Seventy-third session
Item 74 (b) of the provisional agenda*
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.

Summary

The report is divided into two parts: an executive summary of activities undertaken during 2017-18 is the first, introductory part of the report. The second and main part is the final report on the work of the Big Data Open Data Taskforce established by the Special Rapporteur on the right to privacy.

* A/73/150.
** The report was submitted after the deadline to reflect the most recent developments.
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, intelligence services, data protection authorities, intelligence oversight authorities, academics, corporations and other stakeholders.

2. In March 2018, the Special Rapporteur presented to the United Nations 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. The report provided an account of the Special Rapporteur’s 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 to 2021 and to continue the mandate’s important work.

3. The work program schedule was affected when the Special Rapporteur underwent urgent and unexpected surgery in April 2018. The impact upon his commitments was managed well. The Special Rapporteur thanks the Office of the High Commissioner for Human Rights for its support and assistance during the difficult period of his hospitalisation and convalescence. The Special Rapporteur made a full recovery and resumed his duties in June 2018.

A. Work of the ‘Health Data Privacy’ Taskforce

4. The Task Force on Health Data examined issues under the leadership of Dr. Steve Steffensen, MD Associate Professor, Dell Medical School, University of Texas. Although work had commenced on a draft report, unanticipated events meant the consultation planned for 2018 was postponed until 2019. The Vice Chair, Professor Nikolaus Forgo, has agreed to undertake the responsibilities of Taskforce Chair.

B. Work of the ‘Use of Personal Data by Corporations’ Taskforce

5. The right to privacy has never been more at the forefront of political, judicial or personal consciousness than 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 Cambridge Analytica breach, the introduction of legislation such as the Clarifying Lawful Overseas Use of Data Act, CLOUD Act (H.R. 4943), in the United States, the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 in Australia, and the United States v. Microsoft Corp. case before the United States Supreme Court, the Special Rapporteur brought forward the commencement of the Taskforce examining the corporate sector’s use of personal information.

7. The Taskforce 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. The Taskforce will advise the Special Rapporteur on emerging challenges to, and opportunities for the promotion of the right to privacy, including the gender impacts of these issues.

C. Work of the ‘A Better Understanding of Privacy’ Taskforce

8. The Taskforce explores the Human Rights Council’s recognition of the right to privacy as enabling the development of the person, and barriers to this enablement. It will

---

1 A/HRC/37/62.
collaborate with initiatives around the world such as that of the Australian Human Rights Commission’s examination of the impact of the digital era upon human rights.  

9. While all persons are entitled to enjoy the protection provided by international human rights law, there are reports that the enjoyment of the right to privacy is not 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. Relevantly, the Indian Supreme Court read down section 377 of the Indian Penal Code, to the extent it criminalised consensual sexual activity between adults, in a judgment that recognises the rights of the LGBTQI community in India. This judgment will have a significant impact on the gender and privacy discourse in India. It flows from the 2017 right to privacy judgment in the Puttaswamy case.  

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:

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

   (2) Has the digital era produced new or significantly different gender based experiences of privacy? If so, what are these?

   (3) 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?

   (4) 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 to 30 November 2018.

13. This initiative follows the “Privacy, Personality and Flows of Information” consultations of July 2016, May 2017, and September 2017 around the world. The fourth “Privacy, Personality & Information Flows” event planned for May 2018 in Latin America was postponed due to the Special Rapporteur’s inability to travel, and will occur in mid 2019.

D. Work of the ‘Security and Surveillance’ Taskforce

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, applications were lodged with the European Court of Human Rights (ECHR) 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 ECHR recently found that the United Kingdom’s bulk interception regime violated Article 8 of the European Convention on Human Rights (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

---

3 Communication Smitha Krishna Prasad, Centre for Communication Governance, National Law University, Delhi, 24 September 2018.
4 Including experience inclusive of sexual orientation, gender identity, gender expression and sex characteristics.
for examination, and inadequate safeguards for selection of “related communications data” for examination.

16. The Court held the regime for obtaining communications data from communications service providers violated Article 8; and that both the regimes for bulk interception and for obtaining communications data from communications service providers violated Article 10 of the Convention due to insufficient safeguards for confidential journalistic material. It further found that the regime for sharing intelligence with foreign governments did not violate either Article 8 or Article 10.6

17. While this judgement concerned the United Kingdom’s earlier statutory framework for surveillance, its findings are very significant and are brought to the attention of Member States for 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 Government of the United Kingdom’s Consultation on its proposed response, the Special Rapporteur provided input in early 2018. This will be available on the OHCHR website according to usual protocols.

19. In September 2018, the Australian Government introduced into the Australian Parliament the Telecommunications and Other Legislation Amendment (Assistance and Access) 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 equally as likely to endanger security as not; it is technologically questionable if it can achieve its aims and avoid introducing vulnerabilities to the cybersecurity of all devices irrespective of whether they are mobiles, tablets, watches, cars, CCTV, and it unduly undermines human rights including the right to privacy. Assurances that it is not a ‘backdoor’ into encrypted communications are unreliable since it may create, in effect, additional keys to the front door, or even more front doors.

21. The Bill has an overly high level of discretion on the use of exceptional powers. The accountability is not to the Parliament but to 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 amongst other actions into device(s) is disturbingly akin to government hacking. It was introduced into Parliament after an inadequate period of consultation and despite receiving reportedly over 14,000 submissions, just two weeks after consultation close.7

22. The Special Rapporteur’s concerns are compounded by the Australian Government’s stance on remedy for serious invasions of privacy and Australia’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 European adequacy assessment.

23. A new approach to addressing the challenges posed by encryption for law enforcement and national security is required. While there are challenges posed by technology to law enforcement and intelligence services, and countering online child sexual abuse and negating terrorism threats is important, 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,

---

6 European Court of Human Rights, Case of Big Brother Watch and Others v. the United Kingdom, 13 September 2018. (Applications nos. 58170/13, 62322/14 and 24960/15) at https://hudoc.echr.coe.int/eng#{"itemid":"002-12080"}

privacy, and the economy.\textsuperscript{8} Weakening encryption technology puts at risk the modern information economy’s security.\textsuperscript{9}

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

25. I commend to Member States the approach of the Government of the Netherlands, which has recognised 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.\textsuperscript{10}

26. The Special Rapporteur’s International Intelligence Oversight Forum (IIOF) will meet in Malta in late November. Interest is such that the Forum is over-subscribed.

E. Communications

27. The Special Rapporteur submitted 17 communications since 22 September 2017; eight were ‘allegation letters’, seven ‘other letters’, and two were ‘urgent appeals’. Of the 17 communications, 15 were communications submitted jointly with other mandate holders and two communications submitted by the Special Rapporteur alone.

F. Promoting the right to privacy

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

29. The Special Rapporteur has issued eleven press releases and statements. Of these, two were with released jointly with other mandate holders, on the rights of environmental activists in the upcoming 24th Conference of the Parties to the United Nations Framework Convention on Climate Change (COP24)\textsuperscript{11} and on Mexico’s draft security law.\textsuperscript{12}

30. On 19-20 February 2018, the Special Rapporteur delivered a presentation on the role of the right to privacy within the human rights framework and for civic space protection, and moderated a session 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 of Great Britain and Northern Ireland. The Special Rapporteur’s end of mission statement provides preliminary observations.\textsuperscript{13} The final report will be submitted to the 40th session of the Human Rights Council in February/March 2019.
32. In 2015 the Special Rapporteur was very critical of legislative proposals which increased the surveillance powers of the United Kingdom Government. Significant improvements have been made since on the intelligence oversight regime, including the establishment of a better resourced Investigatory Powers Commissioner’s Office (IPCO) 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 or the Foreign Secretary. A positive aspect are those safeguards against arbitrary or unlawful surveillance applying 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 the IPCO perform the dual task of authorizing surveillance and overseeing that very 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 these 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 the early completion of placing Data Guardian’s role on a statutory footing.

35. Other issues within the end of mission statement include anti-radicalization measures, the Prevent program and their impact on Muslims; proposals to criminalise access to extremist material; and matters raised by civil society organisations.

Planned country visits

36. The next official country visit is to the Federal Republic of Germany (29 October to 9 November 2018). It will be preceded by a call for contributions from interested parties via the Special Rapporteur’s website.

Informal visits and international events

37. While visiting Australia for the Big Data – Open Data consultation, the Special Rapporteur visited three States and met with civil society organisations, a Government Minister and the Shadow Attorney General, Government officials, corporations, professional associations, academics and other individuals. The Special Rapporteur met the Australian Human Rights Commissioner and Commission President, and gave public lectures for Grand Challenges-University New South Wales, Sydney; Melbourne University; La Trobe University; and Edith Cowan University. The Optus Macquarie University Cyber Security 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 (iappANZ) organised meetings with privacy practitioners.

38. The Special Rapporteur also participated in the following conferences: 16th International Conference on Cyberspace (Czech Republic, November 2017); 11th International Conference on Computers, Privacy and Data Protection 2018: The Internet of Bodies (Brussels, January 2018); Expert workshop on the right to privacy in the digital age (Geneva, February 2018); the Global Internet And Jurisdiction Conference (Ottawa, February 2018); MAPPING Conference (Malta, February 2018).

H. Developments on the right to privacy

The 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 advised, in his 2018 report, the Human Rights Council on violations of article 12 of the UDHR and article 17 of the ICCPR.

---

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 access a 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 how complex algorithms operate is largely unknown, as is their developmental progression in the case of machine learning. This requires examination from the perspective of all human rights. This assessment is necessary prior to, or in tandem with, policies that encourage and enable the development and deployment of products based on artificial intelligence.15 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 introducing privacy/data protection laws,16 with 2018 having been a particularly active year around the world.

44. Of particular note is India’s draft law following the Puttaswamy decision of the Supreme Court.17 The draft Bill, released in mid-2018, has many positive features also found in the European General Data Protection Regulation 2016/679 (GDPR), 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 datasets. Further, while the use of personal data by law enforcement is to be “necessary and proportionate,” disclosure in legal proceedings has very broad exemptions.18 The Special Rapporteur urges the Indian Government to engage with academics, researchers and civil society organisations raising such issues.

45. In a judgement 26 September 2018, the Indian Supreme Court upheld the constitutional validity of the Aadhar Act, but revoked:

Section 57 whereby private companies could ask consumers for Aadhaar details for identification purposes for their services.

Section 33(2) sharing of data with security agencies on the ground of national security.

Section 47 whereby only the government could complain in case of theft of Aadhaar data.19

The Court required the Government to introduce robust data protection legislation.

46. Within the European Union (EU), there has been significant reform. The GDPR came into force 25 May 2018. Also, a specific Directive on data protection in police and justice areas became applicable from 6 May 2018. The Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications (ePrivacy Directive) is

15 OpenGov Newsletter (Bhunia, P), Taskforce recommends establishment of national mission for coordinating AI-related activities across India, 9 April 2018.
17 http://supremecourtofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf.
18 The Register (Chirgwin, R.), India mulls ban on probes into anonymized data use – with GDPR-style privacy laws, 31 July 2018 https://www.theregister.co.uk/2018/07/31/india_privacy_boffin_ban/.
due to be replaced by the new ePrivacy Regulation\textsuperscript{20}. Regulation (EC) 45/2001 lays down the rules for data protection in EU institutions and the duties of the European Data Protection Supervisor. The European Commission adopted a proposal on 10 January 2017 which repeals Regulation (EC) 45/2001 and aligns it with the GDPR. These are expected to apply from late 2018 onwards. With this reform, the EU will complete the first major modernisation of its framework for protecting privacy and data protection in over 20 years.\textsuperscript{21}

47. These important consolidation measures within the EU apply to all sectors, except to privacy and “national security” - a matter excluded from the EU’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 EU 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 modernisation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108 (Convention 108), was finalised in June 2018 and the enabling legal instrument, Protocol CETS 223 was opened for signature on 10 October 2018. This is an important milestone as this international treaty, unlike GDPR, also covers national security and has been ratified by more than 55 UN member states, with an increasing number of non-European states also joining.

49. In Brazil, the Federal Senate approved a General Data Protection Law to become effective in February 2020. Key elements include\textsuperscript{22}:

- Cross-border jurisdiction
- Privacy principles and risk-based approach
- New rights for individuals
- More legal bases for processing of personal data
- Data-mapping and data protection impact assessments
- Mandatory breach notification and data protection officer
- Restrictions to the cross-border transfer of personal data

50. Non-compliance can result in fines amounting to two percent of the gross sales of the company/group of companies or a maximum sum, per infringement, of approximately USD 12.9 million.

**Indigenous peoples and data**

51. The Special Rapporteur has studied the privacy culture of Aboriginal Australians for many years.\textsuperscript{23} Being one of the most sophisticated, lived expressions of privacy involving individual, familial and group privacy implemented through behaviours, rites and practices such as private and communal spaces, the Special Rapporteur was pleased that the Big Data – Open Data consultation explored Indigenous Data Sovereignty albeit in a modest fashion.

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

---

\textsuperscript{20} Regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications repealing Directive 2002/58/EC.


II. Consultation on interim Big Data-Open Data report

53. The Special Rapporteur presented his interim report on Big Data – Open Data to the General Assembly in October 2017.24 The report reviewed the challenges to the human right to privacy from a defining feature of the digital era, that is, Big Data – Open Data. Since then, the introduction of the GDPR and the Facebook-Cambridge Analytica revelations have occurred.

54. Consultation with Government officials, civil society organizations, companies and individuals on the interim report occurred in Australia on 26 and 27 July 2018. It was preceded by a call for submissions on the interim report which concluded on 28 April 2018 and summarised for the consultation. Further input came from meetings with civil society organisations organised 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; and indigenous data sovereignty, consumer and gender issues, and non-European country perspectives.25 Much of the discussion 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, and for the very fabric of democratic societies. The opening up of government information, particularly the iterative public release of data sets containing personal information, needs more nuanced and closer examination.26

57. The consultation examined the proposition that Big Data analytics can identify individuals despite de-identification.27 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 this 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 (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 very wide field and descriptions vary in different jurisdictions. What most definitions have in common is that the scope of personal information can be very 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:

25 Lo, A. The Right to Privacy in the Age of Big Data and Open Data, article for AHRI, UNSW Sydney, August 2018. (Law student, University of Hong Kong, intern Allens Hub for Technology, Law and Innovation).
26 Submission Professor M. Paterson, Monash University, August 2018.
• the data itself must identify an individual; or
• it must be reasonably possible to identify an individual.

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 organisation which captures, uses and stores that data.

61. Online browsing and purchasing data can be used to increasingly personalise services 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 optimisation, allowing customer churn prediction and even to reveal relationships to other mobile users without knowing the identity of the individuals involved.  

62. A key challenge for sharing data is that there is currently no way to unambiguously determine 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 organisations depending on the perceived risk associated with the data being shared.

63. The development of standards of what constitutes "de-identified" data would help to address 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 organisations must determine what "de-identified" 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 whitepaper exploring the challenges of data sharing. The paper 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 this question is a major challenge as the act of combining datasets creates information. The paper further proposed a modified version of the "Five Safes" framework for data sharing to quantify different thresholds for "Safe". This work continues with the support of Standards Australia and aims to initiate work to create international standards for privacy preserving data sharing. A second whitepaper is planned for October 2018. This is expected to form the basis of international standardisation activities with the goal of ultimately defining robust privacy preserving, data sharing frameworks.

65. An example presented of the limitations of de-identification for protecting unit level records was the release online, in August 2016 of a large longitudinal dataset for a 10% sample of Australians who had claimed Medicare Benefits since 1984, or Pharmaceutical Benefits since 2003. This affected the medical data of around 2.9 million Australians, comprising prescriptions, surgery episodes, tests (excluding results), and visits to general practitioners and specialists (excluding doctors’ notes). The dataset had been downloaded 1,500 times before being taken offline following reports that doctors' IDs could be easily

28 Submission Dr Ian Opperman, CEO and Chief Data Scientist, Data Analytics Centre, NSW Government, Australia, 31 August 2018.
30 Dr Opperman, as above.
decrypted\textsuperscript{33}, and later, that patients could be identified.\textsuperscript{34} The release by the Australian Department of Health sought to facilitate medical research.

66. Important questions raised by such examples are: ‘should government-held personal information datasets be released externally when there are increasing risks of large-scale privacy breaches from re-identification due in part to the availability of other publicly released information, and inadequate organisational technological capabilities?’, and, ‘what is an appropriate response to prevent such incidents re-occurring?’\textsuperscript{35}

67. The consultation 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 level data, and 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 criminalisation of re-identification undertaken to test the security of released datasets.\textsuperscript{35}

68. Participants described existing mechanisms that permit the use of identifiable personal data for research purposes\textsuperscript{36}, pointing out that these could be expanded, as appropriate, for further public interest uses.\textsuperscript{37}

69. The question is ‘if useful data is viewed as a limited resource rather than as an unlimited untapped resource, would we have more sustainable practices?’\textsuperscript{38}

70. Current practices that alienate the data subject are, in effect, ‘killing the goose that laid the golden egg’, as distrust of government and private actors managing personal information appropriately, results in not using services (risking adverse societal impacts, for example, in public health areas) or by providing incomplete or inaccurate information.\textsuperscript{39} These actions also undermine data quality and, ultimately, the accuracy of machine-learning algorithms.

71. Overwhelmingly, the view was the sustainability of data practices increases if data subjects are fully fledged partners in data operations.\textsuperscript{40} Participants heard that nowhere is this more evident and important than for indigenous peoples.

C. Indigenous Data Sovereignty

72. Data are 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.\textsuperscript{41} Existing data and data infrastructure fail to recognise


\textsuperscript{34} The OAIC 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.

\textsuperscript{35} Submissions eg Professor M. Paterson, Monash University, August 2018.

\textsuperscript{36} These mechanisms are commonly subject to oversight by ethics committees with access restricted to researchers under confidentiality obligations.

\textsuperscript{37} For example, based on mechanisms such as the 5 Safes Framework: see ABS, Managing the risk of disclosure: the five safes framework, http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=S.

\textsuperscript{38} Submission from Associate Professor Theresa Dirndorfer Anderson, Course Director, Master of Data Science & Innovation, University of Technology Sydney.


\textsuperscript{40} Submission to ‘Big Data Open Data’ Consultation, Associate Professor Theresa Dirndorfer Anderson, Course Director, Master of Data Science & Innovation, University of Technology Sydney.

or privilege indigenous knowledge and worldviews and do not meet indigenous peoples’ current and future data needs. Current practices around Open Data and Big Data, whether under the auspices of governments or corporations, will likely move indigenous peoples’ data interests even further from where decisions affecting indigenous peoples’ data are made.

73. Indigenous Data Sovereignty (IDS) is a global movement concerned with the rights of indigenous peoples to own, control, access and possess data that derive from them, and which pertain to their members, knowledge systems, customs or territories. IDS 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 IDS is the desire for data to be used in ways that support and enhance the collective wellbeing of indigenous peoples.

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

75. IDS illustrates that good practices in Big Data and Open Data require an awareness of data that is missing, under-represented or misrepresented, 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 LGBTIQ people, 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 accessing services as LGBTIQ 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 in the Taskforce on ‘Privacy and Personality’ and the gender project outlined above, however, in terms of Big Data – Open Data, good data practices require reviewing data collections with an awareness of the possible


43 Submission Professor Maggie Walter Professor Sociology and Pro Vice-Chancellor (Aboriginal Research and Leadership) University of Tasmania, Australia.

44 Submission Associate Professor Dirndorfer Anderson, as above.


46 A/HRC/38/47.

impact of poor privacy practices and differing consequences according to gender and 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 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.\textsuperscript{48}

81. The use of consumers’ personal data by financial services\textsuperscript{49} and other sectors, has given rise to concerns at both public policy and individual levels.\textsuperscript{50} The fair processing of personal data is increasingly part of the reasonable expectations of consumers regarding the services and products they utilise.\textsuperscript{51}

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

83. Following the Cambridge Analytica scandal, in June 2018 California enacted the AB-375 Consumer Privacy Act, to take effect in January 2020, to protect the data privacy of technology users and others by imposing new rules on companies that gather, use, and share personal data.\textsuperscript{52} The Act creates four basic rights\textsuperscript{53}:

- “A ‘right to know’ what personal information a business has about them and where that personal information came from or was sent”;
- “A ‘right to delete’ personal information that a business collected from them”;
- “A ‘right to opt-out’ of sale of personal information about them”; and
- “A ‘right to receive equal service’ and pricing from a business, even if they exercise their privacy rights under the Act”.\textsuperscript{54}

84. “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.”\textsuperscript{55}

85. It is reported these rights need strengthening, as;\textsuperscript{56}


\textsuperscript{50} Pew Research Center (Rainie, L and Duggan, M). Privacy and Information Sharing, 2016: people’s comfort level depends on perception of trustworthiness, what happens post collection, and retention length. Consumer Policy Research Centre (Nguyen, P. Solomon, L.), Consumer data and the digital economy - Emerging issues in data collection, use and sharing, 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.


\textsuperscript{52} https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

\textsuperscript{53} Electronic Frontier Foundation, (Schwartz, A., Tien, L, McSherry, C.) How to Improve the California Consumer Privacy Act of 2018, August 8, 2018.

\textsuperscript{54} Ibid.

\textsuperscript{55} Ibid.

\textsuperscript{56} Ibid.
• ‘business’ is narrowly defined. In the digital era small tech players and individuals can also undermine privacy in a myriad of ways through not having the knowledge, skills or resources to implement adequate data protection,

• businesses can still charge a higher price to users exercising their privacy rights,

• users cannot easily bring violators to court due to narrow exceptions,

• user consent is only required for data sale not collection, and consent for data sale is opt-out,

• the ‘right to know’ is not by specific sources and recipients, and the right to deletion is for information collected from them not for information held ‘about them’, and

• most enforcement responsibility rests with the California Attorney General rather than an independent entity.

86. In EU data-protection law, aspects of the GDPR provide EU consumers with new protections including greater transparency and control of data being collected about them by companies than may be provided by the EU consumer protection directives.

87. Australia is establishing a Consumer Data Right - a data portability right which falls short of the wider protections provided by privacy or data protection law for Australian consumers whose data is being collected, shared and used on a daily basis. The consultation heard that this data portability right, rather than protecting consumers’ data, potentially will expose it to greater use by third parties.

88. There is advantage in strong collaboration between consumer law and privacy law for example, in co-coordinated legal action. 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.

89. Feedback received on practical measures to help entities improve their trust relationship with users included communicating the terms of data use through standard licences akin to the six standardised Creative Commons licences. This was seen as potentially able to alleviate some of the challenges of complex privacy policies, while simplifying and

---

57 "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% or more of its annual revenue from selling personal information (Section 140(c))" Electronic Frontier Foundation, How to Improve the California Consumer Privacy Act of 2018, August 8, 2018.

58 Submission Dr Roland Wen, UNSW Sydney, Australia.


62 Dr Katherine Kemp, Centre for Law, Markets and Regulation, UNSW Sydney, UN SRP Consultation on Big Data – Open Data, 26-27 July, 2018 Sydney Australia.

standardising communication to users in different countries.\textsuperscript{64} Draft licence types could be backed by more detailed ‘standard conditions’ privacy policies.\textsuperscript{65}

90. Capturing privacy risks in privacy rating labels could make privacy choices more accessible to consumers and increase the transparency and disclosure of privacy risks by data controllers.\textsuperscript{66}

\section*{F. Artificial Intelligence}

91. Machine learning and artificial intelligence (AI) 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 AI, has the potential to revolutionise societies positively - but also has the potential to profoundly change our world and our chances of survival, not necessarily for the better.\textsuperscript{67}

92. This latter outcome could occur through the potential negative impact on human rights, including the right to privacy. AI methods can be, and are being, used to identify people who wish to remain anonymous; to enable micro-targeting of messaging; to generate sensitive information about people from non-sensitive data; to profile people based upon population-scale data; and to make decisions using this data thereby profoundly affecting people’s lives.\textsuperscript{68}

93. As more and more actions and decision-making are transferred to machines, there is an urgency in ensuring that machine-learning and algorithms are transparent as to their logic and their assumptions. Algorithms used in machine-learning and AI are increasingly complex and transparency will be difficult to achieve. Yet that complexity should not prevent auditing to ascertain lawfulness.\textsuperscript{69} Currently the use of Big Data related technologies is not being held sufficiently accountable whether under international human rights law, data protection, sectoral privacy regulation or ethical codes and industry standards.\textsuperscript{70} 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 an historical anomaly - it will be a technologically given right.’\textsuperscript{71}

94. The GDPR 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 of the processing for the individual.\textsuperscript{72} There is an overall prohibition (with narrow exceptions) to have decisions made by solely automated processes when such decisions have legal or other significant effects.

95. The GDPR defines profiling as the automated processing of data to analyse or to 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 AI 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 AI, a Data Privacy Impact Assessment could (perhaps should) enable entities to model the

\textsuperscript{64} Submission Allens Hub for Technology, Law and Innovation, 14 August 2018.
\textsuperscript{65} See footnote 66.
\textsuperscript{67} Walsh, T. 2062 \textit{The World that AI Made}, La Trobe Press, 2018.
\textsuperscript{68} Privacy International and Article19, \textit{Privacy and Freedom of Expression In the Age of Artificial Intelligence}, May 2018.
\textsuperscript{70} Walsh, T. 2062 \textit{The World that AI Made}, La Trobe Press, 2018, p171.
\textsuperscript{71} Articles 13, 14 and 22 of GDPR.
effects of their algorithms in much the same way climate scientists model climate change or weather patterns.\textsuperscript{73}

96. The European Union Agency for Fundamental Rights has suggested one way of ensuring 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.\textsuperscript{74}

97. While the means still need to be determined, it is relevant that new technologies have required the strengthening of international humanitarian law throughout the last century.\textsuperscript{75}

**G. Principles for Big Data and Open Data**

98. In the interim report\textsuperscript{76}, 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 for data protection regarded as representing ‘best practice’. At present, these are the EU’s GDPR and the ‘modernised’ Convention 108 (‘Convention 108+’, 2018) which originated at the Council of Europe but is open to accession globally by States which have enacted consistent principles.\textsuperscript{77}

99. GDPR’s influence is not exerted only through local legislative enactments or its extraterritorial application. Companies outside Europe, Microsoft being the most prominent example, are voluntarily adopting ‘GDPR compliance’ across their whole business operations irrespective of a legal obligation to do so. This ‘GDPR-creep’ may be just as significant as legislative adoption.\textsuperscript{78}

100. From another perspective, countries with broad data localisation laws are creating new privacy standards for data collected within their jurisdiction. The Cyber Security Law (CSL) of the People’s Republic of China introduces restrictions on cross-border data transfers that differ from international privacy regimes such as the GDPR and the voluntary Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (CBPR).\textsuperscript{79} While the GDPR and CSL appear to have similar cross-border transfer tests, CSL does not provide for derogations found in the GDPR.\textsuperscript{80} Neither does the CSL contain certain GDPR mechanisms such as Binding Corporate Rules and standard data protection clauses for companies to gain approval.

101. The preliminary recommendations in the Special Rapporteur’s 2017 interim report to the General Assembly\textsuperscript{81} were developed independently from the GDPR and Convention 108+, but are aligned to those instruments (see table below).\textsuperscript{82} The alignment achieved is


\textsuperscript{74} Fundamental Rights Agency, #BigData: Discrimination in Data Supported Decision Making, 2018.

\textsuperscript{75} Walsh, T. Op. cit. p. 146.

\textsuperscript{76} A/72/43103.

\textsuperscript{77} Submission of Professor Graham Greenleaf, School of Law UNSW Sydney, August 2018.

\textsuperscript{78} Greenleaf, G. 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 & New Delhi, 25 May 2018.

\textsuperscript{79} Samm Sacks, Paul Triolo, Graham Webster, “Beyond the Worst-Case Assumptions on China’s Cybersecurity Law”, New America, October 2017 Submission Allens Hub for Technology, Law and Innovation, 14 August 2018.

\textsuperscript{80} Xiaoyan Zhang, “Cross-Border Data Transfers: CSL vs. GDPR”, The Recorder, January 2018 Submission Allens Hub for Technology, Law and Innovation, 14 August 2018.

\textsuperscript{81} A/72/43103, par. 125-131.

\textsuperscript{82} Submission Professor Graham Greenleaf, School of Law, UNSW Sydney, August 2018.
important when considering the wider international context: Convention 108 is steadily being ‘globalised’, and the ‘updated’ Convention (‘Convention 108+’) includes many, though not all, of the GDPR’s new elements. It is likely, in the next five to ten years, that the extraterritorial effects of GDPR with the ever-widening club of Convention 108 countries, will have a significant effect on the deepening world-wide privacy culture. The precise nature of this 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.

While a consistent international framework for the regulation of Big Data and Open Data is needed, it would be premature to commence work on stand-alone 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 GDPR and 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 sui generis rules.

---

83 Since 2011, Convention 108 has added to its 47 European parties, Uruguay, Mauritius, Senegal, and Tunisia; Morocco, Cape Verde, Argentina, Mexico, and Burkina through Accession requests. Eleven other countries, or their data protection authorities, are Observers on its Consultative Committee.
### Alignment of Interim Report Recommendations with GDPR and Convention 108+.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>131(a) Accountability</td>
<td>GDPR 5(2) ‘Accountability’</td>
<td>10(1)</td>
</tr>
<tr>
<td>131(b) Transparency</td>
<td>GDPR 12 ‘Transparency’; 22(3) ‘Automated decision-making’ transp</td>
<td>5(4), 8(1)</td>
</tr>
<tr>
<td>131(c) Quality</td>
<td>GDPR 5(1)(c) ‘data minimisation’, (d) ‘accuracy’</td>
<td>5(1)</td>
</tr>
<tr>
<td>131(d) Predictability of ML</td>
<td>GDPR 22 ‘Automated decision-making’</td>
<td>8(1), (2)</td>
</tr>
<tr>
<td>131(e) Security</td>
<td>GDPR 32-34 security (incl. breach notification)</td>
<td>7(1)</td>
</tr>
<tr>
<td>131(f) Risk identification/mitigation tools</td>
<td>GDPR 35 ‘Data protection impact assessment’ (DPIA); 36 ‘Prior consultation’</td>
<td>10(2);</td>
</tr>
<tr>
<td>131(g) Employee training etc</td>
<td>GDPR 37-39 ‘Data Protection Officer’</td>
<td>–</td>
</tr>
<tr>
<td>131(h) Unambiguous focus of privacy regulation</td>
<td>GDPR 52 ‘Independence’ of DPA</td>
<td>15(5)</td>
</tr>
<tr>
<td>131(i) Sufficient regulatory powers for Big Data</td>
<td>GDPR 57 ‘Tasks’, 58 ‘Powers’</td>
<td>12, 15</td>
</tr>
<tr>
<td>131(j) Privacy laws fit to handle technology advances</td>
<td>GDPR 25 4(1) ‘personal data’; 4(4) ’profiling’; 4(5) ‘pseudonymisation’; 22 ‘Automated decision-making’; 25 DP by design and by default’</td>
<td>8(1), (2); 10(3)</td>
</tr>
<tr>
<td>131(k) Formal consultative mechanisms</td>
<td>GDPR 36 ‘Prior consultation’; 57(b), (c), (d) and (g) DPA ‘Tasks’</td>
<td>–</td>
</tr>
<tr>
<td>131(l) Consultations on dangerous practices</td>
<td>GDPR 36 ‘Prior consultation’</td>
<td>–</td>
</tr>
<tr>
<td>131(m) Investigate new techniques, particularly re de-ID</td>
<td>57(i) DPA ‘Tasks – monitor new technology’; 25 ‘Data protection by design and by default’</td>
<td>10(3)</td>
</tr>
<tr>
<td>131(n) Ensure citizen awareness</td>
<td>GDPR 12 ‘Transparency’; 13-15 Notice to data subjects; 57(b), (c), (e) DPA ‘Tasks’</td>
<td>15(2)(e0</td>
</tr>
<tr>
<td>126 Open Data to have binding requirements of reliable de-identification + robust enforcement</td>
<td>GDPR 25 ‘Data protection by design and by default’; 4(1) ‘personal data’; 4(5) ‘pseudonymisation’</td>
<td>10(3)</td>
</tr>
<tr>
<td>127 Rigorous Privacy Impact Assessments if unit-record data used in Open Data</td>
<td>GDPR 35 ‘Data protection impact assessment’</td>
<td>10(2)</td>
</tr>
<tr>
<td>128 No Open Data or exchange of unit-record data without robust de-identification</td>
<td>GDPR 4(1) ‘personal data’; 4(5) ‘pseudonymisation’</td>
<td>2(d)</td>
</tr>
<tr>
<td>129 Ensure extra protections for sensitive data</td>
<td>GDPR 9 ‘Special categories’</td>
<td>6</td>
</tr>
</tbody>
</table>

Source: Greenleaf, G. Post Consultation Submission, 7 August 2018.
H. Conclusions

103. Data is and will remain a key economic asset, like capital and 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 occasions, 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 recurrences.

105. International human rights law also requires that those who experience a violation of their right to privacy have access to a 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 unambiguously determine if there is personal information in supposedly de-identified datasets 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 accessing data, for example in the context of law enforcement, or that multi-national corporations may have in managing data flows internally.

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

110. The criminalisation of the re-identification (in the public interest) of de-identified datasets 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 AI 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 GDPR needs to be closely monitored on its ability to address automated processing issues arising from the use of AI.

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 tech companies and start-ups.
Where Member States are contemplating legislation for the promotion of Open Data, the consultation furnished the following parameters:

- All legislation must be strongly aligned with each State’s international human rights obligations.
- Best practice data protection legislation should be studied as examples to follow.
- Data ethics frameworks and accountability mechanisms based on principles of fairness and justice, are necessary for public and private sector data practices.
- Adequate regulatory models for privacy and data protection require structural independence, adequate resources and a position holder with the capacity for independence.
- 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.
- Definitions and concepts need to distinguish between data sharing, use, disclosure and release.
- Co-design frameworks using participatory models and mechanisms with sufficiently diverse representation to address issues such as IDS.

I. Recommendations

The original recommendations made in 2017 (A/72/43103) have been expanded based on the consultation, as follows:

(a) Governments’ internal sharing of personal data be distinguished 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 level records.

(c) Work to create international standards for privacy preserving data sharing, and international standardisation activities must continue without delay, and be supported by Member States.

(d) Research into Differential Privacy is necessary. It should be used for aggregate statistics and complex data types, and other privacy-preserving technologies such as homomorphic encryption and secure multiparty computation.

(e) As an interim minimum response to agreeing to detailed privacy rules harmonised at the global level, Member States be encouraged to ratify data protection Convention 108+ using CETS223 and implement the principles contained there through domestic law without undue delay, paying particular attention to immediately implementing those provisions requiring safeguards for personal data collected for surveillance and other national security purposes.

(f) As a matter of alignment of best practices, when reviewing and updating their domestic law as part of the transposition of Convention 108+, Member States outside the EU be encouraged to, if at all possible also incorporate safeguards and remedies found in the GDPR but not mandatory under Convention 108+.

(g) Governments and corporations recognise the sovereignty of indigenous peoples over data that are about them or collected from them, and which pertain to indigenous peoples, knowledge systems, customs or territories, by always including formalised indigenous developed principles, a focus on indigenous leadership and mechanisms of accountability.

(h) Member States review the adequacy of all legal and policy frameworks on AI for the protection of freedom of expression and the right to privacy; to foster strong multidisciplinary collaboration between statisticians, lawyers, social scientists, computer scientists, mathematicians and subject area experts, and to 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 AI.

118. The Special Rapporteur’s initial 2017 recommendations (A/72/43103) (with original paragraph number) were:

(i) Open Data policies require clear statements of the limits to using personal information based on international standards and principles, including an exempt category for personal information with a binding requirement to ensure the reliability of de-identification processes to render this information appropriate for release as Open Data, and robust enforcement mechanisms.

(j) Any open government initiative involving personal information, whether de-identified or not, requires a rigorous, public, scientific analysis of the data privacy protections including a privacy impact assessment.

(k) Sensitive high-dimensional unit-record level data about individuals should not be published online or exchanged unless there is sound evidence that secure de-identification has occurred and will be robust against future re-identification.

(l) Establish frameworks to manage the risk of sensitive data being made available to researchers.

(m) Governments and corporations should actively support the creation and use of privacy-enhancing technologies.

(n) The following options are to be considered when dealing with Big Data:

Governance:

(a) responsibility – identification of accountabilities, decision-making process and as appropriate, identification of decision makers

(b) transparency – what occurs, when and how to personal data prior to it being publicly available, and its use, including ‘open algorithms’.

(c) quality - minimum guarantees of data and processing quality

(d) predictability - when machine learning is involved, the outcomes should be predictable

(e) security - appropriate steps to be taken to prevent data inputs and algorithms from being interfered with without authorisation

(f) develop new tools to identify risks and specify risk mitigation

(g) support – train (and as appropriate accredit) employees on legal, policy and administrative requirements relating to personal information.

Regulatory environment:

(h) Ensure arrangements to establish an unambiguous focus, responsibility and powers for regulators charged with protecting citizens’ data

(i) Regulatory powers to be commensurate with the new challenges posed by big data for example, the ability for regulators to be able to scrutinise the analytic process and its outcomes
(j) Examination of privacy laws to ensure these are ‘fit for purpose’ in relation to the challenges arising from technology advances such as machine-generated personal information, and data analytics such as de-identification.

Inclusion of feedback mechanisms

(k) Formalise consultation mechanisms, including ethics committees, with professional, community and other organisations and citizens to protect against the erosion of rights and identify sound practices;

(l) Undertake a broadbasted consultation on the recommendations and issues raised by this report such as the appetite, for example, for prohibition on the provision of government datasets.

Research

(m) Technical: investigate relatively new techniques such as differential privacy and homomorphic encryption to assess if they provide adequate privacy processes and outputs.

(n) Examine citizens’ awareness of the data activities of governments and businesses, uses of personal information including for research, technological mechanisms to enhance individual control of their data and to increase their ability to utilise it for their needs.

III. Upcoming reports

119. The Special Rapporteur will present further reports:

(a) To the Human Rights Council:
   • “Lessons learned for improved safeguards and remedies in effective oversight of government surveillance”, March 2019;
   • “Proportionality, necessity and law in government surveillance, law enforcement and transborder flows of personal data: effectiveness and improvement of existing legal safeguards and remedies”, March 2020;
   • “Progress, regress and other dimensions of effective oversight of government surveillance”, March 2021.

(b) To the General Assembly:
   • “Improving safeguards and remedies for privacy and health data”, October 2019;
   • “Profits and privacy: monetisation of personal data as a business model and the responsibilities of corporations”, October 2019;
   • “Privacy, personality and flows of information: first global overview of the universal right to privacy from perspectives of time, place and space”, October 2020;
   • “The transborder flow of personal data between corporations, law enforcement and surveillance”, October 2021.

120. The Special Rapporteur will finalise the reports on the official visits to the United States, France and the United Kingdom, for March 2019 and may also report, time and resources allowing, on other issues such as privacy and gender impacts.

IV Acknowledgements

121. The Special Rapporteur thanks OHCHR in Geneva for its ongoing work and support for his mandate. The assistance from the United Nations staff in Geneva is gratefully acknowledged.
122. The Special Rapporteur sourced extra-mural funding and assistance from the Department of Information Policy and Governance, University of Malta, and the Security, Technology & e-Privacy Research Group, University of Groningen, Netherlands.

123. The Special Rapporteur thanks the University of New South Wales Sydney; the Optus Macquarie University Cyber Security Hub and the University of Technology; Allens Hub UNSW Sydney; L-Universita ta’ Malta; the University of Groningen in the Netherlands; Grand Challenges UNSW Sydney; the Australian Human Rights Institute, the Schools of Mathematics, Social Sciences, Built Environment, Computing and Engineering Sciences, and Law UNSW Sydney, and the Australian Human Rights Commission, for supporting the Big Data - Open Data consultation in Sydney. The Special Rapporteur also thanks the moderators, speakers and audience for their contributions.

124. The Special Rapporteur thanks the various Government representatives, civil society organisations, academics and individuals met over the past year.

125. The Special Rapporteur’s work could not be undertaken successfully without the efforts and support of non-governmental organizations, small and large, local, national and international around the world.

126. The Special Rapporteur thanks the many regulatory and professional bodies who have assisted the mandate, the Taskforce Chairs, members, interns, and the volunteers who provide research and secretariat support. Their commitment to human rights and to the work of Special Procedures mandate holders is unsurpassed.