Issue brief no. 1 | August 2020
Good Governance of Children's Data project
Office of Global Insight and Policy

unicef
for every child

State surveillance and implications for children

Steven Feldstein, Senior Fellow at Carnegie Endowment for International Peace

About this paper

Surveillance tools are a core part of states' governing strategies.[1] In the digital era, governments rely on digital surveillance technology to support a range of interests — from national security and public order, to public health and municipal service delivery. Surveillance is generally understood to include technologies or systems that enable care or control of people "through the identification, tracking, monitoring, or analysis of individual data, or systems."[2] A key definitional point is that, while the purpose of surveillance can be to control or discipline individuals, surveillance can also be used to protect and care for citizens.

Surveillance capabilities provide governments with important advantages; they are widely used across different models of governments. While there is significant literature that considers whether governments may legitimately employ surveillance strategies and when their use violates core human rights principles, there is comparatively less discussion about state surveillance standards for children.[3]

This paper focuses on the following questions:

1. To what extent are governments distinguishing between children and adults when employing surveillance measures, including for political activity? What pressing issues of concern emerge in relation to state surveillance of minors?
2. When it comes to state surveillance, what protections are in place for children beyond generalized consent frameworks?
3. How does state surveillance differentially affect children from vulnerable, historically marginalized, or underrepresented groups?
4. Should the international community establish more defined norms or principles to protect children from state surveillance? What role can or should the private sector play in this regard?

Context of state surveillance

The use of surveillance by governments for political purposes is not a new phenomenon. Physical trailing, phone-tapping and house searches are trusted methods of operation that security services have relied on for decades in all types of government regimes. The emergence of new ICT surveillance tools linked to the proliferation of digital data has led to rapid changes in how surveillance works, when it applies, and how to balance individual protections with legitimate state interests. There are more communications data available for scrutiny than ever before. The internet has drastically increased the amount of transactional data available for individuals everywhere.[4] Unsurprisingly, surveillance has become increasingly prevalent, such as tracking public sentiment through social media monitoring, surveilling protests and dissenting speech, monitoring individual persons of interest (e.g. journalists, political opposition, government critics), and tracking voter behaviour.

In my own research, I identify four broad surveillance strategies commonly used by governments: artificial intelligence (AI) and big data approaches, passive surveillance strategies, targeted surveillance tools, and surveillance laws and directives.

AI and big data surveillance tools are automated techniques powered by advanced algorithms designed to identify broader behavioral patterns (mass surveillance), as well as of specific individuals. They include biometric identification systems such as facial recognition technology and genetic surveillance (which are generally less accurate in relation to children), smart cities or safe cities (city networks comprised of thousands of sensors transmitting real -time data to municipal authorities), smart policing techniques (data-driven methods used to enhance law enforcement response, inquiries and investigations, and to undertake predictive analysis), and social media monitoring (machine-driven programs that monitor millions of online communications in order to detect specific keywords or identify more generalized sentiments or patterns). This represents a nascent but growing category of surveillance.[5]

Passive surveillance strategies encompass hundreds of communications surveillance instruments that collect, monitor, and intercept data that has been "communicated, relayed or generated over communications networks to a group of recipients by a third party."[6] Representative technologies include internet monitoring, certain parental control apps, mobile phone tapping, location monitoring, and network interception.

Targeted surveillance techniques are intrusion operations which exploit software, data, computer systems, or networks to gain unauthorized access to user information and devices. In contrast to passive surveillance, which targets a broader range of individuals or groups for mass collection, targeted strategies rely on deployments of malware or spyware to collect information for specific individuals. These tactics are frequently carried out by commercial vendors like NSO Group, FinFisher, and Hacking Team.[7]

Surveillance laws and directives are designed to enable governments to access user content. Often, these laws mandate that cloud servers or social media platforms store data locally (thus expediting law enforcement requests), or they may authorize security agencies to access personal data or communications under specific circumstances — often linked to national security.[8]

The proliferation of digital surveillance presents troubling risks for children

These surveillance strategies have distinct implications for children.[9] In line with the trends described above, governments and private companies are collecting more data than ever related to children through a range of ways and systems. Primarily, the internet has become a ubiquitous presence in many households and children are accessing multiple digital instruments. Online data derived from *social media accounts*, smart phones, internet browsing, and gaming illustrate the many ways in which children's data are being shared. The peer effect associated with these technologies presents particular challenges. As children reach adolescence, there is strong pressure to maintain an active social media presence on apps like Instagram, Facebook, TikTok, and Snapchat, leaving many children prone to bullying, social anxiety, and data exploitation.[10]

Second, even when children are not directly logging on to specific apps, they often access and provide data linked to *home technology* from devices connected to the Internet of Things (IoT), such as smart speakers and connected toys. And third, *outside the home*, children's data are commonly shared in a variety of places, from location trackers in mobile phones and data from classrooms in schools, to video cameras in public areas, and even medical records.

The availability of this data can bring significant consequences when children become adults (not to mention that children's data are often mixed in with adult data).

The proliferation of digital surveillance presents troubling risks for children. When it comes to biometric technology, for example, its capacity to accurately recognize or identify children's faces is plagued by problems. As the UNICEF report "Faces, Fingerprints and Feet" notes, this issue "may be due to the difficulty in capturing the biometric trait (such as an iris scan with very young children); the relatively poor performance of the trait among certain age groups (facial recognition); or the low levels of user acceptance (DNA)."[11] Another challenge is correlating political and ethical risks associated with using this technology on children. In voluntary situations, children have a decreased ability to comprehend and make informed decisions about participating in certain programmes that involve surveillance. Their parents may also lack appropriate understanding to make informed decisions about the processing of their children's data. Involuntary data collection completely cuts out children's agency in determining how their data are collected, retained and used, with implications that may extend for decades. This leads to a third problem: as digital technology becomes increasingly central to individuals' lives, and as the declining cost of technology and data storage enable further exploitation of this data, "more data will be collected on children over their lifetime than ever before," making its future application, use and impact on children unpredictable.[12]

When it comes to protecting children from unwarranted state surveillance, there are few protections that exist in law

The implications for children are sharpened when it comes to political surveillance undertaken by governments. It is one thing for governments to collect data for ostensibly benign reasons, such as tracking school attendance or aggregating health records to monitor epidemiological outcomes. It is quite another to explicitly collect individual data as a means to reinforce political objectives. As will be discussed in the next section, while general standards exist that provide broad contours regarding legitimate and prohibited uses of surveillance, there remains significant ambiguity. When it comes to protecting children from unwarranted state surveillance, there are few protections that exist in law, either internationally or in specific countries. In fact, there are growing concerns about the extent to which education, health, refugee, or aid agency data may feed into state surveillance. There is also a widening recognition about the differential impact such technology may have on marginalized and persecuted groups and its disproportionate effect on children within these groups.

International norms and standards related to surveillance

The accepted international standard for whether a surveillance action is legitimate or not rests on concepts of necessity, proportionality, and legitimacy.[13] It is specifically based on the following considerations:

- Is the surveillance strictly and demonstrably necessary to achieve a legitimate aim?
- Does surveillance represent a proportionate response to that aim?
- Does domestic law authorize circumstances in which surveillance is appropriate, and are these legal regulations formulated with "sufficient precision to enable an individual to regulate his or her conduct accordingly" and made accessible to the public?[14]
- Are the interests justifying the surveillance action legitimate?

When it comes to defining surveillance legitimacy, there is significant disagreement. Many governments use national security or public order justifications for their surveillance programmes, but the line separating legitimate surveillance from abuses of power is purposefully ambiguous. The UN's Office of the High Commissioner for Human Rights (OHCHR) warns that such restrictions may "unjustifiably or arbitrarily" restrict citizens' rights to freedom of opinion and expression. OHCHR maintains that legitimate surveillance requires states to "demonstrate the risk that specific expression poses to a definite interest in national security or public order", and that a "robust, independent oversight system" that entrusts judiciaries to authorize relevant surveillance measures and provide remedies in cases of abuse is required.[15] David Kaye, the outgoing UN Special Rapporteur on the right to freedom of opinion and expression, observes that legitimate surveillance should only

apply when the interest of a "whole nation is at stake" and should exclude surveillance carried out "in the sole interest of a Government, regime or power group".[16] To guard against violations, OHCHR and other human rights watchdogs propose establishing independent oversight that empowers judiciaries to authorize relevant surveillance measures and can also provide remedies for those who have experienced harm.

Digital technology exacerbates these conditions and makes it likelier that governments may carry out surveillance in contravention of international human rights standards. Former special rapporteur Frank La Rue explains: "Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before."[17]

It is important to recognize that state surveillance is not inherently unlawful. Governments have legitimate reasons to undertake surveillance that are not rooted in a desire to enforce political repression and limit individual freedoms. For example, tracking tools play a vital role in preventing terrorism and tamping down on criminal activity, even if some governments exploit these threats as a pretext to crack down on political dissent. They give authorities the ability to monitor critical threats and react accordingly. Legitimate uses of surveillance extend beyond national security issues. As the COVID-19 crisis has demonstrated, health surveillance can be a critical tool for tracking infection rates and stemming the spread of the disease. The pandemic has led to particularly difficult choices when it comes to accomplishing larger public health objectives while protecting children's privacy.

Minimal surveillance protections for children

A critical question is whether more stringent protections exist — beyond the necessity and proportionality framework above — to safeguard children from government intrusion and surveillance. In brief, the answer is no.

Aside from data privacy consent frameworks that narrowly apply to commercial websites, no legal or policy differentiation exists between adults and children as regards government surveillance. Thus children are treated in the same way as adults when subjected to state surveillance, leaving the way open to worrying potential abuse.

Children are treated in the same way as adults when subjected to state surveillance, leaving the way open to worrying potential abuse

The UN Convention on the Rights of the Child (CRC) offers only vague surveillance protections for children.The most relevant passages are Article 13, guaranteeing children the right to freedom of expression (but it also includes national security, public order, public health and morality exceptions), and Article 16, which holds that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence."[18] While Article 16 establishes a minimum standard that can potentially be the basis of more specific protections, it is drafted in general terms that render it largely meaningless in the context of digitized surveillance. In particular, its inclusion of the term "unlawful interference" leaves an open door for governments to claim that state surveillance measures targeting children are legitimately grounded in domestic law.

There are scant efforts to develop more protections for children against surveillance restrictions. A 2018 resolution by the Council of Europe advised states to "take measures to protect children exercising their right to peaceful assembly and association in the digital environment from monitoring and surveillance, whether carried out by State authorities directly or in collaboration with private sector entities."[19] However, it does not appear that these recommendations have gained any traction.

Similarly, in January 2018, the UN special rapporteur on the right to privacy presented a draft framework on government-led surveillance and privacy that included direct reference to children. It states that exercising human rights on the internet, especially rights to privacy and freedom of expression, "is an issue of increasing interest and importance." It notes that while children benefit from new digital

capabilities and opportunities, they are "particularly dependent on efficient safeguards and effective remedies."[20] The proposal does not offer additional detail about how children might be protected under a revised surveillance framework; consequently it has not garnered much support or momentum.

An alternative approach when it comes to developing surveillance protections for children is to look at age of consent frameworks linked to data privacy, and to extend such restrictions to government surveillance. The United States Children's Online Privacy Protection Act of 1998 (COPPA), for example, establishes the age of consent at 13 years, meaning that parental consent is required for processing personal data on websites directed to children under the age of 13, or where companies have actual knowledge that a child under 13 is using their service.[21] But COPPA only applies to operators of commercial websites or online services that collect, use, or disclose personal information from children.[22] Its jurisdiction does not extend to government surveillance and collection of children's data. In the United States and in most other countries, enhanced surveillance protections for children simply do not exist.

In Europe, the General Data Protection Regulation (GDPR) also includes provisions intended to protect children's data rights. GDPR Recital 38 stipulates that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."[23] While this represents a positive step, as European Digital Rights notes, "it is only an explanatory recital, guiding implementation of the GDPR but lacking the legal force of an article."[24] And similar to COPPA, these protections are limited to children's data used for "marketing or creating personality or user profiles". They also do not extend to political surveillance undertaken by governments.

State surveillance of children in practice

Government surveillance of children occurs in different political systems with few legal or policy limitations.[25] State surveillance of children is often explained as a necessary safeguard for children's own interests (e.g. administrators often uphold surveillance measures as the best means for teachers and educators to actually show the extent to which children are achieving learning outcomes, lest they be accused of failing to meet their statutory duty of care). The following examples illustrate surveillance challenges in practice.

In Hong Kong, China, the 2014 Umbrella Movement protests were galvanized in part by high school students, including members of the activist group "Scholarism", founded by Joshua Wong and Ivan Lam Long-in when both were 15 years old.[26] They have faced detentions and arrests as a result of their political activism (occurring when neither had yet turned 18), and their movement has faced significant surveillance obstacles including tracking by facial recognition cameras and cyber monitoring by security officials. Because these young activists incurred severe punishments for participating in the 2014 protests, they developed counter-surveillance tactics used during the 2019 protests.[27]

Law enforcement authorities continue to expand their surveillance efforts in a manner that directly implicates children

In the United States, recent revelations that the Department of Homeland Security (DHS) deployed aerial surveillance (helicopters, airplanes, drones) over 15 cities to monitor anti-racist protests did not indicate any distinction made between children and adults. The *New York Times* reports that the full amount of footage was "fed into a digital network managed by the DHS, called 'Big Pipe,' which can be accessed by other federal agencies and local police departments for use in future investigations."[28]

Beyond political protests, law enforcement authorities continue to expand their surveillance efforts in a manner that directly implicates children. Rachel Levinson-Waldman from the Brennan Center describes how the New York Police Department's (NYPD) Juvenile Justice Division, which focuses on individuals under 18 years of age, has established a "special social networking unit" that "maps out territories covered by crews, block by block, to facilitate the monitoring of crew members on Facebook."[29] Other media outlets report how the NYPD has loaded "thousands of arrest photos of children and teenagers into a facial recognition database" despite their young ages and notwithstanding evidence of a sig-

nificantly higher risk of false matches.[30] In the United Kingdom, a recent report from Privacy International found that "a significant number of local authorities" are using "overt" as well as "covert" social media monitoring as part of their intelligence gathering and investigations, including social media surveillance in the area of "children's social care".[31]

Troubling surveillance activity is occurring in all political contexts

Marginalized and minority groups also encounter differential impacts from political surveillance measures. In the United States, Black Lives Matter protests have resulted in law enforcement agencies using a variety of digital tools to keep tabs on demonstrators — both children and adults — many of whom come from minority communities.[32] In Xinjiang, China, human rights groups have raised concerns about biometric data collection from the population, starting as young as 12 years old, being a potential means of surveillance.[33]

Schools are another vector for state surveillance. In the United Kingdom, researcher Jen Persson writes that new guidance from the Government has led schools to impose "online filtering and monitoring software on pupil and staff devices. Every search, every screen, is recorded, every second."[34] The risks of this strategy are manifold. Not only are tracking tools vulnerable to malicious hacking that could potentially expose the personal information of millions of children, but innocent web searches undertaken by 12- and 13-year-olds could now land children on "watchword lists" by treating minors as potential terrorists and creating "permanent records of interest" for those who are flagged.[35] As the COVID-19 crisis continues, resulting in online-based curricula, surveillance systems may also follow, running the risk that school-based monitoring may increasingly blur the line between the physical classroom and the home.

In Russia, a facial recognition system named "Orwell" has landed a US$29 million contract to install biometric technology in schools across the country. Already, cameras have been delivered to 1,608 schools with the intent to "keep tabs on students' comings and goings and identify strangers who attempt to enter school grounds." While this plan was devised following the increase in crime rates in Russian schools, the programme raises the prospect of curtailing children's speech and suppressing their political expression.[36]

School surveillance is also increasing in the United States. Education officials in western New York's Lockport City School District have started testing facial recognition cameras. New Mexico schools have installed gunfire-detection microphones. New Jersey officials have prototyped iris recognition technology for use in playgrounds.[37]

As these examples illustrate, children around the world face a myriad of state surveillance restrictions similar to measures encountered by adults. These actions run the gamut from surveilling political protests and tracking counter-terrorist activities, to monitoring individuals for crime prevention purposes. Though some of these measures may be deployed for legitimate purposes, often the purpose and intent is not clear nor sufficiently explained to those who are being surveilled.

Ideas for reform

The absence of meaningful regulation or accepted and agreed international standards has allowed government surveillance of children to proliferate. Historically marginalized, underrepresented, and minority groups are especially vulnerable to these measures. Troubling surveillance activity is occurring in all political contexts.

A starting point to address expanding government monitoring and tracking of children would be to develop a normative framework and basic guidelines about the appropriate use of surveillance measures in relation to children. In this regard, building from Article 16 of the CRC, which prohibits arbitrary or unlawful interference with a child's privacy, family, home or correspondence, may be beneficial. Policymakers could consider incorporating the following principles:

1. **Explicitly emphasize the necessity of protecting children's rights to peaceful assembly and association** in the digital environment that is free from state surveillance carried out by government authorities directly or in collaboration with private sector entities;

2. **Underscore the importance of explicitly considering children's needs** and the impacts of digital surveillance when implementing monitoring or tracking measures;

3. **Include a presumption against government surveillance of children** with limited national security exceptions that are concrete, defined, and time-bound, such as enacting time restrictions for the retention of children's data;

4. **Encourage the development of technology that incorporates "privacy by design"** approaches that prioritize children's privacy and agency;

5. **Ensure accountability for state surveillance by authorizing independent judicial authorities** to monitor against abuse and provide remediation as needed;

6. **Recognize the particular vulnerabilities** associated with state surveillance of historically marginalized, underrepresented, and minority groups, and **ensure that access and equity are key components in the design** and use of relevant technologies; and

7. **Resist compelling individuals to use surveillance applications, programs, or systems** unless validated by legitimacy, necessity and proportionality tests.

Generating international consensus about which aspects of state surveillance should be prohibited could have far-reaching impacts. Such an effort could galvanize public opinion against abusive practices and incentivize law enforcement to codify heightened surveillance standards for children. While the immediate effect may be less pronounced in closed contexts, promulgating such norms may force greater scrutiny and constrain surveillance programmes that otherwise face few limitations in law or practice.

Action in this area does not extend only to governments. Private sector actors play critical roles as well. In addition to self-regulation, companies can also pressure governments to conform to international best practices. In situations where there is prevalent misuse of certain technologies, companies can decide to suspend manufacturing or opt to pursue additional testing before allowing their products back onto the market. For example, Amazon recently implemented a one-year moratorium on police use of its "Rekognition" technology, IBM announced it would discontinue selling its general-purpose facial recognition systems, and Microsoft stated that it would also stop selling its facial recognition technology to police departments until appropriate federal regulations are enacted.[38] This can serve as a positive example to other companies that show less interest in taking a difficult public stand in this area.

This aspect of digital surveillance requires greater research and understanding about what policies governments are undertaking and their impact on children. What sort of data sharing agreements exist between private corporations and government law enforcement bodies? As facial recognition systems, big data social monitoring programs, and other technologies process increasing amounts of children's data, what standards guide how they retain and protect data and which entities they share this information with? What regulations, if any, determine whether a ministry of health will share confidential medical records with intelligence or security agencies? What types of authorizations are required? What remediation options are available when harms accrue to children?

As technology continues to evolve, it is critical that researchers and advocates document how new uses of surveillance are managed by governments, specifically as regards children

As technology continues to evolve, it is critical that researchers and advocates document how new uses of surveillance are managed by governments, specifically as regards children. The COVID-19 pandemic has brought additional uncertainty to the field and raises a host of unresolved questions. The blending of legitimate health interventions with political surveillance deployment is an area which needs a high level of attention, particularly for governments which have demonstrated patterns of repressive behaviour.

This paper was developed by members of the Working Group on Good Governance of Children's Data. Learn more about the project ▶

Good Governance of Children's Data project

The Office of Global Insight and Policy is bringing together 17 global experts in a project to explore trends in the governance of children's data, including the tensions between different rules and norms, emerging concepts and practice, and implications for policy and regulation. Debate on the future of children's data affects a diverse range of issues, including data ownership and control, data fiduciaries, profiling for digital marketing purposes, child-friendly privacy notices, data erasure upon request, age verification, parental responsibility, data protection by design and default, algorithmic bias, and individual and group data.

The project aims to highlight the gap between the world we want for children and today's reality, developing a manifesto on how children's data could be optimally managed and what steps need to be taken. To help develop this manifesto, members of the working group will publish short analyses of different approaches to data governance.

Endnotes

1 Portions of this paper derive from previously published material by the author, including Steven Feldstein, "The Global Expansion of AI Surveillance", Carnegie Endowment for International Peace Working Paper, 17 September 2019,

2 Monahan, Torin, Surveillance in the Time of Insecurity (New Brunswick, NJ: Rutgers University Press, 2010), p. 8. See also Lyon, David, "The Search for Surveillance Theories," in David Lyon, ed., Theorising Surveillance: The Panopticon and Beyond (Portland: Willan Publishing, 2006), pp. 3–20.

3 For the purposes of this paper, children are defined as individuals from 0–18 years of age, in accordance with the UN Convention on the Rights of the Child. Convention on the Rights of the Child, New York, 2 September 1990.

4 La Rue, Frank, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", A/HRC/23/40, 17 April 2013.

5 See Feldstein (2019); Feldstein, Steven, "How Artificial Intelligence is Reshaping Repression", Journal of Democracy 30, no. 1 (2019): 40-52. See also "Faces, Fingerprints and Feet," UNICEF, July 2019.

6 "Communications Surveillance", Privacy International, 8 February 2018.

7 See for example Crete-Nishihata, Masashi, et al., "Communities @ Risk: Targeted Digital Threats against Civil Society", The Citizen Lab, 11 November 2014.; Howell O'Neill, Patrick, "The Fall and Rise of a Spyware Empire," MIT Technology Review, 29 November 2019.

8 La Rue (2013). "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression".

9 See "Who Knows About Me? A Children's Commissioner report into the collection and sharing of children's data", UK Children's Commissioner's Office, November 2018.

10 See for example, Ira Glass, host, "Status Update" This American Life (podcast), 27 November 2015; Kardefelt-Winther, Daniel, "Child Rights and Online Gaming: Opportunities and Challenges for Children and the Industry," August 2019.

11 "Faces, Fingerprints and Feet", UNICEF, July 2019.

12 Ibid.

13 "Necessary and Proportionate", Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, 4 March 2016.

14 Kaye, David, "Report of the Special Rapporteur to the Human Rights Council on Surveillance and Human Rights", A/HRC/41/35, 28 May 2019.

15 "The Right to Privacy in the Digital Age", Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30 June 2014. See also article 12 of the Universal Declaration of Human Rights.

16 "Surveillance and Human Rights, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", A/HRC/41/35, 28 May 2019.

17 La Rue (2013). "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression".

18 Convention on the Rights of the Child, New York, 2 September 1990.

19 "Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment", Council of Europe, 4 July 2018.

20 "Draft Legal Instrument on Government-led Surveillance and Privacy 16 Including the Explanatory Memorandum 17 Ver 0.6", OHCHR, 10 January 2018.

21 There is significant fragmentation globally when it comes to applying uniform age of consent standards for children as Ingrida Milkaite and Eva Lievens write in "Children's Rights to Privacy and Data Protection around the World: Challenges in the digital realm." European Journal of Law and Technology 10, no. 1 (2019).

22 Bozzuti, Angela, "A Guide to Protecting Children's Privacy Online", Lexis Practice Advisor Journal, 11 August 2016.

23 "Recital 38: Special Protection of Children's Personal Data", Regulation (EU) 2016/679 (General Data Protection Regulation), 25 May 2018.

24 Alternatif Bilisim, "ePrivacy for Children: What is Data Protection Culture?" EDRi, 13 June 2018.

25 Maria T. Grasso and Judith Bessant, eds., Governing Youth Politics in the Age of Surveillance (New York: Routledge, 2018). p. 3.

26 Lee, Ada, "Scholarism's Joshua Wong embodies anti-national education body's energy", SCMP, 10 September 2012.

27 Dvorak, Phred and Khan, Natasha, "Hong Kong Protesters Adjust Tactics with Lessons from 2014 Umbrella Movement", Wall Street Journal, 13 June 2019.

28 Kanno-Youngs, Zolan, "U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance", The New York Times, 19 June 2020.

29 Levinson-Waldman, Rachel, "Government Access to and Manipulation of Social Media: Legal and policy challenges". Howard LJ 61 (2017): 523.

30 Goldstein, Joseph and Watkins, Ali, "She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database", The New York Times, 1 August 2019.

31 "When Local Authorities Aren't Your Friends", Privacy International, 24 May 2020.

32 Funk, Allie, "How Domestic Spying Tools Undermine Racial Justice Protests", Freedom House, 22 June 2020.

33 "Faces, Fingerprints and Feet", UNICEF, July 2019, p. 17.

34 Persson, Jen, "Child Safeguarding Cloaks State Surveillance and Data Exploitation", Open Democracy, 26 June 2017.

35 Ibid.

36 Luxmoore, Matthew, "Yes, Big Brother IS Watching: Russian Schools Getting Surveillance Systems Called 'Orwell'", Radio Free Europe/Radio Liberty, 17 June 2020.

37 Warzel, Charlie, "Welcome to the K-12 Surveillance State", The New York Times, 2 July 2019; Uchida, Craig D., et al., "Safe Kids, Safe Schools: Evaluating the Use of Iris Recognition Technology in New Egypt, Report prepared for the Department of Justice, December 2004.

38 Hao, Karen, "The Two-year Fight to Stop Amazon from Selling Face Recognition to the Police", MIT Technology Review, 12 June 2020.

39 Portions of this paper derive from previously published material by the author, including Steven Feldstein, "The Global Expansion of AI Surveillance", Carnegie Endowment for International Peace Working Paper, 17 September 2019,

40 Monahan, Torin, Surveillance in the Time of Insecurity (New Brunswick, NJ: Rutgers University Press, 2010), p. 8. See also Lyon, David, "The Search for Surveillance Theories," in David Lyon, ed., Theorising Surveillance: The Panopticon and Beyond (Portland: Willan Publishing, 2006), pp. 3–20.

41 For the purposes of this paper, children are defined as individuals from 0–18 years of age, in accordance with the UN Convention on the Rights of the Child. Convention on the Rights of the Child, New York, 2 September 1990.

UNICEF works in the world's toughest places to reach the most disadvantaged children and adolescents — and to protect the rights of every child, everywhere. Across 190 countries and territories, we do whatever it takes to help children survive, thrive and fulfill their potential, from early childhood through adolescence. And we never give up.

The Office of Global Insight and Policy serves as UNICEF's internal think-tank, investigating issues with implications for children, equipping the organization to more effectively shape the global discourse, and preparing it for the future by scanning the horizon for frontier issues and ways of working. With dedicated expertise in seven policy areas — digital technology, human capital, governance, the environment, society, markets, and finance — the Global Insight team assists the organization in interpreting, and engaging in, a rapidly changing world.

Office of Global Insight and Policy
United Nations Children's Fund
3 United Nations Plaza, New York, NY, 10017, USA

Special thanks to Jake Gutman, graduate student at Princeton University's School of Public and International Affairs, for research assistance in compiling reference material for this paper. Many thanks also to Jasmina Byrne, Linda Raftree and Emma Day for their extensive and thoughtful comments on the text.

This document is interactive and designed for digital viewing.

Please consider the environment and refrain from printing.