifully."

While security and privacy have yet to emerge as major problems for smart toys, they can still suffer the usual troubleshooting pains of hi-tech gadgets. Luke Reiser bought his granddaughter a Hello Barbie for Christmas but had difficulties getting it online. "We are now here with our crying four year old and a Barbie that simply repeats, 'Uh oh I can't find a Wi-Fi network'," he wrote in a review on Amazon. Other users have complained that Hello Barbie is a poor conversationalist.

"I do worry that because these toys are seemingly interactive and seemingly relationship-oriented, we might be more willing to embrace them compared to our caution around screen time," says Donohue. "The research is pretty clear that parent-child interaction helps early literacy and school readiness. In the end, we need to empower parents and help them understand that they should not hand off those responsibilities to a device."

Banning teenagers from social media would be an attack on their human rights

by Larry Magid

New data protection rules could block under-16s from social media access without parental consent, denying them rights to expression and information

The European commission's General Data Protection Regulation, voted on last week, aims to give consumers more control over their personal information and more transparency on how their information is used by companies and governments.

As far as adult internet users are concerned, the reforms presented in these new regulations are mostly empowering. But, whether intentional or not, they could wind up disempowering and disenfranchising millions of young internet users.

When first drafted, the regulations generally reflected the status quo in most of Europe, the US and other regions, by requiring parental consent before commercial services could process personal information from children under 13. But, at the last minute, the age was raised to 16, effectively banning children from accessing Facebook, Snapchat, Instagram and other services without parental consent. After an outcry from technology companies and child protection organisations, the provision was watered down with the proviso that member states can lower it back to 13 .

We don't yet know how individual countries might respond to the age provisions in the regulation, but Janice Richardson, author of the Council of Europe's internet literacy handbook, urges governments to take their time deciding and "consult with all sectors including parents, children, experts, schools and regulators" before making a decision.

Social media, even when it's operated by private companies, is where young people go to express their opinions, interact with peers and family, learn about the news, as well as obtain health information and access to services. Depriving youth from access violates their rights of expression and information as well as their ability to participate in civic engagement.

Of course, there will be teens who are able to get their parents to fill out the necessary forms to allow them to participate in social media, discussion forums and other online venues but there will be others who – for a variety of reasons – will be unable to obtain this permission. This could result in unequal access for children whose parents may not have the literacy, local language skills or technology skills to provide the consent, as well as those parents who may be afraid to fill out forms that they fear might get into the hands of immigration authorities or other government officials.

In increasingly diverse societies, I fear a lack of access to the internet could interfere with the ability of some youth to assimilate into new environments and to explore social, political and religious values that may differ from those of their parents. This is a time when we should be breaking down barriers to interaction and social engagement among youth, not erecting new ones.

While social media has been linked with the radicalisation of some teens, young people are able to use online platforms to connect with each other, promoting understanding rather than violence and extremism. Nobel prize winning youth activist, Malala Yousafzai, for example, has advised social media is the easy place to start taking action against injustice.

The reality is that young people have rights and it is the responsibility of government to protect those rights, regardless of whether their parents are willing to fill out permission slips. In the US, we have a first amendment that says nothing about having to be over a certain age to enjoy the right to free speech. In Europe, countries have ratified the UN Convention on the Rights of the Child which grants children "the right to freedom of expression" including the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print". And there is nothing in that convention that requires parents to sign off on those rights.

Legal and moral issues aside, there are also practical considerations. Even the current law, which effectively restricts access for children under 13, is ignored by millions of pre-teens around the world who lie about their age to access social media, so it's hard to imagine how any government expects teens to refrain from doing likewise. The real effect of this regulation is to encourage European teens to ignore the law and lie.

The good news is that it's not too late for individual countries to reject the call to limit the free speech of teens and keep the age for participation at 13 where it is now in most countries.

© UNICEF/UNI118945/Tylle

How Facebook and Twitter changed missing child searches

Every second counts when a child disappears and social media sites can help speed up investigations

Every three minutes a child is reported missing in the UK; across the EU that number rises to one child every two minutes. In the US, the FBI recorded almost 467,000 missing children in 2014, which is close to one reported every minute.

In the US, milk cartons, posters, flyers, meetings and traditional news reports formed the main missing child search channels until 1996, when Dallas-Fort Worth broadcasters teamed up with local police to develop a warning system that interrupted regular programming on television and radio broadcasts, and highway signs.

The service, Amber Alert, is used only for the most serious of cases, sending out messages via email, text, traffic signs and digital billboards, as well as through Twitter and Facebook.

International non-profit organisation Action Against Abduction long pressed for a similar system in the UK, but it wasn't until 2012, after the abduction of April Jones, that Child Rescue Alert was activated nationally.

In 2015, Child Rescue Alert partnered with Facebook to harness the social network's reach. Now, when a missing child case meets certain criteria of seriousness, law enforcement agencies can issue geo-targeted posts, containing a photo and description, to appear in the newsfeeds of Facebook users in the area where the child is believed to be.

"All over the world, we've seen communities rallying together in times of need, using Facebook to spread the word – and these alerts will make that quicker and help to reach more people than ever before," said Emily Vacher, trust and safety manager at Facebook at the September launch.

"Time is often a crucial element when locating vulnerable missing people who are at risk to themselves or to the public," says Metropolitan Police commander Alison Newcomb. "The use of social media supports our investigations and appeals and has achieved great results, some of which simply could not have happened through traditional communication channels."

Newcomb says the Met operates more than 400 Twitter accounts, but also works closely with other agencies. "One of the many reasons that the police come to us to help with publicity is that we have this wide network on Twitter and Facebook," says Polly Balsom, communications manager at Missing People.

Gavin Portnoy, head of digital media at the National Center for Missing & Exploited Children, which makes active use of Facebook, Twitter, YouTube, Instagram and Snapchat, has proof of the power of sharing.

In 2015 the charity created a video appeal featuring imagery of a missing girl and the person they suspected had kidnapped her. The video was shared widely and a woman spotted them.

"People feel empowered to make a difference; it's the opportunity to do something," he says.

Another example is the case of Bella Bond, a three-year-old girl whose body was washed up on the shores near Boston, US. Her identity was confirmed following an extensive social media campaign in which a computer-generated composite image was estimated to have reached 47 million people on Facebook.

"It was definitely one of those cases where we can say with great confidence that because it went viral and because as many people interacted with it, it got in front of the eyes of the right person who said 'Oh my goodness, I know that girl'," Portnoy says.

Although social media has provided police and other agencies with extended publicity tools, those same tools can also put children at risk. In Sweden, for example, a man got thousands of people to share his unofficial Facebook appeal for his missing children, but the children were living with their mother who was understood to be under protection with a new identity after leaving the man. Geoff Newiss, director of research at Action Against Abduction, says that when it comes to searching for children in abduction cases, which can be more complex than missing child cases, social media has been more of a good addition than a game changer.

"There is certainly an increase in cases where the grooming is facilitated by online contact, so in that sense technology provides risks," he says, adding that teachers need more resources to educate children about this, and that the old "stranger danger" advice needs to be updated.

Portnoy, however, says that while he recognises that social media is by no means a perfect tool, its benefits should be acknowledged. "[It] is another really positive tool that's in the arsenal of the public, of law enforcement, of non-profits like us that are trying to help."

A DAY IN A LIFE

MARIA AUXILIADORA ALFARO LARA
UNICEF: 'protecting children online is everyone's business'

Meet Maria Auxiliadora Alfaro Lara, corporate social responsibility specialist at UNICEF Geneva.

In my role, I focus on how telecommunication companies can protect and empower children, but they aren't the only ones who can

I work on the implementation of the Children's Rights and Business Principles, which are the first universal set of principles looking at how companies impact children's rights as defined by the Convention on the Rights of the Child (CRC) and what businesses can do to maximise their positive impact on children. I specialise in the ICT industry, meaning I focus on how telecommunication companies can protect and empower children through their online products and services.

WHAT I ENJOY AT MY WORK

Creating, inspiring and dreaming about what else the ICT industry can do for children is something I enjoy. Having such an unlimited spectrum of possibilities is what makes me happy. Success, for me, is when we make these opportunities possible, by realizing and creating new ones. It is the same feeling as when you see something for the first time – the same feeling as when you see a child for the first time, a child just born.

WHAT MY WORK INVOLVES

In the last year, I have participated in the development of new business tools for ICT companies to assess their impact on children's rights as part of their corporate social responsibility due diligence processes. I have carried out assessments in pioneering companies such as Lego and collaborated in more than 20 workshops and countries to launch the UNICEF-ITU Guidelines for Industry on Child Online Protection.

I work with colleagues from UNICEF units, such as child protection, research, fundraising, human resources, communication, innovation, finance; and UNICEF regional offices and country offices in three continents, to make all of this possible through the WeProtect project, across 17 countries. There is not success without collaboration.

How I imagine my profession in 10 year's time
Ten years ago, I couldn't have imagined the immense change that technologies would make on our lives or that technology would be at the heart of my work, today, in children's rights. Each evening I always check the pending tasks in the different regions where we are working on child online protection: from Guatemala to Egypt, from India to Namibia, from Bangkok to Kenya. In ten years from now, I want to check on these same countries and see that they have the highest levels of law development, technology access, education, law enforcement capacity and children online support.

History shows that we have made great advances in these regions and countries in collaboration with companies, governments and NGOs. Therefore, I have high hopes. I know that all stakeholders involved can make even bigger changes in the next 10 years. We just have to remember that children are at the heart of everything we do today, in order to build the world of tomorrow.

THE SECRET TO SUCCESSFUL COLLABORATION

When it comes to child online protection, everyone has a role. Precisely because we realise that child online protection is everyone's business, UNICEF has leveraged its success in corporate partnerships to build innovative strategies for 'shared value creation'. Firstly through business to business corporate partnerships with industry leaders, such as LEGO and Millicom, to pilot new tools; secondly, through global industry partnerships, such as the one with GSMA, the global mobile industry association, to raise awareness; and thirdly through collaboration within multi-stakeholder platforms to bring the private sector perspective, for instance, the WeProtect project.

I have learnt that the most fruitful collaboration happens when there is capacity building and knowledge sharing linked to it. As technology evolves and the online risks and opportunities for children rise, companies have a responsibility to tell their stories and to do so in a way that benefits children and the industry as a whole. By sharing corporate good practices and policies, companies set the bar even higher for all of us. At the latest UNICEF-GSMA ICT industry event in London, for instance, we had an impressive representation from more than 30 companies, including Vodafone, Orange, Tencent, Telenor, Millicom, Facebook, Microsoft, Yahoo, BT, Disney, LEGO, Nokia and Safaricom, sharing their experiences. That is successful collaboration.

> **"WHEN IT COMES TO CHILD ONLINE PROTECTION, EVERYONE HAS A ROLE."**


© UNICEF/UNI118948/Tylle

THE LEADING CHANGEMAKER

For me, a "leading changemaker" is the one developing new technology which is safe, affordable and accessible to all children. No child left behind, as we promise in the CRC. I will say this though, probably most important leading change maker for children in the world is actually the parents.

I have read and learnt a lot in the last year, for instance, from the new Global EU Kids Online, but I have also learnt from observing my own nephews. I have learnt that children live, play and participate online as if they were offline. They do homework online, they play online, they keep in contact with friends online. Therefore, children need the same resilience, the same education and the same interest from their parents as they already show in their offline world.

It's common to ask children questions about their day and what they have learnt in class. However, we never ask them about what they played online or who they met online, or what they are reading online. Why? Lack of literacy skills and fear to the unknown are some of the reasons.

APPS FOR PARENTS AND CHILDREN

I would like to see new innovative apps being developed for parents and children to interact online and to help them mutually understand the online world and its risks and opportunities.

I strongly believe that all the different sub-sectors (hardware, software and social media platforms) within the ICT industry need to work together in order to develop apps and technology which go beyond individual company products and services so that online environments as a whole fulfil children's rights. I encourage companies to review our guidelines and to see examples of how to do so, because protecting children online is everyone's business.