United Nations A/HRC/46/37

General Assembly

Distr.: General
25 January 2021

Original: English

Human Rights Council
Forty-sixth session
22 February–19 March 2021
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Artificial intelligence and privacy, and children's privacy

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*, **

Summary

The present report is prepared pursuant to Human Rights Council resolutions 28/16 and 37/2. Never has the human right to privacy been more important and more under siege. Technological trends, as foreshadowed in 2015, have posed ever more challenges for the enjoyment of the right to privacy. In the present report, the final report of the inaugural Special Rapporteur on the right to privacy, he addresses two separate challenges: firstly, artificial intelligence and privacy, then children's privacy, particularly privacy's role in supporting autonomy and positive participation in society. Guidance and recommendations, developed through consultation and research, are outlined to address those challenges. Along with other recommendations of the Special Rapporteur in his previous reports, the present report completes the workplan presented to the Human Rights Council in 2016 (A/HRC/31/64). An overview of the Special Rapporteur's activities conducted under the mandate activities since 2015 is contained in the annexes.

* Agreement was reached to publish the present report after the standard publication date owing to circumstances beyond the submitter's control.

** The annexes to the present report are circulated as received, in the language of submission only.

I. Recommendations on privacy protection for the development and operation of artificial intelligence solutions

Background and purpose

1. The purpose of the present recommendations is to provide guiding principles concerning the use of personal and non-personal information in the context of artificial intelligence (AI)[1] solutions developed as part of applied information and communications technologies (ICTs), and to emphasize the importance of a legitimate basis for AI data processing by Governments and corporations within the overarching framework of the human right to privacy.

2. The recommendations are based on the Universal Declaration of Human Rights and reflect the spirit and the understanding of that Declaration. Above all, articles 7 (non-discrimination) and 12 (right to privacy) are critical to developing or operating AI solutions. The themes and values of those articles are found in articles 2 and 3 (non-discrimination) and 17 (privacy) of the International Covenant on Civil and Political Rights and are obligations upon States that have ratified that treaty.

3. Rights are of crucial importance in the information society. The General Assembly and the Human Rights Council have confirmed that the rights people enjoy offline should also be protected online (A/75/62-E/2020/11, para. 9), as a condition for the Internet to remain global, open and interoperable (Human Rights Council resolution 26/13), and as a driving force in accelerating progress towards development in its various forms, including achieving the Sustainable Development Goals (General Assembly resolution 73/179).

4. The privacy of all data[2] underpinning AI solutions is the focus of the recommendations. They are intended to serve as a common international baseline for data protection standards regarding AI solutions, especially those to be implemented at the domestic level. While recognizing the many economic and social benefits of AI solutions, the recommendations are intended as a reference point on how the right to privacy can be protected in the context of AI solutions.

5. The implementation of the recommendations requires full collaboration between Governments, civil society, the private sector, the technical community and academia, and should be sustained in common human values, such as inclusiveness, respect, human-centredness, human rights, international law, transparency and sustainability.

6. AI solutions involve the application of AI systems intended to guide, predict or make decisions that affect everyone's lives. AI solutions offer benefits along with other impacts currently being debated within society. Those debates – moral, ethical and societal questions involving human rights such as privacy, non-discrimination and free participation – are ongoing. All those questions are preconditioned by lawful treatment from a privacy perspective. That is particularly necessary as most data are held by private corporations that leverage their commercial value, combining diverse data sets to maximize their analytical capacity. A response is required to growing public concern about the intrusiveness and potential impact of data gathering, the risk of surveillance and the increasing use of algorithms using such data sets to automate decisions that affect individuals' lives (A/75/62-E/2020/11, para. 10).

[1] There are several definitions of artificial intelligence. The meaning intended in the present report is the most common one, as defined in the *Oxford Reference*: "The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages". That is far from being an exhaustive list of applications of AI technologies.

[2] The Special Rapporteur, tracing the lineage of data protection to the right to respect for private life in article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, treats data protection law as part of a subset of privacy regulation. While he recognizes that historical developments in Europe have led to the explicit inclusion of data protection as a separate article of the Charter of Fundamental Rights of the European Union, he refers readers to the historical references.

7. The context for deployment of AI requires the effective and independent functioning of a privacy and/or data protection regulatory body oversighting dedicated legislation.

Scope

8. The present recommendations are applicable to the data processing of AI solutions in all sectors of society, including the public and private sectors. Data processing refers to each stage of the life cycle of an AI solution where data is involved, including its design, development, deployment and decommissioning of an AI solution, and any iteration or redesign based on a preceding AI solution.

9. The recommendations are applicable to all managers of AI solutions. That can mean designer, developer or operator (self-responsible or principal), each in their specific function. The intent is that within an organization, each AI solution has either a legal or a natural person with full responsibility for the AI solution.

10. The recommendations do not limit or otherwise affect any law that grants data subjects more, wider or in whatsoever way better rights, protection and/or remedies. They do not limit or otherwise affect any law that imposes obligations on managers and processors where that law imposes higher, wider or more rigorous obligations regarding data privacy aspects.

11. The recommendations do not apply to AI solutions that might be performed by individuals in the context of purely private or household activities.

Considering human rights and ethical aspects

12. There is a responsibility on society to develop AI solutions within a human rights framework, ethically and responsibly. AI solutions affect many areas of daily life now, and will increasingly do so, having a profound influence on people's personal living and working situations. In the future, AI solutions are likely to cover a broader range of fundamental principles reflecting human rights law and ethical questions. How that technology is used is critical.

13. Non-discrimination is essential to avoid inequality, injustice and suffering with the potential to affect the enjoyment of human rights, including economic, social and cultural rights. The use of AI solutions needs to be accurately monitored and any occurrences of discrimination or other outcomes which infringe human rights must be corrected to avoid such adverse effects.

14. The use of AI solutions should not be countenanced for final decisions, but only as part of decision-support in certain areas, for example, judicial or medical decision-making. Human rights assessments should always be undertaken alongside data protection assessments to provide a holistic overview of the necessary framing conditions.

15. Committees around the world, for example, the ad hoc Committee on Artificial Intelligence of the Council of Europe, are currently working on drafting regulatory frameworks and codes of ethics for AI solutions. Reference should be made to them and other relevant guidance, such as the Guiding Principles on Business and Human Rights.

Artificial intelligence and data privacy

16. Current AI systems include or represent a combination of analysis systems based on formalized expert knowledge (data warehouse, business intelligence) and machine learning, as well as the targeted application of what has been learned. There is a difference between pre-programmed, algorithmic systems for the solution of specific problems, and systems that can learn. The latter are equipped with learning algorithms and have to be trained.

17. In the algorithmic decision-making process regularly used as the basis for AI, an assessment is made based on information, which leads to a decision, forecast or recommendation for action. In the case of "supervised learning", the AI system has solution criteria for solving a specific problem, whereas in case of "non-supervised learning", the AI-system itself will choose or recommend the relevant solution criteria.

18. Consequently, both the data processing and the decision made as a result of that processing have potential risks for the data subject.

19. Classic information technology, with its elements “input” – “processing” – “output”, is extended by the abilities to perceive, understand, act and learn. Those activities, previously undertaken only by humans, are performed by machines to an increasing extent. The term “understanding” is new territory in connection with computers and must be accompanied by a critical review of traceability and adherence to human rights and ethical values.

20. Machine learning refers to a series of optimization methods in artificial neural networks, among others. AI systems can have very complex structures between the input and output layers. By mapping several hierarchical processing layers, machine learning can become considerably more efficient (deep learning). That inevitably results in reduced traceability in AI decisions. Due to the complexity of the algorithms and the multitude of arithmetic operations performed by the machine, the deeper processing layers (hidden layers) elude transparency in the decision criteria and their weighting.

21. The disclosure of the algorithms on which the AI is based is a core demand in current debate about AI transparency. The concrete verification of the decision logic of highly complex AI systems using disclosed algorithms is, however, likely to be difficult in practice. Whether one is dealing with interpretable AI or explainable AI, or other models, where there is doubt or a failure in process or outcomes, the capture of digital evidence is necessary to reconstruct what happened and why a certain outcome was advised or actually occurred.

22. Monitoring the decision-making processes of AI systems from outside, by reviewing the decisions themselves against a predetermined purpose of the system and ethics governance, has many benefits, including practicality.

23. AI decisions falling outside the expected range of outcomes or decisions must be identified and an intervention made. Tools developed specifically for the detection of unexpected outcomes and for analysis of AI decisions are a prerequisite. Monitoring machines exclusively by machines increases the possibility of unforeseen risks or “unknown unknowns”. That necessitates the principle that human judgments must always dominate AI monitoring processes.

24. In addition to the efficiency of the learning mechanisms, successful machine learning depends on the quantity and quality of the available data. The big data trend in information technology and the increasing mass availability of high-quality data are significantly accelerating the development of AI systems.

25. The very complex psychological and emotional processes of human knowledge and decision-making are likely to remain the domain of humans rather than machines. Therefore, when evaluating and weighing up applicable law in relation to AI systems and their decision-making, it must be borne in mind that machine decisions are based on different principles and mechanisms (although developed largely by humans) from those applied to human decisions.

26. To achieve the necessary security for AI systems, comprehensive ethical and legal governance for AI decisions must be effectively implemented in the control environment of an entity making use of AI solutions. Also, better digital cooperation is needed, with multiple stakeholders thinking through the design and application of standards and principles such as transparency and non-bias in AI applications in different social settings.

A. Data privacy principles for the use of artificial intelligence solutions

27. Irrespective of the jurisdiction or the legal environment applying to the manager responsible, eight main principles are mandatory considerations in the planning, development and implementation of AI solutions. The principles and their specification do not replace any other or stricter data protection regulation applicable to those working with AI solutions. The principles are:

(a) Jurisdiction;

(b) Ethical and lawful basis;

(c) Data fundamentals;

(d) Responsibility and oversight;

(e) Control;

(f) Transparency and “explainability”;

(g) Rights of the data subject;

(h) Safeguards.

Jurisdiction

28. To create legal certainty and traceability, ideally, there should be a transnational framework reflecting international consensus and containing mechanisms for identifying and regulating liability and responsibility within AI solutions, and for managing known risks.

29. In the absence of such a transnational framework, locally developed solutions and safeguards with local enforcement is one option. In that scenario, where an AI solution uses a distributed decision-making mechanism, that distributed mechanism should also be in a single jurisdiction.

30. Other options are bilateral or multilateral agreements, or local regulation within one jurisdiction facilitated by cross-border arrangements, or where AI continues to be implemented with market forces and risks determining the regulation, whether through consumer law or other forms of redress.

31. Unless and until a specific ad hoc international law mechanism for settling jurisdictional issues in ICT is developed, especially for AI solutions developed in one jurisdiction but used in another, where an AI solution is required to operate across multiple jurisdictions, it should be implemented and operated as a multinational federation of individual single-jurisdiction AI solutions.

Ethical and lawful basis

32. As the processing of personal data of individuals always intrudes on the rights of the data subject, the data processing underlying an AI solution must have a sound ethical and legal basis. That becomes even more important if the processing itself is designed to lead to, or to make decisions affecting, the position or the rights of the data subject. Irrespective of the jurisdiction or the manager’s individual legal environment, one or more of the following scenarios may provide a sufficient legal basis for the processing of data by an AI system:

(a) If a law was drafted in accordance with democratic principles and human rights, it could provide a specific legal basis, if it addresses the conflict of interests between managers and the data subjects, and provides appropriate safeguards for the protection of data subject rights;

(b) If the usage of the AI solution is necessary for the fulfilment of a contract with the data subject and has their explicit consent, and if the contract does not disadvantage the data subject materially or infringe on the human rights of the data subject or others;

(c) If the data subject has freely consented, on an informed basis, covering the AI purpose, the consequences of its use and procedures for withdrawing consent. The consent has to be given by concrete action and the responsible manager must provide a consent management system that allows withdrawal of consent at any time and includes adequate documentation;

(d) On the basis of a legitimate, prevailing interest of the manager and/or major societal interest, if the data subjects are adequately informed before the processing starts and are given the opportunity to object to the processing, or are entitled, at a minimum, to access the mechanism or procedures in place, within a reasonable time period, or to remedy their situation;

(e) Every AI solution is bound by and limited to the purpose for which it was originally designed, implemented and correctly documented. While that does not prevent other or additional uses (such as further processing) or the usage by another manager, the

further use needs to be evaluated anew with regard to the legal basis and safeguarding measures, including seemingly compatible purposes;

(f) Special conditions have been established to protect and provide legal bases for application of AI solutions to data subjects in special, sensitive or vulnerable categories, such as children, prisoners or other groups.

Data fundamentals

33. Data quality includes accuracy, such as currency and non-discrimination, as well as minimization and purpose limitation. Data protection requirements should be addressed, as should any additional requirements for the processing of specific data, such as health-related data or children's data.

Responsibility and oversight

34. Within an organization, each AI solution needs either a legal or a natural person to take full responsibility for the data processing and its results. That covers all aspects of the management of the process and the technology, including the lawfulness of the processing, its documentation, adaption, results, the trusted verifiability of the algorithm dataset, processing, insight consideration and collaboration and the fulfilment of the rights of the data subjects. Where the AI solution is distributed beyond the organization, the responsibilities for subsequent parties needs to be identified, documented and agreed.

35. Those responsibilities, including an eventual processor of the AI solution, must be transparent and adequately accessible by the data subjects and public supervisory authorities and regulators.

36. Appropriate governance, particularly in larger legal entities, can include a data privacy officer, whose responsibilities and functions include providing advice on compliance with data privacy requirements and monitoring the implementation of the AI solution. The post of data privacy officer must be provided with adequate resources and authority to undertake those functions, and the position holder should undergo complete and appropriate training or be qualified, whether by certification or experience, to perform the duties and tasks in an effective and independent manner. The establishment of effective channels of communication between that role and the relevant oversight or supervisory body is strongly encouraged. In smaller States and in start-ups, investment in AI governance is required, whether or not it includes the establishment of such a position.

37. Information on those accountability arrangements is to be made publicly available.

38. Oversight by an independent, competent regulator is required, as is judicial remedy for violation of relevant law.

Control

39. AI solutions, including those procured from a third party, must be under the full control of the relevant manager. From the first design idea to the final switch-off and decommissioning, it must be clear what data are processed in the AI solution, what parameters and data quality metrics provide the basis for the decision-making and how they will be balanced and weighted against each other. The results must be monitored continuously and corrected if necessary. In the area of automated decision-making solutions, no decisions are to be made based on conscious or unconscious bias. Possible bias and discriminatory effects must be checked and corrected before roll-out of a system and at regular intervals throughout its lifetime.

40. In the case of AI for decision support systems, a similar set of controls is required for the decision maker.

41. The manager, in conjunction with processors as necessary, must be able to stop or change the processing at any time. Incorrect results must be documented, as must the corrective measures taken, in order to mitigate any risks for the data subjects. Once their use for identification, corrective or forensic purposes is completed, incorrect results must be deleted without undue delay.

42. Internal and external reviews of the operation of such control are to be established and must be able to address any critical findings regarding the AI solution or its results.

Transparency and "explainability"

43. AI solutions must be made transparent to the public and the data subjects. The information must be meaningful, intelligible and cover all relevant aspects regarding the evaluation of the solution and possible rights of the data subjects. That includes the "explainability" of the purpose, the overall functions, supporting processes, the data sources used and the range of the planned outcome. Those aspects may include:

(a) Data sources and data used to feed and train the AI solution, plus data resulting from the AI solution;

(b) The purpose and legal basis for the processing;

(c) The parameters building the basis for AI decisions and their weighting;

(d) Clarification of whether the AI solution is intended to prepare for final decisions to be made by human beings (decision support) or if it is making the final decision itself (automated decision-making);

(e) How responsibilities are shared between manager and processor, if not identical, and contact details and possible communication channels;

(f) Integration of third parties (e.g. other managers or processors), transfer to other countries (if any) and the reason for the integration and transfer. That also requires a declaration that third parties are bound by the same requirements, such as data protection requirements, as the manager, and have similar roles and responsibilities, no matter where they are located;

(g) The necessary information must be published at a minimum in the data privacy policy covering the AI solution and must be accessible, understandable and relevant to the data subjects.

Rights of the data subject

44. Persons or groups of persons whose personal information or identifiable personal information is processed by the AI solution (data subjects) shall have the rights to:

(a) Understand and query, in order to ascertain in an intelligible form, whether personal data is stored in automatic data files and if so, for what purposes, and which public authorities or private individuals or bodies control or may control their files;

(b) Withdraw consent without negative consequences at any time during processing, if consent was given and utilized as the legal basis for processing;

(c) Object to the data processing for good reason at any time if the processing is based on legitimate interest;

(d) Obtain information regarding the fulfilment of all data privacy requirements listed in the present section;

(e) Gain proportionate access to their data with comprehensive written information about their personal data, how their personal data are used and processed, and the results and how the results might affect their position and their individual rights;

(f) Request a decision by a human being if they have reasonable doubts that the decision proposed or made by the AI solution is not accurate or correct;

(g) Correct data if they are inaccurate;

(h) Make a complaint and receive a remedy if the complaint is upheld;

(i) Erase and purge the data if the purpose of the AI solution ceases to exist or if the data are no longer needed for another legal purpose.

45. Those rights do not overrule other rights and/or exceed rights granted to the data subjects under applicable law in a given jurisdiction.

Safeguards

46. AI solutions should function in a robust way and should be secured by appropriate safeguards against risk, using methods that foster the trust and understanding of all parties involved, including the data subjects and the public. Before deployment, all AI solutions, even if only on a test basis, must undergo at a minimum an initial human rights and data protection risk assessment that identifies the specific risks and criticalities associated with the intended solution. Depending on the outcome of that initial assessment, further assessment of rights and risks may be required.

47. Using a "privacy by design" approach, technical and organizational safeguards to mitigate the identified risks must be assessed individually. That should cover measures like anonymization or pseudonymization, encryption, client separation, access management (limitation), deletion policy, and log and activity monitoring.

48. Emerging new risks and challenges arising from technological, architectural and/or structural developments, like distributed computing, must be examined during the risk assessment.

49. Risk mitigation can be based on international standards such as those published jointly by the International Organization for Standardization and the International Electrotechnical Commission in the ISO/IEC 27000 series (information security management systems). In particular, ISO/IEC 27701 contains data privacy extensions establishing at the minimum measures for:

(a) Protection: controls to protect against the effects of assessed risks;

(b) Detection: controls to detect abnormalities as soon as possible;

(c) Responding: controls to contain and defeat the risk of abnormal events and to ensure that core business processes can still function until such time as the overall solution is found and the situation returns to normal.

B. Assessment of criticality of artificial intelligence solutions

50. The measures to be taken must be human-centred and proportionate to the risks of infringements of human rights, especially discrimination, and of data protection, as well as the complexity or criticality of a data processing solution. Suitable approaches include those listed below.

Human rights assessment in the planning phase

51. All AI solutions must respect the rule of law, human rights, democratic values and diversity. Therefore, every planned AI solution, including algorithms, should undergo a timely human rights assessment, including ethical and equality assessments. The right to equal treatment must not be unlawfully violated by the planned AI solution. For example, AI solutions using information reflecting an unconscious bias will lead to results that might discriminate against certain individuals or groups in society. Moreover, an AI solution fed with the "right" information can lead to "wrong" results, as the learning of the AI solution derived from the collected information might lead to erroneous assumptions by the AI solution.

52. Privacy by design and by default necessitates an assessment in the planning phase of how any human rights, including the right to privacy, might be affected by the implementation of the AI solution.

Test and correction phase – monitoring

53. After the planning phase and the initial human rights assessment, the identified framing conditions must be considered in the further development phase. During the implementation phase and before going live, AI solutions should undergo an intensive test phase with testing data in a separate, self-contained environment to assess whether the underlying general assumptions are not only considered, but also fulfilled. Only if the

responsible manager can be sure that the AI solution runs properly should it be launched for live operations.

54. During the whole running time of the AI solution, until the final switch-off, the results produced by the AI solution must be monitored against the fundamental requirements defined in the planning phase.

55. The difficulties of controlling all aspects of the algorithms' operations and the constant change of algorithms during the running time of an AI solution make it essential to constantly check the results against the initial intended purpose of the solution in another feasible way to provide a point of comparison. If a deviation is suspected or observed, the data feed for the AI solution must be adapted accordingly or the solution itself stopped.

56. To gain the benefits of new creative approaches and widen the horizon of the developer and the manager, input and feedback from privacy, cross-sectoral, cross-industry, civil society and user communities needs to be factored into the development, testing and monitoring of AI solutions. A testing facility must be established for ready-to-run AI solutions, for example, by installing a so-called black box in the Internet where the separated and self-contained solution is open to third parties to input data to ascertain the type of results the AI solution will produce, or the implementation by regulators of sandboxes within organizations involved in introducing AI solutions.

Criticality assessment based on the use of different kinds of data

57. Besides proper planning, testing and implementation, the criticality of data and the intended purpose are relevant also to the measures necessary for proper processing.

58. That applies to general data, like general personal information or data in the context of telecommunication services or health. Health-related data and some other information, for example, the contents of telecommunications, have to be treated more rigorously than less sensitive personal information. That means that the relevant technical and organizational measures must be strengthened relative to other cases, for example, strict purpose limitation and data minimization, encryption, pseudonymization, restricted access and early deletion or anonymization.

59. The intended data use plays a key role in determining the level of protection required. If personal information is processed purely for storage purposes, that might be less critical than profiling uses. The legitimacy of the purpose and safeguarding measures must be assessed extremely carefully.

60. Those actions must be taken and documented during all risk assessments.

Periodic assessment of artificial intelligence systems conducted and logged, with records available to external audit and regulatory bodies

61. The assessment evaluates the system for:

(a) Intended or unintended outcomes;

(b) Fairness for, bias towards and discrimination against individuals and groups;

(c) Trade-offs and mitigations.

C. Additional considerations

External audits and certification

62. Audits and certification schemes should have access to all relevant internal documentation such as evaluation logs to monitor compliance of AI systems with engineering and ethical standards developed using multi-stakeholder and multilateral approaches.

63. External certification of an approved auditor in data privacy who is also formally recognized as having AI expertise should be considered. That may be helpful in allaying the concerns of the public and data subjects. It may be particularly applicable for AI solutions

that could lead to major adverse outcomes and a loss of trust by the public and/or the regulatory community.

Changes in legislation and regulations

64. Changes in legislation and regulations are being considered worldwide and will affect the majority of AI solutions. Compliance will largely depend on:

(a) Meeting existing and emerging national and international standards;

(b) Certification by an appropriate certification authority operating under a national or international agreement.

Engagement in discussions

65. Those responsible for AI strategies and/or or operational AI solutions, as well as those monitoring their uses, should engage in discussions on AI and emerging ethical and technical questions.

Education and awareness

66. AI is a complex subject and the deployment of data in AI systems and their use in AI solutions requires clear, comprehensive explanation to users and data providers, as well as executives, managers and others involved in decisions about AI solutions and their operations. Publication of algorithms alone is insufficient.

II. Principles and recommendations on the right to privacy of children

67. Children are entitled to human rights and freedoms, as are all individuals. International and regional legal instruments articulate the right to privacy and children's right to privacy.[3]

68. The principal instruments enshrining children's rights are the Universal Declaration of Human Rights and the Convention on the Rights of the Child, which has achieved near universal acceptance with ratification by 193 parties.

69. Article 16 of the Convention states that:

(1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

(2) The child has the right to the protection of the law against such interference or attacks.

70. That article must be interpreted broadly to fully accommodate the privacy experiences of children.[4]

71. Children's rights are universal, indivisible, interdependent and interrelated.[5] Their right to privacy enables their access to other rights critical to developing personality and

[3] They include regional instruments, such as the African Charter on the Rights and Welfare of the Child (1990) and the European Convention on the Exercise of Children's Rights (1996), and regional systems, such as the Inter-American system of human rights.

[4] John Tobin and Sarah M. Field, "Article 16: The right to protection of privacy, family, home, correspondence, honour, and reputation", in *The UN Convention on the Rights of the Child: a commentary*, John Tobin, ed. (Oxford, Oxford University Press, 2019).

[5] Committee on the Rights of the Child, general comment No. 16 (2013), para. 12.

personhood,[6] such as the rights to freedom of expression[7] and of association and the right to health, among others. Children's privacy relates to their bodily and mental integrity, decisional autonomy, personal identity, informational privacy and physical/spatial privacy.

72. The foundations of future intellectual, emotional and sexual life are developed in childhood and adolescence, aided by the conditions of a private life.[8] Around the world, experiences of childhood and the right to privacy differ.[9] Intersectional factors such as race affect the construction of childhood.[10]

73. Generally, the domains instrumental to children's formation of their personalities are family and homelife, school and social networks. Like children's rights, those domains are interrelated and reflect underlying structural factors.

74. Children without home and family, such as unaccompanied children, children in street situations, children in "out of home" care, children in conflict zones and in other vulnerable situations, experience many more challenges in accessing their human rights.[11]

75. While privacy means different things to different people, the Special Rapporteur emphasizes the positive, facilitative aspect of the right to privacy that goes to the innate dignity of the person and facilitates the enjoyment of other human rights.[12]

76. "Self-determination" is characterized as the individual's ability to decide whether and to what extent to disclose aspects of his or her personal life.[13] Autonomy is meant as the ability for self-direction in thought, feeling and action. The term "child" refers to an individual under 18 years of age.

Identification of issues

Interests in tension

77. To consider how children's right to privacy and personality invokes autonomy is to examine the tensions and differing perspectives within which those rights rest.

78. The Convention on the Rights of the Child provides States parties and parents with the capacity and obligation, where necessary, to adjudicate children's enjoyment of their article 16 rights consistent with their evolving capacity (art. 5) in order to secure the best interests of the child (art. 3).[14]

79. Traditionally, the privacy rights of children have been regarded as an issue for adults to determine. Children's privacy needs, however, differ from and can conflict with those of

[6] Submission from Office of the United Nations High Commissioner for Human Rights (OHCHR) Regional Office for the Middle East and North Africa Region (permission was not provided to post the submission).

[7] Submission from International Federation of Library Associations and Institutions, p. 2. Where authorization was granted, the submissions received by the Special Rapporteur in response to his consultations will be posted at www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_Privacy_and_Children.aspx.

[8] Submission from Belgian Disability Forum, p. 2.

[9] Submissions from InternetLab and Alana Institute; Office of the Victorian Information Commissioner, Australia.

[10] Rebecca Epstein, Jamila Blake and Thalia González, "Girlhood interrupted: the erasure of black girls' childhood", Georgetown Law Center on Poverty and Inequality, 2017.

[11] Submission from Maat for Peace, Development and Human Rights, p. 7.

[12] See General Assembly resolution 68/167, Human Rights Council resolution 20/8 and A/HRC/13/37.

[13] Abstract of the German Federal Constitutional Court's judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES].

[14] Tobin and Field, "Article 16".

adults.[15] "Sharenting", for example, can bring parents' right to freedom of expression into conflict with their child's right to privacy.[16]

80. Adults' interpretations of children's privacy needs can impede the healthy development of autonomy and independence, and restrict children's privacy in the name of protection.[17] Adult reliance on surveillance to protect children is a case in point. It constrains children's rights to privacy and autonomy,[18] yet children are increasingly subject to technological surveillance by Governments, the private sector, parents, family and peers. Parental surveillance increases rather than decreases with a child's age, that is, when young people are (or should be) becoming more independent.[19] Parents and carers of children with additional needs favour even more protective stances involving high default privacy settings and the ability to determine their children's online privacy.[20]

81. Parental behaviour can contradict parents' avowed concerns. Reportedly, 57 per cent of parents of teenagers aged 13–17 years old worry about their child receiving or sending explicit images,[21] and 85 per cent have concerns about their children's digital privacy. Yet fewer than one in three parents use parental settings on their children's device, and 81 per cent knowingly let their children use general audience YouTube without oversight.[22]

82. The need for evidence-based child-centred risk assessment, policies and regulation is indicated by recent research revealing that adults who had not experienced online harms, such as violent threats or trolling, were more likely to want to restrict information access and online anonymity.[23]

83. As they mature, children desire and require privacy, not only from schools, businesses and Governments, but also from their parents.[24] That need grows as children grow. While children between the ages of 5 and 7 generally do not consider parental monitoring of their online activities as a violation of privacy, teenagers aged between 15 and 17 are often concerned about parental and school monitoring.[25] Adolescents believe that privacy and private spaces away from judgment and monitoring allow them to explore ideas and creative expression and develop independent opinions.[26] Parental controls need to be proportionate to the child's evolving capacity and views.[27]

[15] Submissions from Parental Rights Foundation; Action Canada for Sexual Health and Rights, p. 4; Commission Nationale de l'Informatique et des Libertés (CNIL), p. 11.

[16] Submission from South Australia Commissioner for Children and Young People (in which the term "sharenting" is explained as the increasing tendency of parents and parents-to-be to use the Internet to post information about their children online, which shapes a child's online identity long before the child has the capacity to give consent or begins creating its own digital footprint), p. 3.

[17] Submission from International Child Rights Center and MINBYUN.

[18] Ibid.; Jane Bailey and Valerie Steeves, *Defamation Law in the Age of the Internet: young people's perspectives* (Law Commission of Ontario, Canada, 2017); submission from Ariel Foundation International.

[19] Submission from South Australia Commissioner for Children and Young People.

[20] See www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf.

[21] Monica Anderson "A majority of teens have experienced some form of cyberbullying", Pew Research Center, 27 September 2018.

[22] Submission from ACT/The App Association.

[23] BT/DEMOS, "Online harms: a snapshot of public opinion" (2020). Available at https://demos.co.uk/wp-content/uploads/2020/10/Online-Harms-A-Snapshot-of-Public-Opinion-1.pdf.

[24] Submissions from Future of Privacy Forum; Ariel Foundation International.

[25] Submission from Global Privacy Assembly, Digital Education Working Group, p. 25.

[26] Submission from Office of the Victorian Information Commissioner, Australia.

[27] Submission from CNIL, p. 11.

Personal identity

84. Today's children are the first generation to be born into a digital age,[28] while their parents are the first to rear "digital children".[29]

85. Increasingly, a child's identity commences before birth with in utero images shared by parents and families across the web. Many of those images embed personal information.

86. Children's digital identity formation continues largely through the actions of family throughout childhood, with 80 per cent of children living in developed Western countries having a digital footprint before they are 2 years old.[30] Children's images have also been used without consent for charitable fundraising.[31]

87. Children now participate online in multiple ways and at earlier ages than previously.[32] Their social media use undergoes a step change between ages of 9 to 10 and 11 to 12, doubling from 34 per cent to 69 per cent.[33] The number of online contacts children have doubles between the seventh and eleventh grades.[34] Many children under the age of 13 have social media profiles (38 per cent of 9–12 year olds, according to European surveys)[35] and most have between two and five of them.[36] The coronavirus disease (COVID-19) pandemic has increased that trend, with daily active accounts for Facebook's Messenger Kids growing by 350 per cent from March to September 2020.[37]

88. Increasingly, self-esteem and self-concept, necessary for the formation of personality and identity, are constructed digitally.[38] Children use the Internet as an ongoing report on their lives, the hearts and thumbs up on social media becoming appendages to their thoughts,[39] yet they are concerned about losing control of their information online.[40]

89. Violence, sexual abuse and cyberbullying feature in digital life, particularly for LGBTQI young people (see A/HRC/43/52). Some 25 per cent of teenagers aged between 13 and 17 reported having been sent explicit images without their consent.[41] Some 29 per cent of girls and 20 per cent of boys report being the recipients of unsought explicit images. Unwanted receipt and distribution of images, even when not objectively harmful, offensive or embarrassing, can impair the development of a child's self-esteem, autonomy, relationships and psychosocial development.[42]

90. Child sexual abuse, whether offline or online, is a violation of bodily integrity and decisional autonomy. It has long-term consequences on personality and capacity, and the continued existence online of child sexual abuse material compounds those consequences. The forms and consequences of abuse are embedded in how society views children and their

[28] Submission from Canadian Human Rights Commission, p. 2.

[29] Danah Boyd, "Social network sites as networked publics: affordances, dynamics, and implications", in *A Networked Self: Identity, Community, and Culture on Social Network Sites*, Zizi Papacharissi ed. (Routledge, 2011).

[30] Submission from Hungarian National Authority for Data Protection and Freedom of Information, p. 42.

[31] Submissions from International Child Rights Center and MINBYUN; Ombudsman for Children, Croatia, p. 3.

[32] Submissions from Information Commissioner's Office, United Kingdom; CNIL; Information and Data Protection Commissioner, Albania.

[33] Submission from Economic Commission for Latin America and the Caribbean (ECLAC).

[34] Submission from Hungarian National Authority for Data Protection and Freedom of Information, p. 29.

[35] Ibid., p. 53.

[36] Submission from Information and Data Protection Commissioner, Albania, p. 14.

[37] Submission from Facebook.

[38] Submissions from Anna Bunn, p. 11; Office of the Victorian Information Commissioner, Australia, p. 2.

[39] Submission from Ariel Foundation International.

[40] Submissions from C. Mahieu; Office of the Victorian Information Commissioner, Australia; CNIL.

[41] Monica Anderson, "A majority of teens have experienced some form of cyberbullying".

[42] Submissions from Bunn; Mahieu.

bodies.[43] Countering such abuse requires strategies based on human rights.[44] Young people's immersion in the ever-expanding range of digital technologies produces an ongoing stream of data, collected and enhanced by artificial intelligence, machine-learning applications and facial and speech recognition technologies. Children and their data fuel the business of the digital world.[45] The online advertising market for children could be worth $1.7 billion by 2021, with more than 72 million pieces of data collected for each child by online advertising companies before the child reaches the age of 13.[46]

91. Marketers reach, influence and forge ongoing relationships with young people. Younger children are particularly vulnerable to targeted marketing as they do not differentiate between advertising and content or between fiction and reality, or understand the persuasive nature of advertising.[47] Technology incorporating behavioural techniques (persuasive design/dark practices) maximizes engagement, triggers impulsive behaviours, influences decision-making, sparks fears of exclusion and overrides privacy concerns.[48]

92. Profiling children limits their potential self-development in childhood, adolescence and possibly adulthood, as behavioural predictions and nudging techniques can predetermine options and choices. Technological offerings need to be assessed against children's rights and best interests,[49] as the processing of children's personal data can:

(a) Infringe privacy and data protection, including loss of autonomy and damage to personal reputation;

(b) Harm children's mental and emotional health and physical well-being;

(c) Result in economic harms or commercial exploitation.[50]

93. Children and young people seek responses that minimize corporate access to and use of their data;[51] a zoning of commercial activity, and mechanisms for addressing their best interests, including the ability to erase posted material.[52] Children believe they should be able to exercise their rights to ask any company for a copy of their personal data, and around 40 per cent think they should be able to make access or erasure requests at any age, with 21 per cent saying at 13 or younger. Only 13.5 per cent thought it necessary to be 18 or older to make an access or erasure request.[53]

94. The digital era benefits children's development. However, children must be able to enjoy, unimpaired by commercial practices, their rights to unhindered development of personality.

95. Biometric surveillance and tracking technologies used to identify and monitor children suspected of wrongdoing was reported from South America, as was the failure to protect children's privacy during judicial processes.[54] Identifying children of interest to law enforcement authorities or the offspring of incarcerated parents or of parents associated with

[43] Submission from InternetLab and Alana Institute.

[44] Committee on the Elimination of Discrimination against Women, general recommendation No. 38 (2020); submission from Maat for Peace, Development and Human Rights, p. 7.

[45] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019); submission from InternetLab and Alana Institute.

[46] Submission from CNIL, p. 3.

[47] Submissions from Campaign for Commercial-Free Childhood and Center for Digital Democracy; InternetLab and Alana institute; CNIL.

[48] Submissions from Information Commissioner's Office, United Kingdom; Office of the Victorian Information Commissioner, Australia; Mahieu; Jonathan Crock and others, American University; CNIL; ECLAC.

[49] Submissions from Canadian Human Rights Commission, p. 2; Office of the Victorian Information Commissioner, Australia; Campaign for Commercial-Free Childhood and Center for Digital Democracy.

[50] Submission from Information Commissioner's Office, United Kingdom.

[51] Valerie Steeves, "Young Canadians in a wired world, phase III: trends and recommendations", MediaSmarts, 2014.

[52] Submission from The eQuality Project.

[53] Submission from Global Privacy Assembly, p. 24.

[54] Submission from InternetLab and Alana Institute.

terrorism contravenes privacy, leading to stigmatization and discrimination and impairing the development of personality.[55] Development can be constrained also when those children are not identified to relevant support services,[56] although data sharing can be problematic, particularly with security personnel.[57]

Sexuality, gender, bodily integrity and physical autonomy

96. Children vary enormously in their physical, intellectual, social and emotional capacity. The differences are particularly pronounced in adolescence, a period characterized by rapid physical, cognitive and social changes, including sexual and reproductive maturation.[58]

97. Sexual expression, bodily integrity and physical autonomy are part of the interwoven fabric of children's privacy, and also of their freedom of expression.[59] Adolescents need to be able to make decisions regarding their well-being and bodies, and to safely and privately explore their sexuality as they mature,[60] whether offline or online.[61]

98. The bodily integrity and autonomy rights of children, however, are infringed by the actions of Governments, commercial entities, health-care and other professionals, parents and peers. Infringements identified include:[62]

(a) Girls being subjected to female genital mutilation; forced marriages; forced sex; forced pregnancy and motherhood; forced pregnancy testing; forced sterilizations; denial of reproductive sexual information and services; mandatory parental notification and/or consent for prescribed contraceptives and abortion; "conversion" therapies; criminal penalties for consensual peer sexual activity, including sexting; sexual abuse online and offline; "honour" killings; and "slut shaming";

(b) Boys being subjected to genital mutilation; forced marriages; forced sex; forced sterilizations; denial of reproductive sexual information and services; "conversion" therapies; criminal penalties for consensual peer sexual activity, including sexting; sexual abuse online and offline; harassment; and corporal punishment;

(c) Children with diverse gender identities, sexual orientations and expression, and variations in sex characteristics being subjected to violence; discrimination and harassment; pathologization of their gender identity or body; unnecessary medical treatment; publication of details concerning genitalia; stigmatization; "instructive" rape; "conversion" therapies; withholding of specific health services, including trans health-care and reproductive sexual information and services; denial of access to medical records; criminal penalties for consensual peer sexual activity, including sexting; sexual abuse online and offline; and lack of legal gender recognition.

99. Infringements of bodily privacy impact other rights, such as those enshrined in articles 3, 6, 8, 12, 16, 19 and 29 (1) of the Convention on the Rights of the Child. For example:[63]

(a) Mandatory pregnancy testing infringes girls' rights to dignity, equality and autonomy;

[55] Committee on the Rights of the Child, general comment No. 24 (2019).

[56] Submissions from Children of Prisoners Europe; Families Outside; International Coalition for the Children of Incarcerated Parents; Quaker United Nations Office.

[57] United Nations Office on Drugs and Crime (UNODC), *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System* (Vienna, 2017) pp. 138–139; United Nations, Office of Counter-Terrorism, *Children affected by the foreign-fighter phenomenon: ensuring a child rights-based approach* (2019), p. 103.

[58] Committee on the Rights of the Child, general comment No. 4 (2003).

[59] Submissions from Matimba; Council of Europe; Australian Human Rights Commission.

[60] Submission from Center for International Human Rights.

[61] Submission from ParentsTogether.

[62] Submissions from Crock and others; Human Rights Watch; ILGA-Europe, Transgender Europe and The International Lesbian, Gay, Bisexual, Transgender, Queer and Intersex Youth and Student Organisation; NNID, Netherlands organisation for sex diversity; CHOICE for Youth and Sexuality; OutRight Action International; Australian Human Rights Commission; Center for International Human Rights; Council of Europe.

[63] Submission from Organisation Intersex International Europe.

(b) Surveys to identify sex/gender diverse students violate the right to non-discrimination, and when used to expel students, breach their right to education;

(c) "Voluntary" virginity testing, often imposed by parents, infringes girls' rights to dignity, equality and autonomy;

(d) Highly medicalized processes entailing surgery for legal gender recognition implicate the right to health;[64]

(e) Mandatory parental consent or notification for sexual or reproductive health services implicate the right to health, identity, life, protection from harm and the best interests of the child.

100. Children need and have the right to guidance on healthy sexual relationships, consent and safe practices.[65] Comprehensive sexuality education can help children protect and advance their privacy, independence and autonomy,[66] and facilitate well-being, particularly for LGBTQI young people.[67] Backlashes against providing children and adolescents with comprehensive sexuality education were reported around the world, including in Brazil, the Dominican Republic, Ghana, Kenya and Poland.[68]

Recognition of identity

101. All individuals have rights precisely because of their inherent and equal identity as human beings.[69] Records and record-keeping systems establish official identity,[70] yet rarely afford children agency over their records.

102. Official identity commences with birth registration. Yet many children around the world, and disproportionately among Aboriginal and indigenous communities, are not registered.[71] The lack of legal recognition affects access to many rights necessary for autonomy, such as education.

103. Birth certificates can pose challenges to attaining dignity, identity, privacy and development for transgender and intersex children, children born through international surrogacy arrangements, missing children, unaccompanied refugee children and children in out-of-home care, among others.[72]

Education and schooling

104. The purpose of education is to develop children's personalities, talents and mental and physical abilities to their fullest potential.[73] Education is a human right and the primary vehicle for children to have a life of dignity. It empowers children, individually and collectively, by safeguarding them from exploitation. The right to education requires States to respect, protect and fulfil by removing barriers to education such as gender bans and violence.[74]

[64] Submissions from Matimba; A. McCarthy.

[65] Committee on the Rights of the Child, general comment No. 15 (2013); Committee on Economic, Social and Cultural Rights, general comment No. 22 (2016); submissions from Australian Human Rights Commission; Mahieu; Center for Reproductive Rights, p. 1.

[66] Submissions from Action Canada for Sexual Health and Rights; ILGA Europe, Transgender Europe and The International Lesbian, Gay, Bisexual, Transgender, Queer and Intersex Youth and Student Organisation.

[67] Submission from McCarthy.

[68] Submission from Human Rights Watch, para. 18.

[69] Dinah Shelton, "On identity", *The George Washington International Law Review*, vol. 39 (1999).

[70] Submission from Rights in Records by Design, Monash University and Federation University; *D.Z. v. Netherlands* (CCPR/C/130/D/2918/2016).

[71] Submission from Australian Human Rights Commission.

[72] Submissions from Australian Human Rights Commission; Rights in Records by Design, Monash University and Federation University; Kathryn Allan and David Lacey, "Identity management in disaster response environments: a child exploitation mitigation perspective", *Australian Journal of Emergency Management*, vol. 33, No. 3 (July 2018).

[73] Convention on the Rights of the Child, art. 29 (1) (a).

[74] General Assembly resolution 75/166.

105. Schools play a large part in how children experience privacy on a day-to-day basis. Once the COVID-19 pandemic was declared, by 1 April 2020, 193 countries had closed schools, affecting approximately 90 per cent of the global student population.[75]

106. Online education saw downloads of education applications increase 90 per cent compared to the weekly average in late 2019.[76] The shift to online education amplified existing power imbalances between education technology companies and children, and between Governments and children and parents, with several Governments waiving existing child data privacy laws. In Wales, for example, the Government waived the requirement for parents' and students' consent.[77] In other places, there is no protection for children's right to privacy in government schools.[78] Yet non-State actors routinely control children's digital educational records.[79]

107. The digitalization and storage of children's learning data includes thinking characteristics, learning trajectory, engagement score, response times, pages read and videos viewed.[80] Most children and parents do not have the capacity to challenge educational technology companies' privacy arrangements or to refuse to provide data, as education is compulsory.[81]

108. The selection of applications and web-based learning tools by schools has focused on curriculum and financial considerations over privacy.[82] In September 2020, an analysis of 496 educational technology applications in 22 countries found many were collecting device identifiers, 27 applications were taking location data, and 79 out of 123 manually tested applications were sharing user data with third parties, such as advertising partners.[83] Data security is concerning. Microsoft, for example, reported 5.7 million malware incidents affecting users of its education software between 24 August and 24 September 2020.[84]

109. Schools themselves hold significant amounts of children's information and increasingly track children by monitoring students' online activities and surveillance cameras.[85] Like educational technology applications, usage of that technology requires accountability, meaningful consent, purpose limitation, data minimization, transparency and security safeguards.[86]

110. Educational processes need not and should not undermine the enjoyment of privacy and other rights, wherever or however education occurs,[87] nor intensify existing inequalities.[88]

Age appropriateness and evolving capacity

111. The term "age appropriate" is generally accepted as an alignment between chronological age and behaviours, and an alignment of chronological age with services available to children, such as online content. Age appropriateness in the regulatory sense is

[75] Submission from ParentsTogether.
[76] Submission from Human Rights Watch, para. 44.
[77] Ibid., para. 48.
[78] Submission from South Australia Commissioner for Children and Young People.
[79] See https://rm.coe.int/educational-settings/16809f3ba3.
[80] Submission from Global Privacy Assembly, p. 4.
[81] Submissions from DefendDigitalMe; Council of Europe.
[82] Submission from Office of the Victorian Information Commissioner, Australia.
[83] Alfred Ng, "Education apps are sending your location data and personal info to advertisers", CNET, 1 September 2020.
[84] Submission from Human Rights Watch, para. 49.
[85] Submission from South Australia Commissioner for Children and Young People.
[86] Submissions from InternetLab and Alana Institute; Research Group on Technology, Information and Society, University of Fortaleza, Brazil; Ombudsman of the Autonomous City of Buenos Aires; Council of Europe.
[87] Convention on the Rights of the Child, general comment No. 1 (2001); General Assembly resolution 75/166; submissions from DefendDigitalMe; Ombudsman of the Autonomous City of Buenos Aires; Research Group on Technology, Information and Society, University of Fortaleza, Brazil; Hungarian National Authority for Data Protection and Freedom of Information, case number NAIH/2020/7127/.
[88] General Assembly resolution 75/166; submissions from Ombudsman of the Autonomous City of Buenos Aires; ECLAC; Council of Europe.

a standard against which online providers are held for services suitable to children's ages. The Age Appropriate Design Code in the United Kingdom of Great Britain and Northern Ireland is a recent example.[89] In the United States of America, the Children's Online Privacy Protection Act of 1998 imposes requirements on website operators and online services directed to children under 13 years of age, and on operators of other websites or online services that know they are collecting personal information online from children under 13.

112. Nevertheless, the age appropriate mechanism is not a cure-all, since:

(a) Material may be age appropriate and still harmful to children and their rights. The mechanism may protect and empower a child when individualized, but may not meet the needs of a cohort of children given the considerable variation in intellectual and emotional development among children of the same age;[90]

(b) As a generic threshold, age appropriateness poses inequities for children of differing capacity and is a crude measure of their evolving capacities, potentially constraining the development of their personalities and the autonomous exercise of their rights, and is possibly discriminatory;

(c) When age is the criterion for accessing services, verifiable identity documents are required, raising concerns around security, prescriptive approaches and the lack of age assurance standards, tools and industry certification schemes.[91] Others indicate that age verification processes can be delivered in a way that is compatible with privacy.[92]

113. Age alone has been seen as an imperfect metric to assess the capabilities of children.[93] Some countries recognize capacity not based on chronological age.[94] In early 2020, the authorities in Ontario, Canada, introduced legislation enabling young people to access and request correction of their personal information explicitly on the basis of capacity, not age. In the event of a conflict, the child's rights could prevail over the decisions of parents or guardians.[95]

114. Children's readiness for decision-making and self-responsibility is best determined not by chronological age alone but by context, including the risks and support available, individual experience, the rights affected and capacity for understanding the implications of their actions (or non-actions). Determinations on when children are capable, for example, of consenting to the processing of their personal data, must take into consideration their actual understanding of the data processing, their best interests, rights and views.[96]

115. Essentially, the notion of age appropriateness sits uneasily with the principle of evolving capacity. Calibration of services to children's evolving capacities requires more exploration.

Options for solutions

116. Maximizing children's privacy is a crucial means of acting in their best interests.[97] A best interests approach requires adults to actively seek children's views and treat them seriously. That is not always evidenced in the actions of States, companies, parents and

[89] See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/.

[90] Convention on the Rights of the Child, general comment No. 7 (2005).

[91] Submissions from CNIL, p. 10; Facebook.

[92] Submission from Yoti.

[93] See www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf.

[94] Submission from Global Privacy Assembly, p. 20.

[95] Ibid., p. 25.

[96] Submission from Council of Europe.

[97] Submission from UNODC.

others,[98] but children are recognized under international law as human beings, and not merely becomings, and are therefore entitled to human rights under international law.[99]

117. All parties – Governments, companies, communities, individuals and parents – need to recognize children as the bearers of rights. Effectively and comprehensively combating ICT-facilitated child abuse, for example, requires a human rights-based, multi-stakeholder approach, actively involving children, families, communities, Governments, civil society and the private sector.[100]

118. While children's dependency, hence vulnerability, can result in risks, risk does not equate to harm and navigating some risk is necessary for children to develop resilience and coping skills.[101] Defining children by their vulnerability only, without consideration of their capacity or potential, is likely to result in overly protectionist agendas, potentially harmful to children's personality.

Protecting children's data

119. While privacy is a broader, more complex concept, data protection is closely related. The free development of personality is nurtured when individuals are protected against the unlimited collection, storage, use and sharing of personal data.

120. Many see consent as a fundament. Consent, however, neither necessarily expresses a child's autonomy nor protects it, particularly where power imbalances exist. Furthermore, parental consent may not always be in the best interests of the child or aligned to the child's views.[102]

121. While the European General Data Protection Regulation could better protect children's personal data,[103] it includes special protection of minors by requiring information tailored to minors on processing of their data (art. 12); special vigilance regarding child profiling (recital 71); and a reinforced right to be forgotten (recital 65), and article 8 introduces a child's capacity to consent to data processing between the ages of 13 and 16.[104] Furthermore, the general elements of data protection by design, privacy by default, the right not to be subject to automated individual decision-making (art. 22) and data protection impact assessments are worthy of wider application for protecting the personal data of children.[105]

122. Convention 108+ [106] also protects against decisions made solely on automated processing of data (art. (1) (a)), and the Council of Europe's recently adopted guidelines on children's data protection in an education setting broaden the definition of personal data processing to cover predictions about groups or persons with shared characteristics, and the definition of biometric data processing to cover those types of processing.[107]

[98] Submission from Promsex.

[99] John Tobin, "Understanding children's rights: a vision beyond vulnerability", *Nordic Journal of International Law*, vol. 84, No. 2 (June 2015).

[100] Submissions from UNODC; Facebook.

[101] Submission from South Australia Commissioner for Children and Young People.

[102] Submission from Ombudsman for Children, Croatia, p. 4.

[103] Simone van der Hof and Eva Lievens, "The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR", *Communications Law*, vol. 23, No. 1 (2018).

[104] Below that age, data processing requires consent from the parent or guardian on the child's behalf.

[105] Van der Hof and Lievens, "The importance of privacy".

[106] Convention for the protection of individuals with regard to the processing of personal data as modernised by the Amending Protocol Council of Europe Treaty Series 223. Available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[107] Submission from Council of Europe.

Privacy engineering and digital literacy

123. Technology design can help counter "persuasive design" and "dark practices",[108] and advance the aims of laws and regulations.[109]

124. Along with privacy engineering of digital technologies, children and adolescents need operational skills and cognitive and social abilities to use technologies in thoughtful, ethical and safe ways. Digital literacy education can prevent harmful online behaviour at its source.[110] There is broad agreement, including among children, that digital literacy can build their online safety and autonomy,[111] particularly given the increasingly younger ages at which children go online and the difficulties for parents in providing effective support.[112]

125. Technical solutions and digital literacy alone, however, are insufficient without rigorous and sustained action by States to address structural inequities and ensure children's privacy, data protection and safety.[113] There is considerable scope for States to invest in better partnerships with civil society, industry, academia and children to co-build solutions as prototypes.

III. Conclusions

126. **Promoting children's privacy and nurturing their autonomy requires:**

(a) **Establishing policies, laws and regulations that:**

(i) **Cast children as the bearers of human rights where their rights to privacy, autonomy and equality are inalienable;**[114]

(ii) **Incorporate the broad scope of privacy, not solely data protection, to enable the full development of children's potential;**[115]

(iii) **Incorporate children's views, children's strategies for privacy, findings of child-focused research and/or child privacy impact assessments in public policy settings;**[116]

(iv) **Provide independent means to conciliate, arbitrate and remedy individual or systemic human rights violations against children**[117] **and ensure that enforcement measures are taken in case of infringements;**[118]

(b) **Addressing the structural dynamics that position children as vulnerable and without agency;**

[108] Submissions from Campaign for Commercial-Free Childhood and Center for Digital Democracy; CNIL.

[109] Submission from ACT/The App Association.

[110] Jane Bailey and Valerie Steeves, *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices* (University of Ottawa Press, 2015); Jane Bailey and Jacquelyn Burkell, "Legal remedies for online attacks: young people's perspectives", *The Annual Review of Interdisciplinary Justice Research*, vol. 9 (2020).

[111] Submissions from International Federation of Library Associations and Institutions; Office of the Victorian Information Commissioner, Australia; Future of Privacy Forum; Council of Europe; Australian Human Rights Commission; and Crock and others, p. 5.

[112] Submissions from Information and Data Protection Commissioner, Albania; InternetLab and Alana.

[113] General Assembly resolution 75/166.

[114] Bailey and Steeves, *eGirls, eCitizens*.

[115] Submissions from South Australia Commissioner for Children and Young People; International Child Rights Center and MINBYUN; Hungarian National Authority for Data Protection and Freedom of Information, p. 58.

[116] Submission from South Australia Commissioner for Children and Young People; Bailey and Steeves, *eGirls, eCitizens*.

[117] Submission from Canadian Human Rights Commission.

[118] Submission from 5Rights Foundation.

(c) **Encouraging technological innovations to improve information communication services while protecting children's privacy.**[119]

IV. Recommendations

127. **The Special Rapporteur recommends that States:**

(a) **Ensure that the rights and values of the Convention on the Rights of the Child concerning privacy, personality and autonomy underpin government legislation, policies, decisions, record systems and services;**

(b) **Support comprehensive analyses of children's capacity for autonomous decision-making for accessing online and other services, to enable evidence-based child specific privacy laws, policies and regulations;**

(c) **Adopt age appropriate standards as a regulatory instrument only with the greatest of caution when no better means exist;**

(d) **Promote and require implementation of safety by design, privacy by design and privacy by default guiding principles for products and services for children and ensure that children have effective remedies against privacy infringements;**

(e) **Encourage partnerships with civil society and industry to co-create technological offerings in the best interests of children and young people;**

(f) **Adopt the Special Rapporteur's recommendations for protecting against gender-based privacy infringements** (**A/HRC/43/52, paras. 33**–**34**);

(g) **Develop comprehensive online educational plans of action based on article 29 (1) of the Convention on the Rights of the Child and the Council of Europe guidelines on children's data protection in an education setting;**[120]

(h) **Ensure appropriate legal frameworks are established and maintained for online education;**

(i) **Create public infrastructure for non-commercial educational and social spaces;**

(j) **Remedy all legislative gaps and procedural exceptions to ensure all children in contact with justice systems have their privacy maintained throughout all proceedings, with lifelong non-publication orders for any criminal justice record;**

(k) **Review legal frameworks to enable voluntary action by companies to lawfully and proportionately detect online child sexual abuse material;**

(l) **Ensure that the personal data of children associated with terrorist or violent extremist groups are classified and shared only where strictly necessary to coordinate individual rehabilitation and reintegration;**

(m) **Prior to the linking of civil and criminal identity databases, undertake human rights impact assessments on the implications for children and their privacy, and conduct consultations to assess the necessity, proportionality and legality of biometric surveillance;**

(n) **Establish practices and laws to ensure that information provided to the media does not violate children's right to privacy and that reporting by media and other bodies protects the privacy of children whose parents are in conflict with the law;**

(o) **Ensure that children's privacy is upheld in all contacts with incarcerated parents, including written, electronic and telephone communications, and prison visits;**

[119] Submission from ACT/The App Association.

[120] See www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting.

(p) **Ensure that biometric data is not collected from children, unless as an exceptional measure only when lawful, necessary, proportionate and fully in line with the rights of the child;**

(q) **Ensure that children's personal data is processed fairly, accurately, securely, for a specific purpose in accordance with a legitimate legal basis utilizing data protection frameworks representing best practice, such as the General Data Protection Regulation and Convention 108+;**

(r) **Ensure that those who process personal data, including parents or carers and educators, are made aware of children's right to privacy and data protection;**

(s) **Ensure that information is available to children on exercising their rights on, for example, the websites of data protection authorities, and ensure the provision of counselling, complaint mechanisms and remedies specifically for children, including for cyberbullying;**

(t) **Ensure that anonymity, pseudonymity or the use of encryption technologies by children are not prohibited in law or in practice;**

(u) **Ensure that opportunities are available to children and young people of all backgrounds to participate in decision-making and design of frameworks, policies and programmes aimed at them;**

(v) **Prohibit automated processing of personal data that profiles children for decision-making concerning the child or to analyse or predict personal preferences, behaviour and attitudes, with exemption only in exceptional circumstances in the best interests of the child or an overriding public interest, with appropriate legal safeguards;**

(w) **Ensure that the rights and values of the Convention on the Rights of the Child concerning privacy, personality and autonomy underpin corporate policies, management decisions and services;**

(x) **Implement the Guiding Principles on Business and Human Rights: "Protect, Respect and Remedy Framework" and the gender guidance thereon (A/HRC/41/43, annex);**[121]

(y) **Establish remedial and grievance mechanisms, while ensuring that they do not impede access to State-based mechanisms;**

(z) **Provide understandable information on reporting matters of concern, including complaints, and remedial and grievance mechanisms;**

(aa) **Take reasonable, proportionate, timely and effective measures to ensure their networks and online services are not misused for criminal or other unlawful purposes that are harmful to children;**

(bb) **Engage with law enforcement authorities to support the legal identification and prosecution of perpetrators of crimes against children.**

Future work

128. **The immediate priorities for future work on privacy and children include:**

(a) **Creating an international effort to develop frameworks for design guidance to protect children's privacy in online activities;**

(b) **Involving children, during country visits and in thematic reporting, on their privacy concerns;**

(c) **Researching parental monitoring norms and their effects on child development.**

[121] See also www.ohchr.org/Documents/Issues/Business/Gender_Booklet_Final.pdf.

Annex I

Overview of activities

The key achievements of the mandate since 2015 include:

A. Detailed thematic reports and recommendations on:

Big data and open data, A/72/540 (2017) and A/73/438 (2018)

Health-related data, A/74/277 (2019)

Privacy and gender, A/HRC/40/63 (2019)

Artificial intelligence and privacy, and children's privacy, A/HRC/46/37 (2021)

B. Security and surveillance

The establishment of the International Intelligence Oversight Forum, which met in Bucharest (2016), Brussels (2017), Valletta (2018) and London (2019).

The draft legal instrument on government-led surveillance, while not progressed, has increasingly been demonstrated as needed and a useful reference for future work.

Networks have been established through the use of working parties, consultations and involvement of regional human rights bodies/entities, particularly in Europe.

Discussions with and specific recommendations to intelligence agencies, police forces and/or Governments of Member States concerning reinforcement of safeguards and remedies, including legislation regarding surveillance, encryption and independent oversight authorities.

Intensive work on complaints of infringement of privacy by Julian Assange and President Lenin Moreno, including preparation of interim reports.

The Special Rapporteur presented a report to the Human Rights Council on governmental surveillance activities from a national and international perspective, A/HRC/34/60 (2017).

The Special Rapporteur presented a report to the General Assembly on the implications of the COVID-19 pandemic for the right to privacy, A/75/147 (2020).

Communications to Member States

Since 2015, 101 communications have been issued to Member States concerning practices that appeared inconsistent with the right to privacy. Thirty were issued in 2020 (see annex II).

Visits and events

The COVID-19 pandemic prevented any official country visits during 2020.

Country visits were undertaken in: the United States of America in 2017 (A/HRC/46/37/Add.4); France in 2018 (A/HRC/46/37/Add.2); the United Kingdom of Great Britain and Northern Ireland in 2018 (A/HRC/46/37/Add.1); Germany in 2018 (A/HRC/46/37/Add.3); Argentina in 2019 (A/HRC/46/37/Add.5) and the Republic of Korea in 2019 (A/HRC/46/37/Add.6).

During 2020, the Special Rapporteur continued to promote privacy via online events, including the forty-second International Conference of Data Protection and Privacy Commissioners and multiple civil society organization and non-governmental organization events.

Taskforces

Security and surveillance

The annual International Intelligence Oversight Forum 2020 was postponed due to the COVID-19 pandemic. However, collaborative networks were maintained. The Special Rapporteur continued to work with various countries and their intelligence agencies on the upgrading of laws regulating surveillance and encryption. More detailed laws are needed to protect encryption and thereby, the privacy of communications.

Taskforce on corporations' use of personal data

The Special Rapporteur held five taskforce meetings attended by civil society organizations and leading corporations. The dialogue was highly productive, addressing issues including identity verification, European Court judgments concerning cross border movement of data, artificial intelligence, and privacy and children.

The taskforce's recommendation on artificial intelligence is provided in the main text of the present report. The draft was provided for international consultation, to which 28 submissions were received.

Taskforce on privacy and personality: children

The Special Rapporteur worked independently yet collaboratively with the Committee on the Rights of the Child on new guidelines to protect children's privacy. He also provided feedback to the Committee on its draft general comment No. 25.

The Special Rapporteur released a call for contributions on how privacy affects the development of personality, particularly the evolving capacity of the child and the growth of autonomy. Contributions were sought from interested parties on research, consultations with children and good practice mechanisms. Nearly 60 submissions were received. The principles and recommendations are included in the main body of the present report.

Annex II

Communications on the right to privacy

Communications (joint and from the Special Rapporteur on the right to privacy alone) on the right to privacy sent, and replies received, between 1 June 2015 and 1 January 2021

TIME PERIOD: Sent and Responses Received	*TYPE of COMMUNICATION*						
	Joint Urgent Appeals	*Joint Allegation Letters*	*Joint Other Letters*	*SRP Urgent Appeals*	*SRP Allegation Letters*	*SRP Other Letters*	*Total*[a]
2015–2020 Sent	6	60	19	0	5	11	101
2015–2020 Responses	4[b]	51[c]	10[d]	0	7[d]	5	77[a]
2020 Sent	1	22	5	0	0	2	30
2020 Responses	0	16[e]	4[f]	0	0	2	22[a]

Source: OHCHR communication database, https://spcommreports.ohchr.org/TmSearch/Results.

Abbreviation: SRP, Special Rapporteur on privacy.

[a] The number of replies received is not equal to the number of matters raised, as some replies included more than one response.

[b] Two Joint Urgent Appeals received two responses each.

[c] 44 responses to Joint Allegation Letters included six matters which received two responses, and one matter received a total of three responses, making a total of 51 responses from Member States.

[d] Two replies consisted of two responses.

[e] One reply included three responses.

[f] One reply consisted of two responses.