United Nations A/73/438

General Assembly

Distr.: General
17 October 2018

Original: English

Seventy-third session
Agenda item 74 (b)
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Right to privacy*

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report prepared by the Special Rapporteur on the right to privacy, Joseph A. Cannataci, submitted in accordance with Human Rights Council resolution 28/16.

* The report was submitted after the deadline to reflect the most recent developments.

18-17254 (E) 231018

Report of the Special Rapporteur on the right to privacy

Summary

The present report is divided into two parts: a summary of activities undertaken during the period 2017–2018; and the final report on the work of the task force on big data and open data, established by the Special Rapporteur.

I. Overview of activities of the Special Rapporteur on the right to privacy

1. The period from October 2017 to October 2018 has been extremely productive for the Special Rapporteur on the right to privacy, marked by engagements with civil society, Governments, law enforcement agencies, intelligence services, data protection authorities, intelligence oversight authorities, academics, corporations and other stakeholders.

2. In March 2018, the Special Rapporteur presented to the Human Rights Council a comprehensive review of his first three-year term as the inaugural holder of the mandate created by the Council in March 2015.[1] In that report, he provided an account of his activities in each of the mandate's thematic areas. The Special Rapporteur would like to express that it is a great honour to have had his term extended until 2021 and to continue the mandate's important work.

3. The Special Rapporteur's work schedule was interrupted when he underwent surgery in April 2018. He thanks the Office of the United Nations High Commissioner for Human Rights (OHCHR) for its support and assistance during that time. The Special Rapporteur made a full recovery and resumed his duties in June 2018.

A. Work of the task force on health data privacy

4. The task force on health data privacy examined issues under the leadership of Steve Steffensen from the Dell Medical School, University of Texas, United States of America. Although work had commenced on a draft report, unanticipated events meant the consultation planned for 2018 was postponed until 2019. The Vice Chair, Nikolaus Forgo, has agreed to assume the responsibilities of Chair.

B. Work of the task force on the use by corporations of personal data

5. The right to privacy has never been more at the forefront of political, judicial or personal consciousness than it is now, as the tensions between security, corporate business models and privacy continue to take centre stage.

6. In response to events over the past year, including the breach of data by the firm Cambridge Analytica, the introduction of legislation, such as the Clarifying Lawful Overseas Use of Data Act in the United States, the 2018 bill on telecommunications and other legislation amendments in Australia, and the case of *United States v. Microsoft Corp*. before the United States Supreme Court, the Special Rapporteur

[1] A/HRC/37/62.

brought forward the commencement of the task force on the use by corporations of personal data.

7. The task force met for the first time in Malta in September 2018. Its membership is drawn from large corporations leading the digital era and key players promoting the protection of the right to privacy in the technology world. It will advise the Special Rapporteur on the emerging challenges to and the opportunities for the promotion of the right to privacy, including the gender impacts of those issues.

C. Work of the task force on better understanding privacy

8. The task force on better understanding privacy explores the recognition by the Human Rights Council of the right to privacy as enabling the development of the person, and the barriers to that enablement. It will collaborate with initiatives around the world, such as that of the Australian Human Rights Commission's examination of the impact of the digital era on human rights.[2]

9. While all persons are entitled to enjoy the protection provided by international human rights law, there have been reports that the enjoyment of the right to privacy is neither equal nor universal. Gender is one area where the protective and facilitative effects of privacy and privacy breaches and harms can be experienced differently.

10. In that respect, the Supreme Court of India repealed section 377 of the Indian Penal Code, which had criminalized consensual sexual activity between adults, in a judgment that recognized the rights of the lesbian, gay, bisexual, transgender, questioning and intersex community in India. That judgment will have a significant impact on the gender and privacy discourse in India, and flows from the 2017 judgment on the right to privacy in the Puttaswamy case.[3]

11. The Special Rapporteur has initiated an online consultation on gender perspectives of the right to privacy in the digital era, seeking feedback on questions such as:

(a) What gender issues arise in the digital era? What challenges need to be addressed and what positive experiences can be promoted more widely?

(b) Has the digital era produced new or significantly different gender-based experiences of privacy (including experience inclusive of sexual orientation, gender identity, gender expression and sex characteristics)? If so, what are these?

(c) What are the gendered impacts of privacy invasions on women and men, and individuals of diverse sexual orientations and gender identities, gender expressions and sex characteristics, arising from violations of the right to privacy, including health issues, discrimination in employment, or other areas?

(d) What are good practices in law and service delivery models that address gender-based differences in the enjoyment of the right to privacy?

12. Submissions were requested by 30 September 2018 for reporting to the Human Rights Council in 2019. The Special Rapporteur is happy to accept Member States' late submissions until 30 November 2018.

13. This initiative follows the consultations around the world on the theme: "Privacy, personality and flows of information" of July 2016, May 2017 and

[2] Australian Human Rights Commission, "Major project to focus on human rights and technology," 22 May 2018. Available at www.humanrights.gov.au/news/stories/major-project-focus-human-rights-and-technology.

[3] Communication from Smitha Krishna Prasad, National Law University, Delhi, India, 24 September 2018.

September 2017. The fourth event, on gender aspects, which had been scheduled to be held in May 2018 in Latin America, was postponed owing to the Special Rapporteur's inability to travel and will instead be held in mid-2019.

D. Work of the task force on security and surveillance

14. After Edward Snowden revealed details of surveillance and intelligence-sharing programmes operated by the intelligence services of the United States and the United Kingdom of Great Britain and Northern Ireland, applications were lodged with the European Court of Human Rights concerning the bulk interception of communications, intelligence-sharing with foreign Governments and the obtaining of communications data from communications service providers under the United Kingdom Regulation of Investigatory Powers Act 2000.

15. The Court recently found that the bulk interception regime of the United Kingdom had violated article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights), on the right to respect for private and family life/communications, due to insufficient oversight of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, and inadequate safeguards for selection of "related communications data" for examination.

16. The Court held that the regime for obtaining communications data from communications service providers had violated article 8; and that the regimes for bulk interception and for obtaining communications data from communications service providers had violated article 10 of the Convention owing to insufficient safeguards for confidential journalistic material. It further found that the regime for sharing intelligence with foreign Governments had not violated either article 8 or article 10.[4]

17. While that judgment concerned the earlier statutory surveillance framework of the United Kingdom, its findings are significant and are brought to the attention of Member States for the review of their practices and frameworks.

18. In relation to the December 2016 ruling of the Court of Justice of the European Union regarding the retention of communications data, and the consultation by the Government of the United Kingdom on its proposed response, the Special Rapporteur provided input in early 2018, which will be available on the OHCHR webpage dedicated to the mandate holder.[5]

19. In September 2018, the Government of Australia tabled the telecommunications and other legislation amendments bill, which has profound impacts on human rights and cybersecurity internationally and domestically.

20. The bill is fatally flawed. It is a poorly conceived national security measure that is as likely as not to endanger security; it is technologically questionable if it can achieve its aims and avoid introducing vulnerabilities into the cybersecurity of all devices irrespective of whether they are mobile telephones, tablet computers, smart watches, cars or closed-circuit television networks, and it unduly undermines human rights, including the right to privacy. Assurances that it is not a "back door" into encrypted communications are unreliable since it may create, in effect, additional keys to the "front door", or even more front doors.

[4] European Court of Human Rights, First Section, *Big Brother Watch and Others v. the United Kingdom*, Applications Nos. 58170/13, 62322/14 and 24960/15, Information Note on Judgment of 13 September 2018. Available at https://hudoc.echr.coe.int/eng#{"itemid":["002-12080"]}.

[5] www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

21. The bill has an overly high level of discretion on the use of exceptional powers. Accountability does not lie with Parliament but with agencies and the Attorney General. It lacks judicial oversight or independent monitoring, there is an extremely troubling lack of transparency, and the proposed ability to introduce software among other actions into devices is disturbingly akin to government hacking. It was introduced into Parliament after an inadequate period of consultation and, despite receiving reportedly more than 14,000 submissions, just two weeks after consultation closed.[6]

22. The Special Rapporteur's concerns are compounded by the stance of the Government of Australia on remedy for serious invasions of privacy and the country's limited human rights and privacy protections — that is, no constitutional protection for privacy; no bill of rights enshrining privacy; no tort of privacy; and, unlike its neighbour New Zealand, its Privacy Act has failed the European adequacy assessment.

23. A new approach is required to address the challenges posed by encryption for law enforcement and national security. While technology poses challenges to law enforcement and intelligence services, and it is important to counter online child sexual abuse and negate terrorism threats, protecting the human rights of citizens is also legitimate and necessary in a democratic society. The technologies that empower criminals and terrorists to evade detection or launch malicious attacks also provide enormous benefits for cybersecurity, privacy and the economy.[7] Weakening encryption technology puts at risk the modern information economy's security.[8]

24. Addressing the complications caused for law enforcement investigations and intelligence collection by encryption requires an approach that avoids weakening encryption and hence the national security of other countries.

25. I recommend to Member States the approach of the Government of the Netherlands, which has recognized that national action cannot be seen separately from its international context and the lack of options for weakening encryption products without compromising the security of digital systems that use encryption.[9]

26. The Special Rapporteur's international intelligence oversight forum will meet in Malta late in November 2018. Interest is such that the forum is oversubscribed.

E. Communications

27. The Special Rapporteur has submitted 17 communications since 22 September 2017, including 8 "allegation letters", 7 "other letters" and 2 "urgent appeals". Of the 17 communications, 15 were submitted jointly with other special procedure mandate holders and two communications were submitted by the Special Rapporteur alone.

---

[6] Justin Hendry, "Decryption laws enter parliament", IT News, 20 September 2018. Available at www.itnews.com.au/news/decryption-laws-enter-parliament-512867?eid=1&edate=20180921&utm_source=20180921_AM&utm_medium=newsletter&utm_campaign=daily_newsletter.

[7] James A. Lewis, Denise E. Zheng and William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (Washington, D.C., Center for Strategic and International Studies, 2017). Available at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE.

[8] New America, "Coalition raises serious concerns about Australian draft bill and encryption backdoors", press release, 10 September 2018; Michelle Mosey and Adam Henschke, "Defining thresholds in law — sophisticated decryption and law enforcement", National Security College Policy Options Paper, No. 8 (Australian National University, April 2018).

[9] G.A. Van der Steur, Minister of Security and Justice, and H.G.J. Kamp, Minister of Economic Affairs, The Netherlands, "Cabinets view on encryption", position letter provided to the President of the House of Representatives of the States General, 4 January 2016.

F. Promoting the right to privacy

28. The Special Rapporteur cooperated with other special procedure mandate holders through joint press releases and statements and by exchanging advice and information. The Special Rapporteur acknowledges the constructive consultations with the Special Rapporteur on violence against women, its causes and consequences.

29. The Special Rapporteur has issued 11 press releases and statements. Of those, two were released jointly with other mandate holders: one on the rights of environmental activists in the upcoming 24th session of the Conference of the Parties to the United Nations Framework Convention on Climate Change;[10] and the other on the draft security law of Mexico.[11]

30. On 19 and 20 February 2018, the Special Rapporteur gave a presentation on the role of the right to privacy within the human rights framework and for civic space protection and moderated a session on new and emerging trends at the expert workshop on the right to privacy in the digital age, organized in Geneva by OHCHR.

G. Country visits

31. In June 2018, the Special Rapporteur visited the United Kingdom. In his end-of-mission statement, he provided preliminary observations.[12] The final report will be submitted to the Human Rights Council at its fortieth session.

32. In 2015, the Special Rapporteur had been critical of the legislative proposals that had increased the surveillance powers of the Government of the United Kingdom. Significant improvements had been made since then on the intelligence oversight regime, including the establishment of a better-resourced Investigatory Powers Commissioner's Office and the double-lock system, with the equivalent of five full-time judicial commissioners reviewing the most sensitive authorization decisions signed-off by senior government officials, such as the Home Secretary and the Foreign Secretary. One positive aspect is that those safeguards against arbitrary or unlawful surveillance apply equally to all persons under surveillance by the United Kingdom authorities in its territory, without any distinction based on nationality or residence.

33. The Special Rapporteur remains concerned about possible deficiencies in the new Investigatory Powers Act 2016, including the requirement that the Investigatory Powers Commissioner's Office perform the dual task of authorizing surveillance and overseeing that same surveillance. This may compromise the independence of the post-facto oversight.

34. The Special Rapporteur identified a need for clear, strong guidelines and oversight of any data-sharing agreement for the National Health Service, and strongly recommended that those guidelines be made public at the earliest opportunity. Discussions with the National Data Guardian suggest this could be during the next 12–24 months. The Special Rapporteur recommended that the role of the Data Guardian be made statutory as soon as possible.

[10] Office of the United Nations High Commissioner for Human Rights (OHCHR), "UN experts urge Poland to ensure free and full participation at climate talks", 7 May 2018. Available at www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23042&LangID=E.

[11] OHCHR, "Mexico draft security law threatens rights and should be rejected, UN rights experts warn", 14 December 2017. Available at www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=22535&LangID=E.

[12] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E.

35. Other issues in his end-of-mission statement include anti-radicalization measures and “Prevent” programme and their impact on Muslims; proposals to criminalize access to extremist material; and matters raised by civil society organizations.

Planned country visits

36. The next official country visit is to Germany from 29 October to 9 November 2018, preceded by a call for contributions from interested parties on the OHCHR webpage dedicated to the mandate holder.

Informal visits and international events

37. While visiting Australia for the consultation on big data and open data, the Special Rapporteur visited three states and met with civil society organizations, a government minister and the Shadow Attorney General, government officials, representatives of corporations and professional associations, academics and other individuals. He also met with the Australian Human Rights Commissioner and Commission President and gave public lectures at the University of New South Wales, Sydney; Melbourne University; La Trobe University; and Edith Cowan University. The Optus Macquarie University Cybersecurity Hub held a briefing between the Special Rapporteur and top-listed companies. The Australia and New Zealand section of the International Association of Privacy Professionals organized meetings with privacy practitioners.

38. The Special Rapporteur also participated in the sixteenth International Conference on Cyberspace, held in Czechia in November 2017; the eleventh International Conference on Computers, Privacy and Data Protection, held in Brussels in January 2018; an expert workshop on the right to privacy in the digital age, held in Geneva in February 2018; the Global Internet and Jurisdiction Conference, held in Ottawa in February 2018; and the MAPPING Conference, held in Malta in February 2018.

H. Developments on the right to privacy

Ability to seek remedy

39. The Special Rapporteur continued to draw the attention of relevant Member States to allegations of violations of the right to privacy and, in his 2018 report, advised the Human Rights Council on violations of article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights.

40. The Special Rapporteur remains convinced that repairing the harm caused by breaches of privacy requires confidence in receiving a fair hearing and possible remedy. The ability to have access to remedy is central to the protection of human rights and remains high on the Special Rapporteur’s priorities.

Artificial intelligence

41. As more of the decisions affecting the lives of all individuals are made using algorithms and machine learning, their impact on human rights needs to be carefully and continuously evaluated.

42. These technologies are so pervasive they are even relied upon as evidence in court proceedings. Yet the way in which complex algorithms operate is largely unknown, as is their developmental progression in the case of machine learning. An examination of this from the perspective of all human rights is necessary prior to, or

in tandem with, policies that encourage and enable the development and deployment of products based on artificial intelligence.[13] Strong legal and ethical frameworks are critical to protect affected human rights.

Introduction of privacy and data protection legislation globally

43. There has been a great increase in the number of countries that have introduced privacy or data protection laws;[14] 2018 has been a particularly active year around the world in that respect.

44. Of particular note is the draft law of India following the Puttaswamy decision of the Supreme Court.[15] The draft bill, released in mid-2018, has many positive features also found in the European Union General Data Protection Regulation 2016/679, such as data protection impact assessments, a right to be forgotten and adequate enforcement penalties. But there are also concerns, such as restrictions on research into the potential re-identification of people in supposedly anonymized data sets. Furthermore, while the use of personal data by law enforcement is to be "necessary and proportionate", disclosure in legal proceedings has broad exemptions.[16] The Special Rapporteur urges the Government of India to engage with the academics, researchers and civil society organizations that raise such issues.

45. In a judgment dated 26 September 2018, the Supreme Court of India upheld the constitutional validity of the Aadhar Act, but revoked: (a) section 57, whereby private companies could ask consumers for details using the Aadhaar programme for identification purposes; (b) section 33 (2), on sharing data with security agencies on the grounds of national security; and (c) section 47, whereby only the Government is able to lodge a complaint in case of theft of Aadhaar data.[17] The Court required the Government to introduce robust data protection legislation.

46. Within the European Union, there has been significant reform. The General Data Protection Regulation came into force 25 May 2018, and a specific directive on data protection in police and justice areas became applicable from 6 May 2018. The Directive on Privacy and Electronic Communications 2002/58/EC is due to be replaced by the new ePrivacy Regulation.[18] Regulation (EC) 45/2001 lays down the rules for data protection in European Union institutions and the duties of the European Data Protection Supervisor. The European Commission adopted a proposal on 10 January 2017 that repealed that Regulation and aligned it with the General Data

[13] Priyanar Bhunia, "Taskforce recommends establishment of national mission for coordinating Al-related activities across India", Open Gov, 9 April 2018.

[14] Graham Greenleaf, "Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey — 145 privacy laws and business international report 10, 2017", University of New South Wales Law Research Series, No. 45 (2017).

[15] Supreme Court of India, Civil Original Jurisdiction, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others*, Writ Petition (Civil) No. 494 of 2012, Judgment, 24 August 2017. Available at http://supremecourtofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf.

[16] Richard Chirgwin, "India mulls ban on probes into anonymized data use — with GDPR-style privacy laws", The Register, 31 July 2018. Available at www.theregister.co.uk/2018/07/31/india_privacy_boffin_ban/.

[17] Supreme Court of India, Civil Original Jurisdiction, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others*; Economic Times, "This is what the Supreme Court did not like about Aadhaar", 26 September 2018. Available at http://economictimes.indiatimes.com/articleshow/65961697.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[18] See European Commission, "Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and protection of personal data in electronic communications repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", 10 January 2017.

Protection Regulation; both measures are expected to apply from late in 2018. With that reform, the European Union will complete the first major modernization of its framework for protecting privacy and data protection in over 20 years.[19]

47. These important consolidation measures within the European Union apply to all sectors, except to privacy and "national security" — a matter excluded from the European Union's competence by article 4.2 of the Treaty on European Union. Surveillance within the remit of national security, and not law enforcement, is regulated in a much more disparate manner within the European Union through the efforts of countries like Belgium, France, the Netherlands and the United Kingdom to update their legislation.

48. At the wider regional level, it is encouraging to note that the Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (also referred to as the "Modernized Convention 108"), was finalized in June 2018, and its enabling legal instrument (Protocol CETS 223) was opened for signature on 10 October 2018. This is an important milestone as, unlike the General Data Protection Regulation, the Convention also covers national security and has been ratified by more than 55 States Members of the United Nations, with an increasing number of non-European States also joining.

49. In Brazil, the Senate approved a general data protection law that will become effective in February 2020. Key elements include:[20] cross-border jurisdiction; privacy principles and a risk-based approach; new rights for individuals; more legal bases for processing personal data; data-mapping and data-protection impact assessments; mandatory breach notification and a data protection officer; and restrictions to the cross-border transfer of personal data.

50. Fines for non-compliance can be up to 2 per cent of the gross sales of the company or group of companies, or a maximum sum, per infringement, of approximately $12.9 million.

Indigenous peoples and data

51. The Special Rapporteur has studied the privacy culture of Aboriginal Australians for many years. Given that this culture is one of the most sophisticated, lived expressions of privacy at the individual, familial and group level, implemented through behaviours, rites and practices, such as private and communal spaces, the Special Rapporteur was pleased that the consultation on big data and open data explored indigenous data sovereignty, albeit in a modest fashion.

52. The Special Rapporteur encourages Governments and corporations to recognize the inherent sovereignty of indigenous peoples with respect to data about them or collected from them, and which pertain to indigenous peoples' knowledge systems, customs or territories.

II. Consultation on the previous report of the Special Rapporteur to the General Assembly

53. In his October 2017 report to the General Assembly (A/72/540), the Special Rapporteur reviewed the challenges to ensuring the human right to privacy in the context of one of the defining features of the digital era: big data and open data. Since

[19] See https://edps.europa.eu/data-protection/data-protection/legislation_en.
[20] See www.onetrust.com/what-is-the-brazil-general-data-protection-law-lgpd/.

then, the General Data Protection Regulation was introduced and the revelations concerning Facebook and Cambridge Analytica occurred.

54. Consultations with government officials, civil society organizations, companies and individuals on that report were held in Australia on 26 and 27 July 2018. They were preceded by a call for submissions that concluded on 28 April 2018 and were summarized for the consultation. Further inputs came from meetings with civil society organizations organized by the Australian Privacy Foundation and from submissions received after the consultation.

A. Summary of feedback

55. The public consultation considered the origins and uses of big data and open data; the potential benefits and harms of each; the impact of the use of personal data on other human rights; the adequacy of de-identification techniques; good practices on the use of personal data; the importance of human rights and ethics in automated decision-making technologies; indigenous data sovereignty; consumer and gender issues; and the perspectives of non-European countries.[21] Much of the discussions concerned open data and the privacy consequences of its interaction with big data.

B. Open data

56. Big data analysis and computational techniques based on artificial intelligence provide benefits while raising potential privacy risks for individuals and communities, as well as for the fabric of democratic societies. The opening-up of government information, particularly the iterative public release of data sets containing personal information, requires a more nuanced and closer examination.[22]

57. The consultation examined the proposition that big data analytics can identify individuals despite de-identification.[23] Participants heard how identifying whether data or the results of a data analytics project contain personal information is dependent on the circumstances of the use or disclosure, and how that can change depending on other factors. Consequently, re-identification is best described in terms of risk levels rather than as an absolute. Risk levels are based on who has access to the data, how granular the data is (the size of the smallest group in the data), what other data sets can be accurately linked to the data and the associated external context.

58. “Personal information” within data covers a wide field and descriptions vary in different jurisdictions. What most definitions have in common is that the scope of personal information can be broad and looks at the ability to identify an individual, not just whether the data itself identifies the individual.

59. Two key aspects for identifying data that contains personal information are either: (a) the data itself must identify an individual; or (b) it must be reasonably possible to identify an individual.

[21] Amanda Lo, “The right to privacy in the age of big data and open data”, The Allens Hub for Technology, Law and Innovation, University of New South Wales, 21 August 2018.

[22] Submission from M. Paterson, Monash University, August 2018.

[23] See Office of the Victorian Information Commissioner, “Protecting unit-record level personal information: the limitations of de-identification and the implications for the Privacy and Data Protection Act 2014”, May 2018. Available at https://ovic.vic.gov.au/resource/protecting-unit-record-level-personal-information/.

60. The three main mechanisms for data-sharing — explicit, derived and inferred — each come with considerations about the degree of personal information contained and the obligations of the organization that captures, uses and stores that data.

61. Online browsing and purchasing data can be used to personalize services increasingly without knowing the identity of the user. However, concerns have been raised as to whether highly targeted anonymous identifiers constitute personal information. Mobile network data has been used for purposes beyond network optimization, allowing customer churn prediction and even to reveal relationships to other mobile users without knowing the identity of the individuals involved.[24]

62. A key challenge for sharing data is that there is currently no way to determine unambiguously if there is personal information within aggregated data or whether disaggregated data can be re-aggregated. The risk of re-identification depends on access to (and the ability to link) related data sets, the techniques used to de-identify and the level of aggregation or perturbation of data. Consequently, different techniques and levels of aggregation of data are used across organizations depending on the perceived risk associated with the data being shared.

63. The development of standards to determine what constitutes "de-identified" data would help in addressing the challenges of dealing with privacy. Internationally, there is currently only very high-level guidance, and certainly nothing quantitative, as to what "de-identified" means, hence many organizations must determine what it means to them on a case-by-case basis, based on different data sets and on how they can reasonably be used or combined with other data.

64. In 2017, the Australian Computer Society released a technical white paper in which it explored the challenges of data-sharing and highlighted that a fundamental challenge for the creation of smart services is the issue of whether a set of data sets contains personal information. Answering that question is a major challenge as the act of combining data sets creates information. The paper further proposed a modified version of the "five safes" framework for data-sharing to quantify different thresholds for "safe". That work continues with the support of Standards Australia and aims to initiate work to create international standards on preserving privacy and data-sharing. A second white paper is planned for October 2018, which is expected to form the basis of international standardization activities with the goal of ultimately defining robust frameworks on preserving privacy and data-sharing.[25]

65. An example of the limitations of de-identification for protecting unit record-level records was the release online in August 2016 of a large longitudinal data set for a 10 per cent sample of Australians who had claimed Medicare benefits since 1984, or pharmaceutical benefits since 2003.[26] This affected the medical data of around 2.9 million Australians, including prescriptions, surgery episodes, tests (excluding results), and visits to general practitioners and specialists (excluding

[24] Submission from Ian Opperman, Data Analytics Centre, Government of New South Wales, Australia, 31 August 2018.

[25] Ibid., including Australian Computer Society, *Data Sharing Frameworks*, Technical White Paper (Sydney, 2017). Available at www.acs.org.au/content/dam/acs/acs-publications/ACS_Data-Sharing-Frameworks_FINAL_FA_SINGLE_LR.pdf.

[26] Submission of Vanessa Teague to the Special Rapporteur during the "Big data-open data" consultations, 26 and 27 July 2018, University of New South Wales, Sydney, Australia. See also Office of the Australian Information Commissioner, "Publication of MBS/PBS data", Commissioner-initiated investigation report, 20 March 2018, pp. 7–9. Available at www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/0publication-of-mbs-pbs-data.pdf.

doctors' notes).[27] The data set had been downloaded 1,500 times before being taken offline following reports that doctors' identifications could easily be decrypted[28] and, later, that patients could be identified.[29] The release by the Australian Department of Health sought to facilitate medical research.

66. The important questions that such examples raise include whether government-held personal information data sets should be released externally when there are increasing risks of large-scale privacy breaches from re-identification, owing in part to the availability of other publicly released information, and inadequate organizational technological capabilities; and what an appropriate response would be to prevent such incidents from re-occurring.

67. From the information gathered at the consultation, it was clear that the release of government-held information requires adequate privacy protections and regulatory responses. There were strong views that unrestricted access to unit record-level data, as well as other personal data unable to be disclosed safely in aggregate form, is incompatible with the right to privacy. Feedback was unsupportive of regulatory responses reliant upon the criminalization of re-identification undertaken to test the security of released data sets.[30]

68. Participants described existing mechanisms that permit the use of identifiable personal data for research purposes,[31] pointing out that these could be expanded, as appropriate, for further public interest uses.[32]

69. The question would appear to be whether we would have more sustainable practices if useful data were viewed as a limited resource, rather than as an unlimited untapped resource.[33]

70. Current practices that alienate the data subject have been described metaphorically as "killing the goose that laid the golden egg", as distrust of the ability of government or private actors to manage personal information appropriately results in people either not using services — which in turn presents the risk of adverse societal impacts, for example, in public health areas — or providing incomplete or

[27] Vanessa Teague, Chris Culnane and Ben Rubinstein, "The simple process of re-identifying patients in public health records", University of Melbourne, Pursuit, 18 December 2017. Available at https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records.

[28] Chris Culnane, Benjamin Rubinstein and Vanessa Teague, "Health data in an open world", report on re-identifying patients in the MBS/PBS dataset and the implications for future releases of Australian Government data, University of Melbourne, 18 December 2017. Available at https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf.

[29] The Office of the Australian Information Commissioner found doctors were identifiable, and that patients could also be identified but not "reasonably identifiable" in the terms of the Australian Privacy Act. It is understood affected people have not been notified.

[30] Submissions from, inter alia, M. Paterson.

[31] These mechanisms are commonly subject to oversight by ethics committees with access restricted to researchers under confidentiality obligations.

[32] For example, based on mechanisms such as the Five Safes Framework: see Australian Bureau of Statistics, "Managing the risk of disclosure: the five safes framework", Confidentiality Series, part 3, August 2017. Available at www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=S.

[33] Submission from Theresa Dirndorfer Anderson, University of Technology, Sydney, Australia.

inaccurate information.[34] These actions also undermine data quality and, ultimately, the accuracy of machine-learning algorithms.

71. The overwhelming view at the consultation was that the sustainability of data practices increases if data subjects are fully fledged partners in data operations.[35] Participants heard that nowhere is this more evident and important than for indigenous peoples.

C. Indigenous data sovereignty

72. Data is a cultural, strategic and economic resource for indigenous peoples. Yet indigenous peoples remain largely alienated from the collection, use and application of data about them, their lands and cultures.[36] Existing data and data infrastructure fail to recognize or privilege indigenous knowledge and worldviews and do not meet indigenous peoples' current and future data needs. Current practices around big data and open data, whether under the auspices of Governments or corporations, will likely move indigenous peoples' data interests even further away from where decisions affecting indigenous peoples' data are made.

73. Indigenous data sovereignty is a global movement concerned with the rights of indigenous peoples to own, control, have access to and possess data that derives from them and which pertains to their members, knowledge systems, customs or territories.[37] It is supported by indigenous peoples' rights to self-determination and governance over their land, resources and culture, as described in the United Nations Declaration on the Rights of Indigenous Peoples. Implicit in indigenous data sovereignty is the desire for data to be used in ways that support and enhance the collective well-being of indigenous peoples.

74. Indigenous data sovereignty has a place as an underpinning principle in governance arrangements related to big data and open data. It is practised through indigenous data governance that comprises principles, structures, accountability mechanisms, policy relating to data governance, privacy and security, and legal instruments. Indigenous data sovereignty frameworks can be applied to internally controlled and owned nation/tribal data, as well as data that is stored or managed externally. The indigenous data sovereignty networks in Australia and New Zealand are developing protocols around indigenous data governance.[38]

[34] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey, 2017* (Canberra, 2017). Available at www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017; Australia, Office of the Australian Information Commissioner, *Community Attitudes to Privacy Survey: Research Report 2013* (Canberra, 2013). Available at www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf.

[35] Submission from Theresa Dirndorfer Anderson.

[36] Tahu Kukutai and Maggie Walter, "Recognition and indigenizing official statistics: reflections from Aotearoa New Zealand and Australia", *Statistical Journal of the IAOS*, vol. 31, No. 2 (2015).

[37] Tahu Kukutai and John Taylor, "Data sovereignty for indigenous peoples: current practice and future needs" and C. Matthew Snipp, "What does data sovereignty imply: what does it look like?", both in Kukutai and Taylor (eds), *Indigenous Data Sovereignty: Towards an Agenda*, Research Monograph, 2016/38 (Canberra, Australian University Press, 2016). Available at https://press.anu.edu.au/publications/series/centre-aboriginal-economic-policy-research-caepr/indigenous-data-sovereignty.

[38] Submission from Maggie Walter, University of Tasmania, Australia.

75. Indigenous data sovereignty illustrates that good practices concerning big data and open data require an awareness of data that is missing, underrepresented or misrepresented,[39] and of the interests served, or not, by such practices.

D. Gender issues

76. The consultation heard that privacy can be experienced differently by persons of different gender or gender identity.

77. Privacy is a heightened concern for lesbian, gay, bisexual, transgender, questioning and intersex persons, for example, and can also be essential for the safety of those, usually women, fleeing domestic, familial or religious violence.

78. While inclusive data-collection practices communicate acceptance and respect, intrusive collection can be a significant barrier to gaining access to services, as the lesbian, gay, bisexual, transgender, questioning and intersex communities and others have justified concerns for privacy following experiences of discrimination, stigma and targeted violence.

79. This issue will be explored in greater depth by the task force on privacy and personality. However, in terms of big data and open data, good practices require the review of how data is collected, with an awareness of the possible impacts of poor privacy practices and differing consequences on people of different gender or gender identity.

E. Consumer rights and personal data collection and use

80. In data-driven consumer markets, the use of more and more data for developing, selling and promoting consumer products has meant that many data protection issues also become consumer issues, and vice versa. The distinction between consumer law and data protection law is now less sharply defined.[40]

81. The use of consumers' personal data by financial services and other sectors has given rise to concerns at both the public policy and individual levels.[41] The fair processing of personal data is increasingly part of the reasonable expectations of consumers regarding the services and products they utilize.[42]

82. The consultation compared the approaches of consumer law and privacy/data protection law, noting that some countries are introducing consumer privacy initiatives.

83. Following the Cambridge Analytica scandal, in June 2018 the state of California in the United States enacted the Consumer Privacy Act, to take effect in January 2020, to protect the data privacy of technology users and others by imposing new rules on

[39] Submission from Theresa Dirndorfer Anderson.

[40] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, "The perfect match? A closer look at the relationship between EU consumer law and data protection law", *Common Market Law Review*, vol. 54 (2017).

[41] Lee Rainie and Maeve Duggan, "Privacy and information sharing", 14 January 2016 (people's comfort level depends on perception of trustworthiness, what happens post collection, and retention length). Phuong Nguyen and Lauren Solomon, *Consumer Data and the Digital Economy — Emerging Issues in Data Collection, Use and Sharing* (Consumer Policy Research Centre, 2018) (found consumers wanted more options over what data is collected, its use, and the Government to participate in improving consumer control over data and protections from data misuse).

[42] Helberger, Zuiderveen Borgesius and Reyna, "The perfect match?".

companies that gather, use and share personal data.[43] The Act creates four basic rights for individuals: the right to know what personal information a business has about them and where that personal information came from or was sent; the right to delete personal information that a business collected from them; the right to opt-out of the sale of personal information about them; and the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the act.[44] The Act also creates a limited right for consumers to sue businesses for data security breaches, based on California's existing data breach notification law.

84. However, it has been reported that the rights enshrined in the Act need to be strengthened, for the following reasons:

(a) The term "business" is narrowly defined.[45] In the digital era, small technology players and individuals can also undermine privacy in a myriad of ways by not having the knowledge, skills or resources to implement adequate data protection;[46]

(b) Businesses can still charge a higher price to users exercising their privacy rights;

(c) Users cannot easily bring violators to court owing to narrow exceptions;

(d) User consent is only required for data sale not collection, and users need to opt out of consenting to the sale of data;

(e) The "right to know" does not provide specific sources and recipients, and the "right to deletion" is for information collected from them, and not for information held about them;

(f) Most enforcement responsibility rests with the California Attorney General rather than an independent entity.

85. Under European Union data-protection law, aspects of the General Data Protection Regulation provide for new protections for consumers within the European Union, including greater transparency and control of data being collected about them by companies than may be provided by the European Union consumer protection directives.[47]

86. Australia is establishing a "consumer data right" — a data portability right[48] that falls short of the wider protections provided under privacy or data protection laws for Australian consumers whose data is being collected, shared and used on a daily basis.[49] The consultation heard that this data portability right, rather than protecting consumers' data, could potentially expose it to greater use by third parties.[50]

[43] See https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[44] Adam Schwartz, Lee Tien and Corynne McSherry, "How to improve the California Consumer Privacy Act of 2018", Electronic Frontier Foundation, 8 August 2018.

[45] Ibid., "the Act defines a "business" as a for-profit legal entity with: (i) annual gross revenue of $25 million; (ii) annual receipt or disclosure of the personal information of 50,000 consumers, households, or devices; or (iii) receipt of 50 per cent or more of its annual revenue from selling personal information (Section 140(c))".

[46] Submission from Roland Wen, University of New South Wales, Sydney, Australia.

[47] Helberger, Zuiderveen Borgesius and Reyna, "The perfect match?".

[48] Australian Competition and Consumer Commission, "Consumers' right to their own data is on its way", press release, 16 July 2018. Available at www.accc.gov.au/media-release/consumers-right-to-their-own-data-is-on-its-way.

[49] Nguyen and Solomon, *Consumer Data and the Digital Economy*.

[50] Submission of Katherine Kemp to the Special Rapporteur during the consultations on big data and open data, 26 and 27 July 2018, University of New South Wales, Sydney Australia.

87. There is an advantage in establishing a strong connection between consumer law and privacy law, for example, in co-coordinated legal action.[51] Consumer law can be a useful tool to safeguard the overall balance in the commercial relationship between consumers and suppliers and can be used to assess the fairness of situations in which companies require consumers to consent to the processing of disproportionate amounts of data, and/or to the sharing of data with third parties.

88. Feedback received on practical measures to help entities improve their trusting relationship with users included communicating the terms of data use through standard licences akin to the six standardized Creative Commons licences. This was seen as a potential means of alleviating some of the challenges of complex privacy policies, while simplifying and standardizing communication to users in different countries.[52] Draft licence types could be backed by more detailed "standard conditions" privacy policies.

89. Capturing privacy risks by using privacy rating labels could make privacy choices more accessible to consumers and increase the transparency and disclosure of privacy risks by data controllers.[53]

F. Artificial intelligence

90. Machine learning and artificial intelligence use enormous quantities of data and, in turn, create more data. The combination of data availability, computing power and analytic capabilities using sophisticated algorithms, coupled with machine learning and artificial intelligence, has the potential to revolutionize societies positively, but could also profoundly change our world and our chances of survival, and not necessarily for the better.[54]

91. The latter outcome could occur through the potential negative impact of artificial intelligence on human rights, including the right to privacy. Artificial intelligence methods can be and are being used to identify people who wish to remain anonymous; to enable the microtargeting of messaging; to generate sensitive information about people from non-sensitive data; to profile people based on population-scale data; and to make decisions using that data, thereby profoundly affecting people's lives.[55]

92. As more and more actions and decisions are transferred to machines, there is an urgency in ensuring that machine-learning and algorithms are transparent as to their logic and their assumptions. The algorithms used in machine-learning and artificial intelligence are increasingly complex, and transparency will be difficult to achieve. Yet that complexity should not prevent auditing to ascertain lawfulness.[56] Currently, the use of big data-related technologies is not being held sufficiently to account as to its compliance with international human rights law, data protection regulations,

[51] United States and European Union consumer groups have jointly asked consumer agencies and data protection authorities to look at data protection and consumer law infringements of connected toys. See Helberger, Zuiderveen Borgesius and Reyna, "The perfect match?".

[52] Submission from the Allens Hub for Technology, Law and Innovation, 14 August 2018.

[53] See Lorrie Faith Cranor, "Necessary but not sufficient: standardized mechanisms for privacy notice and choice", *Journal on Telecommunications and High Technology Law*, vol. 10, iss. 2 (Summer 2012).

[54] Toby Walsh, 2062: *The World that AI Made*, (Carlton, Victoria, Australia, La Trobe University Press, 2018).

[55] Privacy International and Article 19, "Privacy and freedom of expression in the age of artificial intelligence", April 2018.

[56] European Union Agency for Fundamental Rights, *#BigData: Discrimination in Data Supported Decision Making* (Luxembourg, European Union Publications Office, 2018).

sectoral privacy regulations, ethical codes or industry standards.[57] It has been argued that machines should be held to higher ethical standards than humans and that, with the right choices, privacy will not be a historical anomaly, but instead a technologically given right.[58]

93. The General Data Protection Regulation limits the use of automated decision-making in certain circumstances and requires individuals to be provided with information as to the existence of automated decision-making, the logic involved and the significance and envisaged consequences for the individual of the processing of that data.[59] There is an overall prohibition, with narrow exceptions, of decisions made solely by automated processes when such decisions have legal or other significant effects.

94. The Regulation defines profiling as the automated processing of data to analyse or make predictions about individuals and sets an obligation to incorporate data protection by design and by default. Data privacy impact assessments will be mandatory for many privacy-invasive artificial intelligence and machine learning applications that fall within the scope of data protection law and have substantial anticipated risks, such as the processing of sensitive data. In the case of artificial intelligence, a data privacy impact assessment could — perhaps should — enable entities to model the effects of their algorithms in much the same way that climate scientists model climate change or weather patterns.[60]

95. The European Union Agency for Fundamental Rights has suggested that one way to ensure effective accountability could entail establishing dedicated bodies with an exclusive mandate to provide oversight of big data-related technologies, similar to the role of data protection authorities.[61]

96. While the means still need to be determined, it is relevant that new technologies have required the strengthening of international humanitarian law throughout the twentieth century.[62]

G. Principles for big data and open data

97. In his October 2017 report, the Special Rapporteur raised the development of principles for regulating big data and open data. The consultation indicated that any such development should, as far as possible, draw from international agreements on data protection regarded as representing “best practice”. At present, these are the General Data Protection Regulation and the Modernized Convention 108, the latter of which originated at the Council of Europe but is open to accession globally by States that have enacted consistent principles.[63]

98. The influence of the General Data Protection Regulation is not exerted only through local legislative enactments or its extraterritorial application. Companies

[57] Lee Rainie and Janna Anderson, *Code-Dependant: Pros and Cons of the Algorithm Age* (Pew Research Center, 2017).

[58] Walsh, 2062: *The World that AI Made*.

[59] European Union General Data Protection Regulation 2016/679 of 27 April 2016, articles 13, 14 and 22.

[60] Andrew Smith, “Franken-algorithms: the deadly consequences of unpredictable code”, The Guardian, 30 August 2018. Available at https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger, quoting Neil F. Johnson and others, “Population polarization dynamics and next-generation social media algorithms”, 16 December 2017. Available at https://arxiv.org/pdf/1712.06009.pdf.

[61] European Union Agency for Fundamental Rights.

[62] Walsh, 2062: *The World that AI Made*.

[63] Submission from Graham Greenleaf, University of New South Wales, Sydney, August 2018.

outside Europe — Microsoft being the most prominent example — are voluntarily adopting compliance with the Regulation across their whole business operations, irrespective of a legal obligation to do so. Such voluntary adoption may be just as significant as legally required adoption.[64]

99. From another perspective, countries with broad data localization laws are creating new privacy standards for the data collected within their jurisdiction. In China, the Cyber Security Law introduces restrictions on cross-border data transfers that differ from international privacy regimes, such as the General Data Protection Regulation and the voluntary Cross-Border Privacy Rules of the Asia-Pacific Economic Cooperation.[65] While the Regulation and the Law appear to have similar cross-border transfer tests, the latter does not provide for derogations found in the former.[66] The Law also does not contain certain mechanisms provided under the Regulation, such as binding corporate rules or standard data protection clauses for companies to gain approval.

100. The preliminary recommendations of the Special Rapporteur in his October 2017 report to the General Assembly were developed independently from the General Data Protection Regulation and the Modernized Convention 108, but are aligned to those instruments (see table).[67] The alignment achieved is important when considering the wider international context: the Modernized Convention 108 is steadily becoming global and includes many, though not all, of the Regulation's new elements.[68] It is likely, in the next 5 to 10 years, that the extraterritorial effects of the Regulation with the ever-widening club of States parties to the Convention, will have a significant effect on the deepening worldwide privacy culture. The precise nature of that evolution is still emerging, as is its relevance to the need for further developments, such as stand-alone principles for big data and open data.

101. While a consistent international framework for the regulation of big data and open data is needed, it would be premature to commence work on standalone principles relating specifically to big data and/or open data before there has been sufficient time to ascertain the robustness and international effect of the General Data Protection Regulation and the Modernized Convention 108.

102. The big data and open data recommendations are to be understood, therefore, in the spirit of existing privacy and data protection principles, rather than any new unique rules.

[64] Graham Greenleaf, "Global convergence of data privacy standards and laws: speaking notes for the European Commission events on the launch of the General Data Protection Regulation in Brussels and New Delhi", University of New South Wales Law Research Series, No. 56, 25 May 2018. Available at www.austlii.edu.au/au/journals/UNSWLRS/2018/56.html.

[65] Samm Sacks, Paul Triolo and Graham Webster, "Beyond the worst-case assumptions on China's cybersecurity law", blog post, New America, 13 October 2017; and submission from the Allens Hub for Technology, Law and Innovation, 14 August 2018.

[66] Xiaoyan Zhang, "Cross-border data transfers: CSL vs. GDPR", The Recorder, 2 January 2018; and submission from the Allens Hub for Technology, Law and Innovation, 14 August 2018.

[67] Submission from Graham Greenleaf, August 2018.

[68] Since 2011, Convention 108 has added to its 47 parties that are members of the Council of Europe through accession requests from Argentina, Burkina Faso, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay. Eleven other countries, or their data protection authorities, are observers on its Consultative Committee.

Recommendations of the Special Rapporteur in his October 2017 report and their alignment with the General Data Protection Regulation and the Modernized Convention 108

Paragraph of the October 2017 report of the Special Rapporteur (A/72/540)	*Section of the European Union General Data Protection Regulation*	*Article of the Modernized Convention 108*
131 (a), on accountability	5 (2) 'Accountability'	10 (1)
131 (b), on transparency	12 'Transparency'; 22 (3) 'Automated decision-making' and transparency	5 (4), 8 (1)
131 (c), on quality	5 (1) (c) 'data minimization', (d) 'accuracy'	5 (1)
131 (d), on predictability of machine learning	22 'Automated decision-making'	8 (1), (2)
131 (e), on security	32–34 'security' (incl. breach notification)	7 (1)
131 (f), on risk identification and mitigation tools	35 'Data protection impact assessment'; 36 'Prior consultation'	10 (2);
131 (g), on employee training	37–39 'Data Protection Officer'	–
131 (h), on unambiguous focus of privacy regulation	52 'Independence' of data protection authority	15 (5)
131 (i), on sufficient regulatory powers for "big data"	57 'Tasks', 58 'Powers'	12, 15
131 (j), on privacy laws fit to handle technology advances	4 (1) 'personal data'; 4 (4) 'profiling'; 4 (5) 'pseudonymization'; 22 'Automated decision-making'; 25 data protection by design and by default';	8 (1) and (2); 10 (3)
131 (k), on formal consultative mechanisms	36 'Prior consultation'; 57 (b), (c), (d) and (g) data protection authority 'Tasks'	–
131 (l), on consultations on dangerous practices	36 'Prior consultation';	–
131 (m), on new techniques	57 (i) data protection authority 'Tasks — 'monitor new technology'; 25 'Data protection by design and by default'	10 (3)
131 (n), on citizen awareness	12 'Transparency'; 13–15 'Notice to data subjects'; 57 (b), (c), (e) data protection authority 'Tasks'	15 (2) (e)
126, on binding requirements and robust enforcement for open data concerning de-identification	25 'Data protection by design and by default'; 4 (1) 'personal data'; 4 (5) 'pseudonymization'	10 (3)
127, on rigorous privacy impact assessments if unit record-level data is used in open data	35 'Data protection impact assessment'	10 (2)
128, No open data or exchange of unit record-level data without robust de-identification	4 (1) 'personal data'; 4 (5) 'pseudonymization'	2 (d)
129, Ensure extra protections for sensitive data	9 'Special categories'	6

Source: Graham Greenleaf, Post-consultation submission, 7 August 2018.

H. Conclusions

103. **Data is and will remain a key economic asset, like capital or labour. Its integral dependency upon personal information demands accommodation with privacy and data protection laws.**

104. **International human rights law requires that any interference with the right to privacy must be lawful, necessary and proportionate. On occasion, the challenge to privacy may be lawful, but whether it is ethical is another issue. It is questionable whether some examples discussed here are ethical, lawful, necessary and proportionate. Recent cases of mismanagement of personal data by private and public entities require strong responses to prevent reoccurrences.**

105. **International human rights law also requires that those who experience a violation of their right to privacy have access to remedy. This is even more significant in the big data and open data era.**

106. **A key challenge for releasing data publicly as open data is the absence of a way to determine unambiguously if there is personal information in supposedly de-identified data sets or aggregated data.**

107. **Economic and political drivers underlie the policies and practices surrounding open data. The business models inherent in capitalist economies have little incentive to protect personal data when there is no resultant economic disadvantage in counterbalance to the profits to be made.**

108. **An international framework with consistent data protections and clear rules for transnational access would help weigh privacy protections and the competing interests that nations may have in gaining access to data, for example in the context of law enforcement, or that multinational corporations may have in managing data flows internally.**

109. **Initiatives enabling the unrestricted sharing of data and those dismantling existing legal safeguards on privacy are contrary to the protection of the right to privacy and must cease.**

110. **The criminalization of the re-identification (in the public interest) of de-identified data sets is not supported as a safeguard for personal data.**

111. **Detailed unit record-level data (identifiable data) should not be disclosed or published online without the data subject's consent. The use of physical and technical methods, such as secure research environments, to restrict access to sensitive unit record-level data is appropriate.**

112. **Consumer law and data protection law can usefully complement each other. Privacy law, with its human rights and societal dimensions, provides an anchor for consumer law. Sole reliance upon consumer law will deny individuals the broader enabling aspects of the interdependency between fundamental human rights and their remedial mechanisms.**

113. **The current and potential manifestations of artificial intelligence require independent oversight by experts in different subject fields. The evolution of this technology needs a strong legal and policy framework grounded in human rights. This is urgent and critical.**

114. **The application of article 22 of the General Data Protection Regulation needs to be closely monitored with respect to its ability to address automated processing issues arising from the use of artificial intelligence.**

115. **It is essential to address the lack of technological capabilities required to engineer appropriate systems, methods and processes and to ensure robust systems, methods and processes for strong protection for personal data. This should involve small technology companies and start-ups.**

116. **Where Member States are contemplating legislation for the promotion of open data,[69] the following parameters are recommended:**

(g) **All legislation must be strongly aligned with each State's international human rights obligations;**

(h) **Best practice data protection legislation should be studied as examples to follow;**

(i) **Data ethics frameworks and accountability mechanisms based on principles of fairness and justice are necessary for public and private sector data practices;**

(j) **Adequate regulatory models for privacy and data protection require structural independence, adequate resources and a regulator with the capacity for independence;**

(k) **Dismantling privacy and data protection laws to enable open data is contrary to global trends, ill-advised and contrary to States' international human rights obligations on the right to privacy;**

(l) **Definitions and concepts need to distinguish between data-sharing, use, disclosure and release;**

(m) **Co-design frameworks need to use participatory models and mechanisms with sufficiently diverse representation to address issues such as indigenous data sovereignty.**

I. Recommendations

117. **The original recommendations that the Special Rapporteur made in his report to the General Assembly dated 19 October 2017 (A/72/540) have been expanded based on the consultation, as follows:**

(a) **Governments' internal sharing of personal data should be distinguishable in legislation, policies and practices from releasing data to the public as open data;**

(b) **Unless and until it is possible to unambiguously determine if there is personal information within aggregated data or that disaggregated data cannot be re-aggregated, then open data should not contain unit record-level records;**

(c) **Work to create international standards for privacy that preserve data-sharing and international standardization activities must continue without delay and be supported by Member States;**

(d) **Research into differential privacy is necessary and should be used for aggregate statistics and complex data types as well as other privacy-preserving technologies, such as homomorphic encryption and secure multiparty computation;**

(e) **As an interim minimum response to agreeing to detailed privacy rules harmonized at the global level, Member States are encouraged to ratify the Modernized Convention 108 through its enabling legal instrument (Protocol CETS 223) and implement without undue delay the principles contained therein**

[69] For example, see the proposals of Australia in "New Australian Government data sharing and release legislation: issues paper for consultation", available at www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation, in the submission from M. Paterson.

through domestic law, paying particular attention to implementing immediately those provisions requiring safeguards for personal data collected for surveillance and other national security purposes;

(f) **To align with best practices, when reviewing and updating their domestic law as part of the implementation of the Modernized Convention 108, Member States outside the European Union are encouraged where possible also to incorporate those safeguards and remedies found in the General Data Protection Regulation but that are not mandatory under the Convention;**

(g) **Governments and corporations should recognize the sovereignty of indigenous peoples over data that is about them or collected from them and that pertains to indigenous peoples, knowledge systems, customs or territories, by always including formalized indigenous developed principles, a focus on indigenous leadership and mechanisms of accountability;**

(h) **Member States should review the adequacy of all legal and policy frameworks on artificial intelligence for the protection of freedom of expression and the right to privacy; foster strong multidisciplinary collaboration between statisticians, lawyers, social scientists, computer scientists, mathematicians and subject area experts; and devise strategies to prevent or address any negative impact on the enjoyment of human rights emerging from the use of algorithms, automated processing, machine learning and artificial intelligence.**

118. **The Special Rapporteur also reiterates the recommendations he made in his previous report (see A/72/540, paras. 126–131).**