unicef
for every child

DISCUSSION PAPER SERIES:
Children's Rights and Business in a Digital World

PRIVACY, PROTECTION OF PERSONAL INFORMATION AND REPUTATION

DISCLAIMER

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

AUTHORS

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

ABOUT THIS DISCUSSION PAPER SERIES

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

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

CONTENTS

INTRODUCTION

Privacy and the Internet have a complex relationship. On the one hand, technology has enhanced privacy by offering more accessible means to communicate and access information. For example, activities that once required in-person visits to banks, post offices, libraries, shops and doctors' offices can now be carried out alone from the sanctity of home. Accompanying advances in encryption have made many online transactions and interactions increasingly secure, with users enjoying greater protection of their messages from prying eyes.

At the same time, new and varied threats to privacy have emerged with the growth of the digital universe. Government surveillance is exponentially easier and cheaper, painting a detailed picture of individuals' communications, movements and browsing habits. Sophisticated identity thieves, cybercriminals and hackers have exploited vulnerabilities in online banking and e-commerce platforms for financial gain. Online retailers, search engines and email providers track users' behaviour, collating and selling information to advertisers and marketers.

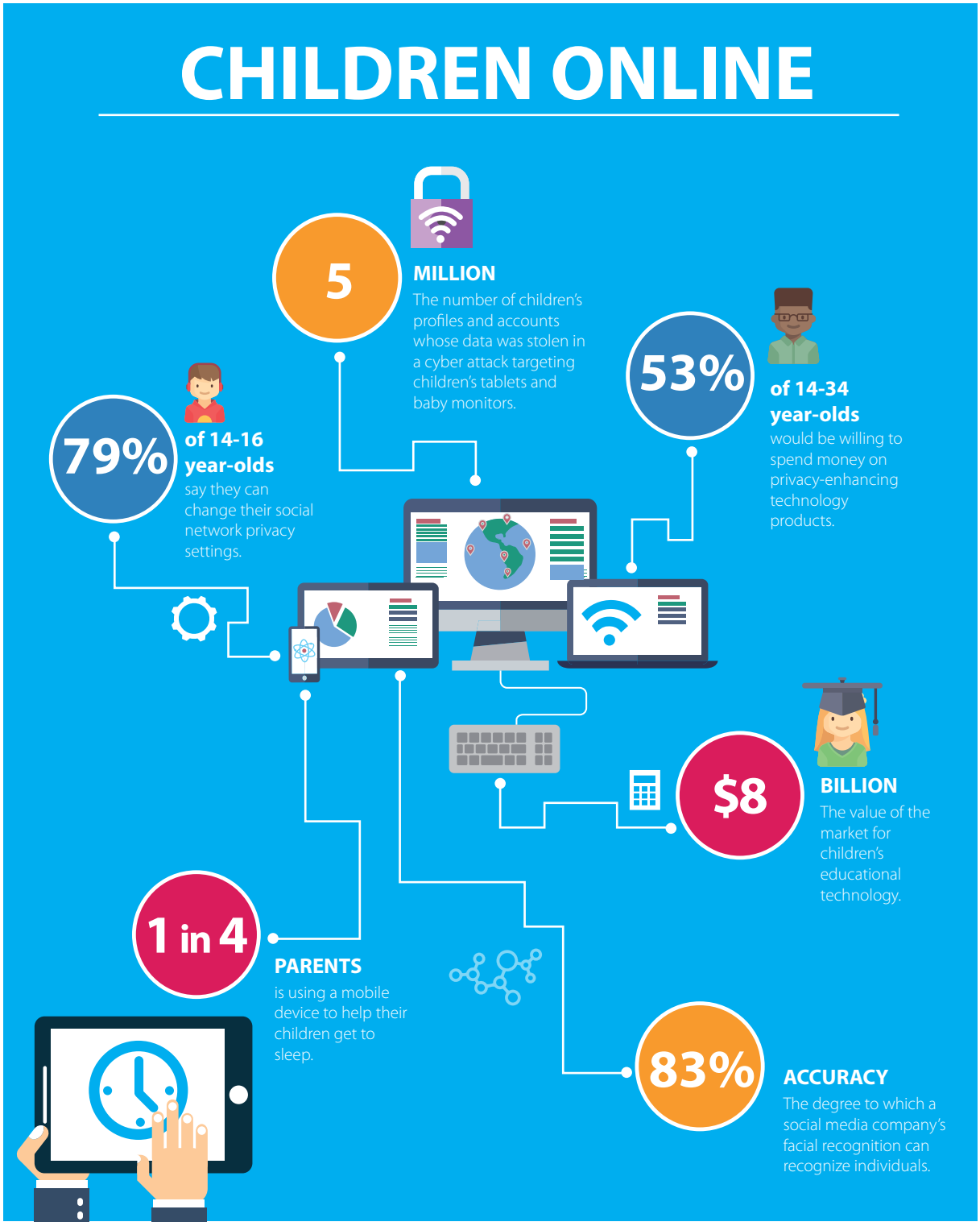
If the relationship between privacy and the Internet is complex for adults, it is doubly so for children. On one hand, the Internet offers children a way to connect and learn away from the physical oversight of adult authority figures. Communications that previously required the clandestine passing of notes behind teachers' backs can now take place on social networks, and information that could formerly be accessed only under the watchful eye of a librarian is now available in a free and unbridled way. The Internet has undoubtedly enhanced children's autonomy and independence, key aspects of the right to privacy.

On the other hand, children experience more serious threats to their privacy from a greater range of actors than any other group. Children's privacy online is placed at serious risk by those who seek to exploit and abuse them, using the Internet as a means to contact and groom children for abuse or share child sexual abuse material. Yet children's privacy is also at risk from the very measures that have been put in place to protect them from these threats. Laws designed to facilitate the prevention and detection of crimes against children online often mandate Internet monitoring and surveillance, oblige intermediaries to generate and retain personal information, and provide government authorities with access to privately-held data. Meanwhile, at home, popular parental control mechanisms to monitor and restrict Internet access promise to expose every last detail of children's online activity.

Against this backdrop, and driven by the value and power of children as a consumer demographic, companies have likewise acquired seemingly unfettered access to extensive information on children. Children's personal data is now collected almost from birth, with wearable trackers being introduced in the bassinet and infant photographs adorning parents' online profiles. Increasingly, individual children are intimately known and understood by commercial forces long before they make their first purchase.

It is fair to say that children's rights to privacy and the protection of personal information and reputation must be considered, even attenuated, in the context of the need to protect children from harm and abuse and to preserve the role of parents as a source of guidance and support in the exercise of children's rights. However, these rights must not be neglected as children's privacy enjoys equal, albeit qualified, protection under international human rights law.

As such, this discussion paper investigates the nature of children's right to privacy (Part I), explores the threats to children's right to privacy (Part II), assesses the role of the ICT sector in mitigating and ameliorating threats to children's rights (Part III), and concludes by identifying legal and policy measures for States to support and enforce the responsibilities of the ICT sector (Part IV).



Sources: Livingstone, Sonia, Giovanna Mascheroni, Kjartan Olafsson and Leslie Haddon, 'Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile', November 2014, available at <http://netchildrengomobile.eu/ncgm/wp-content/uploads/2014/11/EU-Kids-Online-Net-Children-Go-Mobile-comparative-report.pdf> (pdf); Simon, Stephanie, 'Privacy bill wouldn't stop data mining of kids', Politico, 23 March 2015, available at <http://www.politico.com/story/2015/03/privacy-bill-wouldnt-stop-data-mining-of-kids-116299>, Peterson, Andrea, 'Toymakers are tracking more data about kids – leaving them exposed to hackers', The Chicago Tribune, 20 November 2015, available at <www.chicagotribune.com/business/ct-toy-hackers-20151130-story.html>, Cassandra Report Digest, 'Online Privacy Has Become a Luxury', 27 January 2015, available at <https://cassandra.co/tech/2015/01/27/cassandra-report-digest-online-privacy-has-become-a-luxury>; 'Facebook can recognise you in photos even if you're not looking', The New Scientist, 22 June 2015, available at <www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking#.VYlaDBNViko>; Toppo, Greg, 'Techie tykes: Kids going mobile at much earlier age', USA Today, 2 November 2015, available at <www.usatoday.com/story/tech/2015/11/02/pediatrics-mobile-devices-study/75012604/>.

PART I

CHILDREN'S RIGHT TO PRIVACY UNDER INTERNATIONAL LAW

WHY PRIVACY?

Before examining the content of legal rights and entitlements related to privacy, it is important to understand their history and background. While the right to privacy is now well-established in international law,[1] understandings of privacy have continued to differ significantly across cultures, societies, ethnic traditions and time.[2] Even the United Nations Special Rapporteur on the right to privacy has remarked on the lack of a universally agreed definition, despite the fact that "the concept of privacy is known in all human societies and cultures at all stages of development and throughout all of the known history of humankind".[3]

Privacy is at the heart of the most basic understandings of human dignity, and the absence of an agreed definition does not prevent the development of broad understandings of privacy and its importance in a democratic society. As set out below, current conceptions of the right to privacy draw together three related aspects: decisional privacy, informational privacy and physical privacy.

- Decisional privacy: A comprehensive view of privacy looks to individuals' ability to make autonomous life choices without outside interference or intimidation, including the social, political and technological conditions that make this 'decisional privacy' possible.[4] This makes privacy a social value as well as a public good[5], and offers protection against outside intrusion into peoples' homes, communications, opinions, beliefs and identities.[6]
- Informational privacy: Privacy has more recently evolved to encapsulate a right to 'informational privacy', also known as data protection. The right to informational privacy is increasingly central to modern policy and legal processes, and in practice means that individuals should be able to control who possesses data about them and what decisions are made on the basis of that data.
- Physical privacy: A third and more straightforward conception of privacy is that of 'physical privacy', the right of an individual to a private space and to bodily integrity. Among other things, the right to physical privacy has underpinned jurisprudence supporting autonomy with respect to sexual and reproductive choices.

GENERAL PRIVACY PROVISIONS IN INTERNATIONAL LAW

In 1948, the Universal Declaration of Human Rights (UDHR) recognized privacy as an international human right for the first time, stating that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[7] The right to privacy became treaty law on the same terms with the entry into force of the International Covenant on Civil and Political Rights (ICCPR) in 1976,[8] and has since been incorporated into other conventions, including the Convention on the Rights of the Child.[9] As understandings of privacy have become both more nuanced and more contested, further international guidance has begun to take shape. In recent years, key resolutions and reports have made clear that rights apply

1 See, e.g., Louis Brandeis and Samuel Warren,'The right to privacy', 4 Harvard Law Review, pp. 193–220 (1890).
2 Whitman, James Q., 'The Two Western Cultures of Privacy: Dignity versus Liberty', 1 Yale Law School Legal Scholarship Repository 1 (2004).
3 A/HRC/31/64, Report of the Special Rapporteur on the right to privacy, 9 March 0216 at [20].
4 Roessler, Beate, The Value of Privacy (Cambridge: Polity Press, 2005), p. 62.
5 Habermas, Jurgen, Structural Transformation of the Public Sphere, (Cambridge: Polity Press, 1994).
6 Westin, Alan, 'Privacy and Freedom', Scribner, June 1967.
7 Universal Declaration of Human Rights, Article 12.
8 International Covenant on Civil and Political Rights, Article 14. It is also now well accepted that the UDHR represents customary international law.
9 Convention on the Rights of the Child, Article 16.

equally offline and online;[10] that interferences with privacy can only be justified when necessary, proportionate and in accordance with the law;[11] and that privacy obligations are extraterritorial.[12]

THE RIGHT TO PROTECTION OF PERSONAL INFORMATION

The invention and public adoption of computers forced an expansion in the understanding of privacy to include a right to the protection of personal information. Accordingly, in 1971, the German State of Hessen adopted the world's first data protection law to regulate the conditions under which public and private actors could handle individuals' personal information. This was followed by regional and international initiatives at the Organisation for Economic Co-Operation and Development, the Council of Europe and the European Union.[13] Today, there are more than 100 national data privacy laws around the world, many of which closely mimic European standards.[14]

As it is now understood, the right to the protection of personal data is implicated by the generation, collection, publication, storage, retention or analysis of data. Personal data is handled for a wide range of purposes, from the delivery of public services and promotion of corporate products to real-time journalistic reporting and law enforcement investigations. Notably, the Internet and digital technology have raised new challenges for the creation and control of personal information, and have blurred the lines between private personal information and that which is properly in the public domain.

THE RIGHT TO PROTECTION OF REPUTATION

Reputation is recognized as a protected interest under both the UDHR and ICCPR, which grant individuals the right to be defended against unlawful attacks on their personal image. Nonetheless, specific international standards on the right to reputation remain lacking, and national legal understandings lag dramatically behind evolving societal experiences of reputational harm. The online proliferation of these harms has led some to refer to the present digital era as 'the reputation economy', in which retailers, insurers and service providers increasingly market and sell products on the basis of individuals' quantifiable characteristics, the demonstration of trustworthiness and public reviews of past performance.

In the reputation economy, online histories are arguably more valuable than credit histories. This has led some to decry tension between an individual's right to protection of reputation and others' right to freedom of expression, with a European Union court decision on the "right to be forgotten" in search engine results bringing this apparent conflict into the limelight.[15] As more information becomes available online, the developing right to reputation will undoubtedly have serious implications for privacy.

---

10 United Nations Human Rights Council Resolution A/HRC/20/L.13 on the promotion, protection and enjoyment of human rights on the Internet, June 2012.

11 United Nations General Assembly Resolution A/68/167 on the right to privacy in the digital age, December 2013.

12 Report of the United Nations High Commissioner of Human Rights A/HRC/27/37 on the right to privacy in the digital age, June 2014.

13 See Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108); European Union Data Protection Directive 95/46/EC.

14 Greenleaf, Graham, Asian Data Privacy Laws (Oxford, Oxford University Press: 2014), p. 55. For details about each of the domestic frameworks, see BakerHostetler, 2015 International Compendium of Data Privacy Laws, available at <www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf>.

15 *Google Spain v AEPD and Marioa Costeja Gonzalez*

CHILDREN'S PRIVACY

The Convention on the Rights of the Child (CRC) makes clear that children have a specific right to privacy. Tracking the language of the UDHR and ICCPR, Article 16 of the CRC states that "[n]o child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation," and reaffirms that "the child has the right to the protection of the law against such interference or attacks." Taken together, these standards imply that children and adults should be given the same level of protection for their right to privacy as adults.[16] When contextualizing children's right to privacy in the full range of their other rights, best interests and evolving capacities, however, it becomes evident that children's privacy differs both in scope and application from adults' privacy.

A differentiated approach to children's privacy does not necessarily mean that children should enjoy less protection of this right. In fact, with respect to informational privacy, there is a strong argument that children should be offered even more robust protection. Especially given that informational privacy protections are often circumvented by asking users to consent to lengthy terms and conditions for the collection and processing of the personal information, children's more limited levels of literacy and comprehension would demand heightened scrutiny and vigilance.

Equally, though, there are arguments for interfering with children's right to privacy in light of their ongoing physical and mental development.[17] For example, necessary health assessments and medical care can require invasions of young children's physical privacy that they may not fully appreciate. By the same token, while preventing children from engaging with the world without supervision can curtail their freedom, it can also create safe spaces for them to play, learn and communicate in ways that are central to their growth and empowerment.

In practice, respecting children's privacy is often a difficult balancing act. Some interferences with children's privacy are clearly justifiable; until children have the capacity to make fully informed decisions, giving them unbridled autonomy and independence is not in their best interests. In these circumstances, it can be appropriate and sensible to rely on parents and guardians to manage their children's privacy.

Even so, some argue that parents have been given too much authority over their children's privacy online. Requiring parental involvement and consent for the use of widely-available online services, for instance, can impede children's freedom of expression, access to information and development of digital literacy. Parental controls can similarly threaten children's free and confident use of technology, and applications installed to track children online may generate even more data about children's Internet use. Perhaps most concerning, parents who threaten their children's safety may use their power to cut off digital lifelines for seeking outside assistance.[18]

Albeit unintentionally, many parents also take actions that adversely impact their children's reputation online. While it is now commonplace for parents to share information about their children online, most children are not in a position to either scrutinize the information or object to its posting. As there is frequently no way for children to request that offending content be removed, even when they reach adulthood, parents may inadvertently be compromising their children's privacy far into the future.

---

16 For further discussion on the various debates on the content of children's right to privacy, see Kirsty Hughes, 'The Child's Right to Privacy and Article 8 European Convention on Human Rights', in Michael Hughes (ed.), Law and Childhood Studies: Current Legal Issues 2011, Volume 14 (Oxford: Oxford Univesity Press, 2011).

17 Shmueli, Benjamin, and Ayelet Blecher-Prigat, 'Privacy for Children', 42 Columbia Human Rights Law Review 759 (2011).

18 Livingstone, Sonia, 'Children's privacy online: experimenting with boundaries within and beyond the family', in Robert Kraut, Malcolm Brynin and Sara Kiesler (eds.), Computers, Phones, and the Internet: Domesticating Information Technology, Human technology interaction series (New York: Oxford University Press, 2006), pp. 145–167.

PART II
THREATS TO CHILDREN'S RIGHTS ONLINE

As technologies advance, the threats to children's privacy, personal information and reputation grow and the consequences of unjustified interferences multiply. Illicit government monitoring and unlawful corporate data collection[19] are not only violations of children's privacy in and of themselves, but may also chill children's free expression online and increase their exposure to identify theft. Moreover, such impacts are becoming increasingly complex and interrelated. For example, recording websites visited by Internet users could also facilitate government surveillance of browsing activity and create a honeypot of data subject to attack by cybercriminals. As summarized below, a number of threats to children's privacy and reputation directly engage, result from or are affected by the actions of private sector actors and Internet intermediaries.

CORPORATE DATA COLLECTION, ANALYSIS AND SALE OF CHILDREN'S BROWSING DATA

Children are of incredible interest to businesses. They are the largest and most powerful consumer group; they are more susceptible to advertising and marketing techniques; and their preferences and behaviours are more open to influence and manipulation. In many ways, they are the ideal audience for the new digital economic paradigm, in which companies possess tremendous amounts of information about individuals' digital behaviour that can be used to shape their online activities. In the words of a Chief Data Scientist for a major technology company, "[t]he goal of everything we do is to change people's actual behaviour at scale. When people use our app, we can capture their behaviours, identify good and bad behaviours, and develop ways to reward the good and punish the bad. We can test how actionable our cues are for them and how profitable for us."[20]

Private sector data collection is a complicated web of legitimate, questionable and illegitimate data acquisition, analysis, brokerage and sale. There is little standard corporate practice, particularly outside Europe where companies may be constrained only by piecemeal sectoral legislation and self regulatory initiatives. Companies based in the United States, which dominate the market in online applications, search engines, communication tools and the Internet of Things, are known to collect, store and use digital data in vastly different ways that make it nearly impossible to paint a comprehensive picture of data collection practices. Nevertheless, a number of key themes and issues emerge.

ONWARD SALE AND DISCLOSURE OF PERSONAL INFORMATION TO ADVERTISERS, DATA BROKERS AND THIRD PARTIES

The most common form of corporate data collection is voluntary. When users sign up for online accounts, whether to access news, social media, email or e-commerce, they are obliged to provide certain personal details and may be encouraged to share additional information. Internet services, social media networks and hardware manufacturers often combine this personal information with data they collect about how these same users interact with their services, including data about external websites or separate services accessed through company-owned platforms. Some ICT companies then package and sell this information on to third party advertisers and aggregators who correlate it with other data sets for further sale.[21]

---

19 See, for example, FTC, "VIZIO to pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent," 6 February 2017, available at https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it; Kevin O'Brien, "Germany Sues Google Over Data Collection," The New York Times, 22 April 2013, available at http://www.nytimes.com/2013/04/23/technology/germany-fines-google-over-data-collection.html; Doug Bolton, "Facebook loses first round of court battle over 'unlawful' storing of users' biometric data," The Independent, 6 May 2016, available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-sued-court-biometric-data-face-facial-recognition-privacy-bipa-a7016366.html.

20 Zuboff, Shoshana, 'The Secrets of Surveillance Capitalism', Frankfurter Allgemeine, 5 March 2016, available at <www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616-p2.html?printPagedArticle=true>.

21 For more information on data brokerage, see <www.eff.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-data-brokers-show-you-targeted-ads>.

Effectively, there is now an entire industry around the brokerage of personal data. While governments regulate the onward sharing and sale of personal information in different ways, it is typically legal for companies to collect, combine and sell personal information. Notably, some jurisdictions restrict the collection of sensitive personal information like health status or political affiliation. Others, like the European Union, require explicit user consent for the onward sale of data, although this consent is rarely meaningful in the context of exceedingly complex terms and conditions.

Given children's young age, tremendous quantities of personal information will be amassed before they reach the age of majority, much of it without their knowledge or awareness. Even where children are given an opportunity to grant permission for this data to be collected, combined and resold, they are not likely to fully appreciate the many ways in which this may impact their long-term privacy.

BEHAVIOURAL TARGETING AND ADVERTISING

In addition to selling data, internet companies sell advertising space based on a quantified understanding of customer behaviour, purchasing patterns and browsing history. Essentially, companies collect information on users' browsing habits, generate profiles of products or services that would interest these users, and then sell advertising space to entities that offer these products or services. While behavioural advertising provides a way for companies to offer consumers greater convenience, this brings a concomitant risk to users' privacy as behavioural profiling incentivizes the collection of increasingly larger amounts of personal data. A company might not only track how users engage with their online services, for instance, but also how they behave elsewhere on the Internet, how they use their mobile devices, where they are located, and even how they use their cursor.[22]

With children's greater susceptibility to advertising and marketing messages, and as measures designed to track behaviour segue into measures to influence behaviour, risks to children's privacy from behavioural targeting appear likely to become more entrenched. In addition, above and beyond generally available online services that are used by children, behavioural tracking and targeting are also deployed in products designed for and marketed to children. For example, school computers and online educational services can be set to automatically collect information on students' Internet activity.

USE OF BIOMETRICS

Biometric data is unique and intimate, making it more sensitive than other types of personal information. Yet for these same reasons, biometric technology is an increasingly appealing way to identify individuals. Facial recognition technology has already been deployed by social networks, online photo-sharing services and mobile applications to tag and organize pictures, including photos of children.[23] Some Internet of Things-enabled devices and toys already have voice recognition features that record and communicate with children.[24] Reportedly, recent advancements will soon recognize people through other aspects of their appearance such as their hair, clothes and body shape[25], and companies are now poised to use biometric data for identity authentication, geolocation and other purposes.[26]

22 See, e.g., Van Alsenoy, Brendan, et al., 'From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms', 25 August 2015, available at <www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf>.

23 See, e.g., Ionescu, Daniel, 'Facebook Adds Facial Recognition to Make Photo Tagging Easier', PCWorld, available at <www.pcworld.com/article/213894/Facebook_Adds_Facial_Recognition_to_Make_Photo_Tagging_Easier.html>; Elgan, Mike, 'Is facial recognition a threat on Facebook and Google?', Computerworld, 29 June 2015, available at <www.computerworld.com/article/2941415/data-privacy/is-facial-recognition-a-threat-on-facebook-and-google.html>.

24 Slack, Becky, 'Is the Internet of Things putting your child's privacy at risk?', The Guardian, 29 February 2016, available at <www.theguardian.com/sustainable-business/2016/feb/29/is-the-internet-of-things-putting-your-childs-privacy-at-risk>.

25 McHugh, Molly, 'Facebook can recognise you even if you don't show your face', Wired, 24 June 2015, available at <www.wired.com/2015/06/facebook-can-recognize-even-dont-show-face>.

26 See, e.g., <http://redpepper.land/lab/facedeals>.

Advocates have criticized the use of biometric data as invasive, and have expressed concerns that errors and inaccuracies in biometric authentication could prevent individuals from accessing services and products.[27] The Article 29 Working Party, a gathering of European data protection authorities, has called for strict restrictions on the use of facial recognition technology[28] and prompted its withdrawal from online services.[29] In the United States, attempts to bring industry and privacy advocates together in the United States to develop multi-stakeholder privacy guidelines for the use of biometrics have so far been largely unsuccessful.[30]

While the risks to children's privacy posed by biometric data are evident, it may also offer new opportunities to protect children's rights. For example, facial recognition technology has been promoted as an effective means to detect and analyse child sex abuse images.[31] Equally, this may enable law enforcement authorities and technology companies to work together in identifying potential victims from child sex abuse images.[32]

AGE VERIFICATION AND MANDATORY USE OF IDENTITY

To protect children from inappropriate services and products, such as pornography, many ICT companies employ age verification protocols. These might involve the use of peer-based models, semantic analysis, credit/debit cards, publicly available data, social security numbers, electronic ID cards or offline confirmation such as a phone call to a parent.[33] Age verification has also become a business in and of itself, with a range of services now commercially available,[34] and some countries have explored digital certificates for children that verify their age and sex.[35]

Governments have promoted age verification technology as part of a broader initiative that emphasizes online identity verification as a way to prevent and detect cybercrime, including child sexual abuse and exploitation. Some governments now require that individuals prove their identities to purchase SIM cards, to open Internet service accounts, or even to go online at cybercafés or libraries.[36] Increasingly, Internet companies also verify and mandate the use of real names and identities online before their services can be accessed.[37]

While the stated goals of age and identify verification practices are laudable, they prevent individuals from being anonymous online and can therefore undermine the right to privacy. As noted by the United Nations Special Rapporteur on freedom of expression, anonymity plays a central role in a range of human rights issues including

27 'Biometrics: friend or foe of privacy?', Privacy International, available at <www.privacyinternational.org/node/245>.

28 Article 29 Working Party Opinion 02/2012 on facial recognition in online and mobile services, 22 March 2012, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf>.

29 McHugh, Molly, 'Facebook moments is a smarter photo app – much smarter', Wired, 15 June 2015, available at <www.wired.com/2015/06/facebook-moments>.

30 'Face recognition row over right to identify you in the street', New Scientist, 19 June 2015, available at <www.newscientist.com/article/dn27754-face-recognition-row-over-right-to-identify-you-in-the-street>.

31 Geddes, Linda, 'Does sharing photos of your children on Facebook put them at risk?', The Guardian, 21 September 2014, available at <www.theguardian.com/technology/2014/sep/21/children-privacy-online-facebook-photos>.

32 Smith, Jack, 'Facebook is teaming up with law enforcement to combat sex trafficking', Miccheck, 15 October 2015, available at <http://mic.com/articles/126813/facebook-is-teaming-up-with-law-enforcement-to-combat-sex-trafficking#.Q2epl7QTX>.

33 Polonetsky, Jules, 'Online Age Verification for Our Children: A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives', 2009, available at <https://fpf.org/wp-content/uploads/2009/11/madrid-presentation-online-verification1.pdf>.

34 See, for example, Veratad, <http://veratad.com>.

35 See, e.g., 'Denmark makes strikes towards combatting online sexual exploitation of children', ECPAT, 25 June 2013, available at <www.ecpat.net/news/denmark-makes-strides-towards-combating-online-sexual-exploitation-children>.

36 Givvs, Samuel, 'UK government launches consultation for porn age-verification plan', The Guardian, 16 February 2016, available at <www.theguardian.com/technology/2016/feb/16/uk-government-launches-consultation-porn-age-verification-plan>.

37 Notably, some of these policies have been criticized for excluding ethnic minorities and those who have political, religious or other societal reasons to use pseudonyms, in some cases depriving these individuals of access to information and communications services. Holpuch, Amanda, 'Native American activist to sue Facebook over site's 'real name' policy', The Guardian, 19 February 2015, available at <www.theguardian.com/technology/2015/feb/19/native-american-activist-facebook-lawsuit-real-name>; Ortutay, Barbara, 'Real users caught in Facebook fake-name purge', SF Gate, 25 May 2009, available at <www.sfgate.com/business/article/Real-users-caught-in-Facebook-fake-name-purge-3231397.php>.

civic participation and political accountability.[38]

For children, the ability to communicate and search anonymously online provides immense protection to their identity[39], privacy and personal information. This can prevent children from being targeted online by savvy cybercriminals or inundated with invasive commercial messages. On the other hand, anonymity also facilitates the very criminal activity that places children in danger online. Anonymization can make it more difficult for law enforcement authorities to detect and prevent crime, and enables the existence of online marketplaces for child sex abuse material.

ENCRYPTION AND DEVICE SECURITY

Encryption converts electronic data into a form that is unreadable by anyone for whom the information is not intended. Three forms of encryption are prevalent in day-to-day Internet usage:

- End-to-end encryption: In end-to-end encryption, the keys to decrypt communications are held exclusively by the sender and recipient. When end-to-end encryption is employed, any intermediate device, service provider or potential interceptor is unable to read the content of communications. End-to-end encryption is offered by popular messaging services and applications.
- Disk / device encryption: Disk or device encryption is used to protect stored information. This means that data held on a disk or device cannot be read or accessed by anyone who does not possess the PIN or password, including hardware manufacturers and software providers. Device encryption is commonly used in computers and smartphones.
- Transport encryption: Transport encryption follows information as it traverses a computer network and can thereby encrypt individuals' browsing activity. Once data reaches site operators, however, it can be accessed or disclosed. Transport encryption is frequently offered by interactive websites, and includes HTTPS, Secure Socket Layer and Transport Layer Security.

The use of encryption is on the rise. More hardware manufacturers offer device encryption, more messaging applications have introduced end-to-end encryption, and more websites now facilitate transport encryption. Some also believe that recent Internet-of-things-related security breaches, including the hacking of online cameras to publish video footage from baby monitors, foreshadow the greater availability of encryption in connected products.[40]

Encryption can secure communications, web browsing and online transactions against outside monitoring and interference in ways that protect human rights, but it can also frustrate legitimate government surveillance and the apprehension of cybercriminals. By the same token, while encryption can protect children's data from illegitimate external monitoring and unauthorized access, encryption can equally be used to evade detection by those who wish to do them harm. Law enforcement authorities have in particular noted the challenges that encryption poses to investigating and preventing cases of child sexual exploitation.[41]

38 A/HRC/29/32, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015, para. 47.
39 Children have an express right to preserve their identity. See Convention on the Rights of the Child, Art. 8.
40 'Chinese hackers turn to ransomware', BBC News, 15 March 2016, available at <www.bbc.co.uk/news/technology-35811777>; Kerr, Dara, 'FTC and TrendNet settle claim over hacked security cameras', C Net, 5 September 2013, available at <www.cnet.com/uk/news/ftc-and-trendnet-settle-claim-over-hacked-security-cameras>.
41 Cook, James, 'POLICE: "Apple will become the phone of choice for the paedophile"', Business Insider UK, 26 September 2014, available at <http://uk.businessinsider.com/police-apple-will-become-the-phone-of-choice-for-the-pedophile-2014-9>.

GOVERNMENT SURVEILLANCE

MASS SURVEILLANCE

Over the past decade, rapid advancements in communications technology and new understandings of global security and cybersecurity have motivated governments to eschew the traditional limitations of lawfulness, necessity and proportionality on surveillance. It is perceived that reviewing every communication is necessary to understand all aspects of potential threats to national security, as each message could be the proverbial needle in the digital haystack. This has led to the development of mass surveillance, also known as bulk collection or bulk interception, which captures extensive amounts of data from the undersea fibre-optic cables that carry most of the world's data.

Mass surveillance programmes form a key part of many national security apparatuses and can be purchased on the private market, including by oppressive regimes.[42] Mass surveillance is often neither lawful nor acknowledged by national authorities, although a recent wave of legal reform aims to grant the practice greater legitimacy. It is often conducted without the knowledge and assistance of telecommunications companies and mobile network operators, who typically own and manage the channels by which information is communicated, although telecommunications companies and Internet service providers are in many instances informed of, asked to cooperate with, or compelled to facilitate government surveillance programmes.[43]

Mass surveillance not only compromises the very essence of privacy, but also jeopardizes the enjoyment of other human rights such as freedom of expression and freedom of assembly and association.[44] This can undermine democratic movements, impede innovation, and leave citizens vulnerable to the abuse of power. The implications of mass surveillance for children's privacy are clear, but are difficult to quantify as it is currently impossible to know how data is processed, how long it is retained, and how it might be used in the future. If governments are able to link individual profiles with data intercepted by mass surveillance, as many believe feasible, this would allow authorities to build and maintain records of children's entire digital existence.

MANDATORY RETENTION OF AND ACCESS TO BROWSING RECORDS AND COMMUNICATIONS DATA

Whereas intelligence agencies engage in mass surveillance, law enforcement authorities more typically request discrete data on a particular person, account or IP address directly from communications service providers and Internet intermediaries. These kinds of access requests have risen dramatically over the past several decades, tracking the consumer shift to digital communications networks and the corresponding decline in the collection and availability of traditional data sources.[45]

As pay-as-you-go mobile phones, email and messaging applications have gained in popularity, governments have mandated that telecommunications companies and Internet service providers generate and retain communications metadata such as the date, time, location, sender and recipient of a message, for up to two years. This metadata can reveal an individual's relationships, movements, connections, patterns of behaviour, and political and religious affiliations. For these reasons, it is of tremendous interest to intelligence and law

---

42 FIDH, 'Amesys and Qosmos targeted by the judiciary: is there a new law on the horizon?', 18 June 2013, available at <www.fidh.org/en/region/europe-central-asia/france/amesys-and-qosmos-targeted-by-the-judiciary-is-there-a-new-law-on-the-13966>.

43 'Spy cable revealed: how telecoms firm worked with GCHQ', Channel 4 News, 20 November 2014, available at <www.channel4.com/news/spy-cable-revealed-how-telecoms-firm-worked-with-gchq>; James Ball, Luke Harding and Juliette Garside, "BT and Vodafone among telecoms companies passing details to GCHQ", The Guardian, 2 August 2013, available at https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq>.

44 In the recent decision of the Court of Justice of the European Union in Schrems v Data Protection Commissioner of Ireland (Judgement of 6 October 2015), the Court concluded, in the context of mass interception of digital communications, that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life […]"

45 Google Transparency reports, <www.google.com/transparencyreport/userdatarequests/?metric=users_accounts>.

enforcement authorities, and there is increasing pressure across the ICT industry for companies to collect greater amounts of metadata about their users.[46]

Much like mass surveillance, mandatory data retention and bulk data acquisition programmes raise serious privacy concerns and pose the same clear threats to freedom of expression and freedom of assembly and association. These programmes also threaten freedom of the press and the right to information, as police forces can now request and access previously confidential data about journalistic sources.[47]

Protecting children from harm is the most frequently cited justification for requiring companies to retain and disclose data, and anecdotal evidence suggests that user data is regularly sought to help locate missing or suicidal children.[48] While combatting violence against children and providing children with social and psychological assistance remain important objectives, it must also be recognized that laws requiring the blanket retention of communications data represent a significant interference with all users' privacy. This interference is particularly acute for children, many of whom begin using mobile devices even before they have celebrated their first birthday and will generate nearly a full lifetime of metadata.[49]

OPEN SOURCE INTELLIGENCE GATHERING

Publicly available information sources like government records, news reports and classified advertisements have always been a valuable way for intelligence services, law enforcement authorities and corporate entities to gather data about individuals' private lives. In recent years, an exponential rise in the quantity of publicly available information, combined with the enhanced capacity for collection and analysis, have fundamentally changed the nature of so-called "open source" intelligence gathering. Today, intelligence agencies and police forces are able to quickly sift through extensive feeds of raw data from a vast array of sources including social media networks, digitized public records, live travel information and up-to-date coverage from every newspaper and television network in the world.

Open source intelligence gathering has particular implications for children's right to privacy. As more public records become available online, greater amounts of data on individuals are being gathered and made readily accessible to all for years to come. Parents share information publicly on sites like social media networks, and children increasingly do the same. Children may not even realize that they are making personal information public, and are less likely to appreciate how this information might be used to track and monitor their behaviour.

---

46 See, e.g., Boycott, Owen, 'Half a million communications data intercepts authorised in UK last year', The Guardian, 12 March 2015, available at <www.theguardian.com/world/2015/mar/12/more-than-500000-communications-data-intercepts-auhorised-in-uk-last-year>.

47 Interception of Communications Commissioners Office, Inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act to identify journalistic sources, 4 February 2015, available at <www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf>.

48 See, for example, 'Australia's PM says data retention laws think of the children', The Register, 17 February 2015, available at <www.theregister.co.uk/2015/02/17/pm_campaigns_for_data_retention_laws>.

49 Toppo, Greg, 'Techie tykes: Kids going mobile at much earlier age', USA Today, 2 November 2015, available at <www.usatoday.com/story/tech/2015/11/02/pediatrics-mobile-devices-study/75012604>.

USE OF PARENTAL CONTROLS

Parental controls can provide a powerful means to help children exercise their rights online. By allowing parents to designate content that is suitable for their children, to monitor their children's Internet searches and browsing behaviour, and to track the timing and duration of their children's Internet use, parental controls promise to preserve the benefits of digital education, information-sharing and connectedness all the while avoiding the web of online pitfalls and dangers.

Parental controls are now widely available in the commercial marketplace and have been readily adopted. In some countries, more than half of teenagers' parents have installed controls or other means of blocking, filtering or monitoring their child's online activities.[50] While the motivation to protect children from harmful content, sexual exploitation and disclosing personal information is undoubtedly legitimate, parental controls also present a clear interference with children's privacy.

They raise serious questions about the extent and nature of children's right to privacy in the home, the development of children into responsible digital citizens who can think critically and act independently online, and the support necessary for children to build trust, curiosity and creativity.

The tension between parental controls and children's right to privacy can best be viewed through the lens of children's evolving capacities. While parental controls may be appropriate for young children who are less able to direct and moderate their behaviour online, such controls are more difficult to justify for adolescents wishing to explore issues like sexuality, politics and religion. Furthermore, children's privacy may inadvertently be threatened by data collection and security concerns inherent in parental control software; investigations have uncovered instances where children's personal data was disclosed to third-party marketers without parents' consent[51], and have in some cases revealed grossly inadequate security protections.[52] Importantly, parental controls may also hamper children's ability to seek outside help or advice with problems at home.[53]

MANAGING REPUTATION ONLINE

The protection of reputation online is an increasingly contentious legal and political question [54], and the Internet has transformed the concept of managing reputation by dramatically increasing the scale, scope and reach of information. For instance, inaccurate or revealing news items that would traditionally have been rectified with a retraction are now duplicated innumerable times and effectively stored in perpetuity. Similarly, as Internet users publish personal information about themselves and others at progressively greater rates, antisocial attacks on reputation have proliferated and been memorialized in the public domain. Concerns about reputation online are

50 'Parents, Teens and Online Privacy', Pew Research Center, 20 November 2012, available at <www.pewinternet.org/2012/11/20/parents-teens-and-online-privacy-2>.

51 Federal Trade Commission Press Release, 'FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers', 30 November 2010, available at <www.ftc.gov/news-events/press-releases/2010/11/ftc-settles-company-failed-tell-parents-childrens-information>.

52 'South Korea ditching Smart Sheriff child monitoring app over "catastrophic" security woes', Japan Times, 2 November 2015, available at <www.japantimes.co.jp/news/2015/11/02/asia-pacific/south-korea-ditching-smart-sheriff-child-monitoring-app-catastrophic-security-woes/#.VzrGCRUrKZI>.

53 Qvist, Bella, 'Parents, is it okay to spy on your child's online search history?', The Guardian, 5 November 2015, available at <www.theguardian.com/sustainable-business/2015/nov/05/parents-children-online-search-history-microsoft-windows-10-privacy>.

54 The law has traditionally considered claims around reputation under the rubric of civil actions concerning defamation and libel. Generally speaking, under domestic laws, defamation claims are only substantiated when false and intentionally harmful, with freedom of expression concerns weighing heavily in the equation. Increasingly, however, claims around reputation are being cast in human rights terms under the umbrella of privacy.

particularly challenging for children, especially with a view to the long-term impact of damaging information.[55] Issues of specific importance to children include:

- **Unauthorized use of children's images**
  Many Internet applications enable the sharing, reproduction and publication of images featuring children, including where the individuals pictured are neither informed nor given an opportunity to consent to their distribution. Children's resulting inability to control how their photos are shared not only has a bearing on their reputation, but may also place them at risk; in the worst cases, images of children have been captured and shared within networks for child sexual abuse material. Even where children have voluntarily posted images, they may not understand, contemplate or expect that their photographs could later resurface should their lives or personal situations become of public interest.

- **Bullying and harassment**
  Cyberbullying is growing in prevalence and severity as users intimidate, threaten and harass others online, including children, in some cases maliciously disseminating private images to deliberately harm reputations. To make matters more complicated, many legal measures introduced to criminalize this behaviour have themselves proved problematic with respect to children's rights to privacy and freedom of expression. For example, cyberbullying laws may provide far-reaching online investigatory powers, authorize the revocation of Internet access as a form of punishment, or criminalize the consensual publication of images.[56] Worryingly, children have been prosecuted for sending sexual images to peers, and 18-year-olds have been added to the sex offender registry for sharing images of their teenage partners.[57]

- **The permanence of information published by or about children on the Internet**
  Perhaps most significant to children's reputation is the sheer volume of information available about them online, with children leaving ever longer and deeper trails of electronic information. This includes blogs, personal websites, social media posts and electronic public records like exam results, health care data, sporting league results and school bulletins. Even simple activities like playing an online game, attending a public event, or commenting on a news article can indefinitely capture discrete moments in children's lives. Taken together, this information creates public online representations of children's lives about which they may neither know nor feel comfortable. This not only has clear and immediate implications for children's privacy and autonomy, but also extends well into adulthood as it may impact future employment, relationships and financial inclusion.

55 See, e.g., 'Parents, Teens and Online Privacy', Pew Research Center, 20 November 2012, available at <www.pewinternet.org/2012/11/20/parents-teens-and-online-privacy-2>.

56 See, e.g., Mullin, Joe, 'Arizona makes deal with ACLU, won't enforce bad law on "revenge porn"', Arstechnica, 12 July 2015, available at <http://arstechnica.com/tech-policy/2015/07/arizona-makes-deal-with-aclu-wont-enforce-bad-law-on-revenge-porn>.

57 Deborah Feyerick and Sheila Steffen, '"Sexting" lands teen on sex offender list", CNN, 8 April 2009, available at <http://edition.cnn.com/2009/CRIME/04/07/sexting.busts/index.html?iref=24hours>.

PART III

THE REPSONSIBILTIES OF AND OPPORTUNITIES FOR THE ICT SECTOR

HUMAN RIGHTS AND THE ICT SECTOR

While there has been much international attention on the ICT sector's responsibility to respect human rights[58], children's rights have rarely featured in these discussions. When children are mentioned, it has been almost exclusively in the context of sexual abuse, exploitation and harmful content without recognition of children's full range of rights. Given the many threats to these rights detailed above, the dialogue on digital rights must now be expanded to consider the ICT sector's impacts on children's rights to privacy, protection of personal information and reputation. The *Guidelines for Industry on Child Online Protection* published by UNICEF and the International Telecommunications Union provide a useful framework to consider these rights, and highlight five key activities that ICT companies can undertake to respect and promote children's rights in a digital world:

1. Integrating child rights considerations into all appropriate corporate policies and management processes;
2. Developing standard processes to handle child sexual abuse material;
3. Creating a safe and age-appropriate online environment;
4. Educating children, parents and teachers about children's safety and their responsible use of ICTs; and
5. Promoting digital technology as a mode for increasing civic engagement.[59]

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND PROCESSES

By explicitly recognizing children's rights to privacy, protection of personal information and reputation in corporate policies and processes, ICT companies can better empower children to fully exercise all of their rights online. In some instances, this might even bring about a shift in fundamental business models that rely on revenue gained through the capture and exploitation of children's private information.

To translate their commitments to children's privacy and reputation into action, ICT companies could consider:

- **Conducting privacy impact assessments** as a matter of course to determine how products and services affect children's privacy. These assessments might be independent or incorporated into a wider human rights due diligence process, and could be conducted with a view to addressing and mitigating potential negative impacts.
- **Collecting minimal information** on children and applying enhanced security measures to protect any personal data that is collected, including location-related information. This would mean not generating more data than necessary to provide children with a particular service, and not retaining this data for any longer than required for this purpose. Following this principle, behavioural advertising and targeting commercial messages would not be considered legitimate reasons to gather or store children's personal information.

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

[59] Guidelines for Industry on Child Online Protection, available at <www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf>

- **Providing and communicating child-friendly terms and conditions** in clear, accessible language that is appropriate for young users with varying levels of literacy. Terms and conditions should be fair and guided by legal requirements and international standards, with consistent definitions throughout and all relevant information gathered in one place.
- **Acquiring explicit consent** for each element and purpose of processing children's data, above and beyond the acceptance of general terms and conditions, in recognition of children's evolving capacities. For children unable to provide informed consent by virtue of their age or level of understanding, parental consent or offline verification of a child's capacity to consent could be sought. Before seeking parental consent, the potential impacts on children's ability to freely and confidently access online services should also be considered.
- **Making children's online profiles private by default**, and working to ensure that children are explicitly informed about the potential implications of sharing their information publicly. Children should fully understand that public data is searchable by individuals, governments and businesses, and be able to appreciate that others might capture and distribute their images without their express permission. Similarly, parents should be informed about the potential consequences of publicly sharing photographs of their children.
- **Refusing to facilitate unlawful government surveillance** by interpreting demands as narrowly as possible, seeking clarification on the scope and legality of requests, requiring the delivery of a court order, and communicating transparently with users about compliance.[60] Children should understand when and how their data could be shared with law enforcement authorities, and where possible notified if this occurs.
- **Offering simplified, accessible reporting and complaints mechanisms** that enable children to request that harmful content be removed, even where its publication or distribution does not contravene the law, and putting similar processes in place to delink information from children's identity where this information is irrelevant, outdated or excessive. Importantly, these measures would also need to take into account the full context of requests made and their potential impact on children's other rights, including freedom of expression and the right to information.
- **Respecting anonymity online** by not requiring individuals to use or verify their identities unless mandated by law. Even where there are compelling reasons to ask that users reveal their identities, consideration should be given to cultural and contextual sensitivities that indicate greater protection of children's personal information.

DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL

Procedures for handling child sexual abuse material should account for the full range of children's rights, in particular the right to privacy. The investigation and removal of child sexual abuse material is an essential public policy goal, but the detection and prevention of violence against children online should never be used as a pretence to infringe on the privacy rights of children and other Internet users. In most cases, the **disclosure of children's data to law enforcement authorities**, including children's identities, personal information and communications, should occur only where authorized by a judicial authority in line with international standards.

[60] A/HRC/27/37, Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 30 June 2014.

Facial recognition technology could be appropriately deployed to facilitate law enforcement efforts related to child sexual abuse material, provided that data collection and retention are limited by the minimum requirements for the technology to operate. It should be noted, however, that cooperation with law enforcement would not justify the use of facial recognition technology on children in a commercial context.

CREATING A SAFE AND AGE-APPROPRIATE ONLINE ENVIRONMENT

When ICT companies take steps to protect children from exposure to inappropriate content online, this should be done with an awareness of how these measures impact the right to privacy. For example, while **age verification** protocols could block access to adult-oriented content like pornography, they would inevitably entail the collection of personal information from users.

Encryption offers a strong tool to protect children's privacy, and computers, tablets, smartphones, toys, baby monitors and other Internet-enabled devices used by or for children could be encrypted to provide additional security for personal data. Similarly, messaging applications, websites, online games and other Internet platforms aimed at and available to children could deploy encryption to better protect children's information.

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

Children's online safety education should cover the protection of personal data, including instruction on selecting privacy controls, setting strong passwords, using encryption, and understanding when and how to retain anonymity online. Good digital hygiene practices, like avoiding unknown memory sticks and regularly clearing browsing history, could be a focus of awareness-raising initiatives. By the same token, parents might also benefit from a greater appreciation of children's right to privacy in order to effectively use, adjust and eventually remove **parental controls** as children develop the independent capacity to safely and confidently navigate the Internet.

PROMOTING DIGITAL TECHNOLOGY AS A MODE FOR INCREASING CIVIC ENGAGEMENT

Children should be encouraged to responsibly engage in public debate and discourse over the Internet, and should be able to access material that helps them to make informed political, religious, societal and sexual choices. With this in mind, companies can consider the extent to which their data collection, online tracking and behavioural advertising practices could impede children's digital civic engagement. As above, **encryption and anonymization technology** could be provided and promoted to enable children to use the Internet without fear of adverse impacts on their reputation and privacy.

PART IV
THE ROLE OF STATES

Governments have an obligation to ensure that businesses respect children's rights, and should take appropriate steps to prevent and redress abuses of children's rights to privacy, the protection of personal information and reputation online. For example, governments can prohibit police harassment and the misuse of personal information; set strict parameters for the collection, use and analysis of children's data; and support and encourage the development of anti-bullying and privacy-friendly policies across the ICT sector. At the same time, governments must also respect children's rights in their own activities, and should bear children's right to privacy in mind when requesting, collecting, retaining or sharing data as part of surveillance programmes, law enforcement operations and the maintenance of public records.

LEGISLATIVE MEASURES

- **Harassment and misuse of personal information**

  Criminal and civil laws should be amended to sufficiently address violations of children's rights to privacy, the protection of personal information and reputation. Legislation should at minimum cover online harassment, cyberbullying, the sharing of images without consent, and the misuse of personal information. These laws should not, however, be crafted or enforced in ways that seek to criminalize children; rather, governments should develop holistic policies that guarantee respect for the rights of all concerned.

- **Data protection**

  Governments should provide a clear and predictable regulatory environment for the collection, processing, use and sale of children's data. As transnational ICT companies face significant challenges in complying with divergent national data protection regimes, governments should also work together to develop and implement universal standards that offer children consistent protection for their privacy and personal information around the world.

- **Surveillance**

  Many government surveillance programmes lack adequate transparency and coherence, and it is increasingly difficult for ICT companies to respond to requests for users' personal information, communications data and Internet activity records in ways that ensure respect for human rights. Domestic laws on surveillance must comply with international human rights norms, including the right to privacy, and governments should work towards streamlining and standardizing requests for digital information. In practice, this means that government requests for communications data should be judicially authorized, narrowly targeted, based on reasonable suspicion, and necessary and proportionate to achieve a legitimate objective. Notably, measures that would restrict the use of encryption or preclude anonymity are problematic under international human rights law [61], as is the mass interception and blanket retention of communications data.

[61] <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>

- **Open data and freedom of information**

  Governments should enact additional protections for children's personal data in the context of open data policies and freedom of information legislation. For example, children's personal information should be exempted from freedom of information requests, and open datasets pertaining to children, such as school enrolment statistics, should be rigorously anonymized.

ENFORCEMENT MEASURES

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

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

POLICY MEASURES

- **Develop guidelines for business entities**

  As technology often advances more quickly than regulatory frameworks, governments can develop principles, guidelines, best practices and codes of conduct to shape business impacts on children's privacy and reputation. Such initiatives might involve representatives from industry, civil society and international organizations to build awareness and support across all sectors.

- **Privacy impact assessments**

  Governments should conduct privacy impact assessments for any proposed legal or policy measures that relate to children's rights and the ICT sector. Similarly, governments can require, guide and encourage ICT companies to conduct privacy impact assessments that evaluate how corporate activities, operations and relationships affect children's privacy.

- **Review child protection measures**

  Governments should review measures to protect children from online violence against the full spectrum of children's rights. Such measures might include requirements that ICT companies collect and retain personal information, disclose user identities, or employ facial recognition technology. Measures that would interfere with children's privacy should only be introduced where this interference is both necessary and proportionate.

CONCLUSION

Digital technology and the Internet have perhaps forever changed conceptions of children's rights to privacy, the protection of personal information and reputation. On an ever more connected planet, it seems children face threats to their privacy and reputation online with increasing severity and frequency. From invasive data collection and mandatory identity verification to mass surveillance and overly strict parental controls, these threats jeopardize many of the benefits that the Internet has promised to bring into children's lives.

Despite mounting concerns, children enjoy at present only limited protection of their privacy and reputation. It is thus essential that all actors who operate in the ICT sector devote greater consideration to these rights. This paper has presented a range of practical steps that can be taken to prevent unjustified interference with children's privacy and to protect against unwarranted attacks on children's reputation online. In so doing, it is hoped that businesses and governments alike will adopt measures to better protect and empower children as full rights-holders in a digital world.

unicef

for every child