|  |  |  |
| --- | --- | --- |
|  |  | A/HRC/40/63 |
|  | **Advance Unedited Version** | Distr.: General27 February 2019Original: English |

**Human Rights Council**

**Fortieth session**

25 February – 22 March 2019

Agenda item 3

**Promotion and protection of all human rights, civil**

**political, economic, social and cultural rights,**

**including the right to development**

 Right to privacy

 Report of the Special Rapporteur on the right to privacy[[1]](#footnote-2)\*

|  |
| --- |
| *Summary* |
|  In his report, prepared pursuant to Human Rights Council resolutions 28/16 and 37/2, the Special Rapporteur on the right to privacy focuses on issues in intelligence oversight; and provides the first report of the ‘Privacy and Gender’ work of the ‘Privacy and Personality’ Taskforce, and that of the Health Data Taskforce. Annexures provide the preliminary reports of these two UNSRP Taskforces. |
|  |

Contents

 *Page*

 I. Overview of activities 3

 II. Privacy in context 3

 III. Security and surveillance 6

 IV. The right to privacy: a gender perspective 10

 V. Health data protection 17

 VI. Privacy metrics 21

 Annexes . 23

 I. Overview of activities

1. Since March 2018, the Special Rapporteur has progressed the mandate through examining relevant information, including challenges arising from new technologies; undertaking official and ‘non-official’ country visits; promoting the protection of the right to privacy; advocating privacy principles; contributing to international events to promote a coherent approach to the right to privacy; raising awareness on the right to privacy and effective remedies, and reporting on alleged violations.

2. The Special Rapporteur reported to the General Assembly on ‘Big Data – Open Data’ in October 2018.

3. The Special Rapporteur’s activities since the 2018 Annual Report to the Human Rights Council have included:

1. Progressing, with Taskforce Chairs, the work of five Thematic Action Stream Taskforces on Security and Surveillance; Big Data – Open Data; Health Data; Corporations use of Personal Data, and Personality and Personality.
2. 24 communications to Member States raising matters concerning the right to privacy, and 14 press releases and statements.[[2]](#footnote-3)
3. Official country visits to the United Kingdom of Great Britain and Northern Ireland (June 2018) and Germany (November 2018).
4. Given keynote and other papers **(Annex 1)**.
5. Consulting a range of bodies for example, the Irish Civil Liberties Council, the Japanese Civil Liberties Union, the Japan Federation of Bar Associations, Privacy International, the Northern Ireland Commission for Human Rights, multiple activities at the Internet Governance Forum, RightsCon, amongst many others.
6. Exchanging information with various Governments (at national and sub-national levels); data protection and privacy commissioners; Chairperson, European Union’s "Article 29 Working Party"; Chairperson, Council of Europe’s Consultative Committee on Data Protection (T-PD); standards setting organizations, such as the International Telecommunication Union (ITU); the Institute of Electrical and Electronics Engineers; civil society organizations; Permanent Missions to the United Nations in Geneva; Special Procedures mandate holders, the Office of the High Commissioner for Human Rights, researchers, academics and professional bodies.

 II. Privacy in context

4. The right to privacy can facilitate the enjoyment of other human rights. Equally, its infringements constrain the enjoyment of other human rights.

5. There are several historical examples of Member States ratifying international instruments on human rights while lacking the genuine will to take the necessary measures for their implementation. One of them is the former German Democratic Republic, which, by ratifying the International Covenant on Civil and Political Rights (ICCPR) on 8 November 1973, took upon itself the obligation to respect, among others, the right to privacy (article 17), while maintaining a surveillance regime known for its widespread and systematic violations of the privacy of a large number of its citizens.

6. Regrettably, the Special Rapporteur often finds similar contradictions today: while most Member States unequivocally commit themselves to protecting the right to privacy, many are acting in ways that increasingly put it at risk, by employing new technologies that are incompatible with the right to privacy, such as, in certain modalities, Big Data and health data, infringing upon the dignity of its citizens based on gender or gender identity and expression, as well as by arbitrarily surveying their own citizens.

7. The right to “self-determination”, proclaimed in article 1.1 of ICCPR, allows all peoples to determine their political status and freely pursue their development. Similarly, all basic liberties in ICCPR, including the right to freedom of movement (Article 12) or the right to freedom of association (Article 22), the right to freedom of religion (Article 18), the right to freedom of expression (Article 19) or the right to privacy (Article 17), protect the right of all individuals to their personal autonomy. The right of a citizen to choose what, when, where and how to be, whom to be with and what to think and say are part of the inalienable rights that countries have agreed to protect within the ICCPR.

8. The right to privacy is integral to discussions about personal autonomy. As early as 1976 Paul Sieghart identified the following links between privacy, information flows, autonomy and power:

*“in a society where modern information technology is developing fast, many others may be able to find out how we act. And that, in turn, may reduce our freedom to act as we please – because once others discover how we act, they may think that it is in their interest, or in the interest of society, or even in our own interest to dissuade us, discourage us, or even stopping us from doing what we want to do, and seek to manipulate us to do what they want to do”.[[3]](#footnote-4)*

9. A position which the Special Rapporteur linked to privacy in the following way “Shorn of the cloak of privacy that protects him, an individual becomes transparent and therefore manipulable. A manipulable individual is at the mercy of those who control the information held about him, and his freedom, which is often relative at best, shrinks in direct proportion to the extent of the nature of the options and alternatives which are left open to him by those who control the information”[[4]](#footnote-5)

10. This is why privacy is so closely linked to meaningful personal autonomy. Infringing upon privacy is often part of a system which threatens other liberties. It is often carried out by State actors to secure and retain power, but also by non-State actors, such as individuals or corporations wishing to continue to control others. This is why in many cases the Special Rapporteur’s mandate must consider how violations of the right privacy are linked to other violations.

 Privacy as a qualified right and the standard of necessity in a democratic society

11. The right to privacy is not an absolute right but a qualified right. It may be limited but always in a very carefully delimited way. According to the standard established in ICCPR’s article 17, interferences with the right to privacy are only permissible under international human rights law if they are neither arbitrary nor unlawful. The Human Rights Committee explained in General Comment 16 that the term “unlawful” implies any interference has to be envisaged by the law, and the law itself must comply with the provisions, aims and objectives of ICCPR. The concept of arbitrariness, according to the Human Rights Committee guarantees that “even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances”.

12. In its general comment No. 31 on the nature of the general legal obligation on States parties to the Covenant, the Human Rights Committee provides that States parties must refrain from violation of the rights recognized by the Covenant, and that “any restrictions on any of [those] rights must be permissible under the relevant provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights.” The Committee further underscored that “in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.”

13. The term “necessary in a democratic society” is explicitly cited in three articles of the ICCPR: Article 14 – (Right to a free trial), Article 21 (Freedom of Association) and Article 22 (Freedom of Assembly) but not in Article 17.

14. Article 8 of the European Convention of Human Rights (ECHR) is explicit as to the nature of the qualification:

*2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

15. Democracy was proclaimed as part of the essential context for the enjoyment of human rights in the 1948 Universal Declaration of Human Rights, where the concept of “the general welfare in a democratic society” appeared in Article 29. The interplay between the authors and signatories of the ECHR adopted in 1950 and the authors of the ICCPR continued for the best part of 15 years until the latter’s launch in 1966. The concept of necessary in a democratic society is present in at least six articles of the ECHR including Article 8 cited above, then transposed into the ICCPR and best exemplified by Article 22(1):

*“No restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others.”*

16. Article 22, however, relates to freedom of assembly and not to the right to privacy. It is for historians examining the development of UDHR and the ICCPR to explain why the wording “necessary in a democratic society” is explicit in Articles 14, 21 and 22 and not in Article 17, but the Special Rapporteur must reasonably apply the same standard i.e. that the right can only be qualified by measures provided for by law (Article 17(2)) and that such measures must be necessary in a democratic society by way of an interpretation of “arbitrary or unlawful interference” consistent with Articles 14, 21 and 22 of the ICCPR.

17. This interpretation is consistent with the resolution of the Human Rights Council of March 2017[[5]](#footnote-6) reaffirming that “States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality”, reflecting the terms used in the jurisprudence of the Human Rights Committee[[6]](#footnote-7).

18. The essential, four-fold test is then that any legitimate infringement of privacy cannot be: a) arbitrary and must be provided for by law; b) for any purpose but for one which is necessary in a democratic society; c) for any purpose except for those of “national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others”; and, d) the measure must be proportionate to the threat or risk being managed.

19. The dual tests of “necessity” and “necessity in a democratic society” are essential ones for any measure taken by a Member State which may be held to infringe privacy. They must also be taken into account when examining infringements of other rights whose exercise depends on the right to privacy.

20. The context for privacy and the links between autonomy, privacy and necessary measures in a democratic state explain why the Special Rapporteur is prioritizing States with solid democratic institutions and safeguards, as those are the contexts where his intervention is more likely to have a positive impact on the enjoyment of the right to privacy. In countries where democratic safeguards are weaker, he is seeking to identify opportunities to intervene positively.

21. During 2019-2020, the Special Rapporteur will be focussing further on Africa, Asia and South America, with one visit scheduled in each of those regions; but he will continue to monitor the situation in other countries with the assistance of civil society amongst others. This is not insensitivity to the experiences of privacy in other regions of the world. It is not possible to investigate these experiences in the detail or manner that the Special Rapporteur would wish. This is on account of three factors: time, resources and opportunity to carry out meaningful investigations on the ground. Thus, the Special Rapporteur will continue to monitor those States where the rule of law is replaced by the ‘rule by law’ and where the law becomes an instrument of regime control and oppression. He will assess the creation of cybercrime legislation in the Middle East and North Africa region, which may be posing a risk to the enjoyment of the right to privacy.[[7]](#footnote-8)

 Privacy, technology and other human rights from a gender perspective

22. This report presents the first results of the mandate’s ongoing work on Privacy and Gender. Within the Taskforce on ‘Privacy and Personality’, work will continue on the link between privacy and equality of genders regardless of form or expression. In addition to consultation on the report in Annex 2, the Special Rapporteur plans to dedicate more attention over the next three years to this area, including the links between privacy, autonomy and the male guardianship system present to varying degrees in a number of countries.

23. Member States wishing to participate in consultations on ‘Privacy and Gender’ should register their interest by 31 March, 2019.

 Privacy and health data

24. This report also provides the mandate’s continuing work on Privacy and Health Data. Like the Gender work, there are major emerging issues such as genetics, genome research and biobanking. A question before the Special Rapporteur is whether it is necessary and proportionate for the entire population of a given country to have its DNA data collected. The Special Rapporteur’s mandate will be engaging about these with States legislating such measures.

25. The Taskforce on Health Data has identified issues ranging from matters concerning Indigenous Data Sovereignty, prisoner populations, forensic databases, 'Smart' implanted health devices devices/prostheses that transmit ongoing real life data back to companies and others, which positions the 'body as data' and subject to use in legal proceedings, and artificial intelligence/machine learning and automatic processing. These matters will be explored in consultations during 2019.

 III. Security and surveillance

26. The Special Rapporteur’s mandate arose from the international furore surrounding the revelations by Edward Snowden about the activities of intelligence agencies, especially concerning national security protection.

27. To reinforce privacy safeguards in the intelligence field, the Special Rapporteur initiated the International Intelligence Oversight Forum (IIOF) in 2016 (Romania), 2017 (Brussels) and 2018 (Malta). Following IIOF2018, the Special Rapporteur reports:

1. Recent regional initiatives such as the EU’s General Data Protection Regulation[[8]](#footnote-9) (GDPR) (effective 25 May 2018) and the EU’s Police Directive[[9]](#footnote-10) (effective 6 May 2018), while important, are insufficient for extending privacy protection to the field of national security, including the oversight of intelligence activities undertaken for national security purposes.[[10]](#footnote-11)
2. The modernisation of Convention 108[[11]](#footnote-12), a recent global initiative formally launched on 10 October 2018, in which 70 of the UN’s 193 member states have participated, is commended for Article 11 with its high-level set of principles and safeguards which, unlike GDPR, are also applicable to activities undertaken for national security purposes.

28. The Special Rapporteur’s 2018 report to the General Assembly recommended to all UN Member States to adhere to Convention 108+. In the context of intelligence oversight and national security activities which may be privacy intrusive, the immediate deployment by UN Member States of the standards and safeguards outlined in Convention 108+, Article 11, is appropriate for the protection of the fundamental right to privacy.

29. These key safeguards and standards, particularly of proportionality and necessity, have informed the reasoning of two landmark judgements of the European Court of Human Rights during 2018, both of which are closely related to the activities of intelligence services: Centrum for Rattvisa vs. Sweden (19 June 2018) and Big Brother Watch and others vs. UK (13 September 2018).

30. These judgements can potentially have a worldwide impact given the wide membership of the Council of Europe, with 47 Member States, and the global reach of intelligence services from the region.

31. The Special Rapporteur supports the strict application of the tests of proportionality and necessity in a democratic society as an important benchmark with global repercussions. The intelligence agencies in other regions may be influenced by the growingly strict standards applied in Europe. Thus, intelligence analysis containing personal information and other personal data transferred from and to Europe needs to come under correspondingly strict oversight to ensure that these privacy-respectful standards are upheld in Europe and serve as a possible good practice and model worldwide.

32. It is important to note the qualifier, “a democratic society”, is a fundamental part of the test when evaluating the legal protections afforded in any UN Member State. A number of new technologies, especially the Internet, smartphones, Big Data analytics, wearables, smart energy, smart cities, etc. render individuals and communities more vulnerable to surveillance by Governments in corporations in their country, as well as by the intelligence agencies of foreign States and corporations.

33. The potential for States to use new technologies in this way is a significant risk to privacy and other human rights such as freedom of expression, freedom of association and freedom of religion or belief. The discrete and cumulative effects of these technologies gives the State the ability to closely profile and monitor the behaviour of individuals in new ways and to an unprecedented extent.

34. These technologies may be used to undermine human rights and democracy. Democracy may be an imperfect mechanism but historically, it has provided the best eco-system possible for nurturing human rights. Hence impacts upon democracy are a key base metric against which privacy-intrusive measures need to be evaluated.

35. The Special Rapporteur will continue to implement its global mandate in cooperation with all Member States, even if he is aware that the success of his cooperation and, ultimately, the respect for the right to privacy, is likelier in those countries that enjoy solid democratic institutions and safeguards.

36. Throughout 2018, a key concern was what happens to intelligence analysis containing personal data once those are shared by the intelligence service or law-enforcement agency of one country with those of another country. Are the data, and thus the privacy of the individuals concerned, protected by the same standards in the receiving state as those upheld in the transmitting state? The importance of this warrants action as recommended.

37. On 14 November 2018 five oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland, all parties to Convention 108 and therefore bound by its provisions imposing constraints on the use of personal data for national security purposes, issued a joint statement concerning a potential oversight gap and ways to tackle this risk, when overseeing international data exchange by intelligence and security services.[[12]](#footnote-13) This document is an important and welcome development brought to the attention of the international community.

38. Participants in the IIOF2018 considered that initiative as an important parallel development to the establishment the Five Eyes Intelligence Oversight and Review Council (FIORC) of the agencies responsible for the oversight of intelligence within the “Five Eyes Alliance”: Australia, Canada, New Zealand, United Kingdom and United States. The Special Rapporteur welcomes the establishment and activities of FIORC, especially given the location and global reach of the five states which are part of that Alliance. Each of these five states, since 2013, has introduced legislative reform to reinforce the oversight and privacy safeguards related to intelligence activities in the national security and other sectors. The reforms of some of these states have been more comprehensive than others; the latest legislation in Australia, for instance, has been identified by the mandate holder as a cause of concern from a privacy protection point of view.[[13]](#footnote-14)

39. The United Kingdom’s Investigatory Powers Commissioner’s Office (IPCO) issued a statement[[14]](#footnote-15) welcoming the declaration by the oversight agencies of Belgium, Denmark, the Netherlands, Norway and Switzerland. IPCO has the potential and perhaps even a special responsibility inherent to its geographical location, of providing a bridge between continental European oversight agencies and those collaborating within FIORC.

40. The Special Rapporteur will facilitate and support this, and other initiatives, to the extent that they lead to the embedding of international human rights standards and safeguards relating to the exchange of personal information between the intelligence services and law enforcement agencies of one country with those of another.

41. The oversight of intelligence activities was the main focus of the intervention of the Special Rapporteur in the proceedings of the European Data Protection Board when considering the adequacy of Japan’s domestic law and safeguards. The Special Rapporteur’s submissions and evidence were discussed at the debate which led to the rejection[[15]](#footnote-16) on 5 December 2018, for a period, of an adequacy finding regarding Japan.

42. As indicated, in September 2018 the ECtHR found 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 for examination, and to inadequate safeguards for selection of “related communications data” for examination.[[16]](#footnote-17)

1. 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.
2. It further found that the regime for sharing intelligence with foreign governments did not violate either Article 8 or Article 10.

43. 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.

44. This development highlights the importance of detailed and effective safeguards – legal and procedural - in domestic law and within the practices of intelligence agencies and their oversight authorities.

45. During the Special Rapporteur’s official visit to Germany in November 2018, good practices in the exercise of bulk powers were debated and a related compendium of such good practices developed by the Stiftung neue verantwortung (Annex 5) is recommended for the consideration of States.

 Recommendations

46. The Special Rapporteur recommends:

47. The incorporation by UN Member States into their domestic legal system of the standards and safeguards set out in Convention 108+ Article 11, for the protection of the fundamental right to privacy, especially:

1. the creation of legal certainty by ensuring that any and all privacy-intrusive measures, even for the purposes of national security, defence and public safety as well as the prevention, investigation and prosecution of crime are provided for by laws which are the subject of proper public consultation and parliamentary scrutiny;
2. the establishment of the test of “a necessary and proportionate measure in a democratic society” as the key metric which internal compliance units within intelligence and law enforcement agencies need to apply to any privacy-intrusive measure and against which the actions of such agencies will be measured and held accountable by independent oversight authorities and courts within the competent jurisdiction;
3. the establishment of one or more independent oversight authorities empowered by law and adequately resourced by the State in order to carry out effective review of any privacy-intrusive activities carried out by intelligence services and law-enforcement agencies.

48. The adoption of the principle “If it’s exchangeable, then it’s *oversightable*”[[17]](#footnote-18) in relation to any personal information exchanged between intelligence services and law enforcement agencies within a country, and across borders;

1. All UN Member States should amend their laws to empower their independent authorities entrusted with oversight of intelligence activities, to specifically and explicitly, oversight of all personal information exchanged between the intelligence agencies of the countries for which they are responsible.
2. Whenever possible and appropriate, the independent oversight authorities of both the transmitting and the receiving States should have immediate and automated access to the personal data exchanged between the intelligence services and/or law enforcement agencies of their respective States;
3. All UN Member States should amend their legislation to specifically empower their national and state Intelligence Oversight Authorities to have the legal authority to share information, consult and discuss best oversight practices with the Oversight Authorities of those States to which personal data has been transmitted or otherwise exchanged by the intelligence agencies of their respective States;
4. When an intelligence agency transmits intelligence analysis containing personal information or other forms of personal data received from another State to a third State or group of States, this latter exchange should be subject to those States’ intelligence oversight authorities.

49. The competent authorities in Member States when contemplating the use of bulk powers for surveillance, should first examine, then prioritise and adopt to the greatest possible extent, the measures for introducing the good practices that are recommended in the compendium of Stiftung Neue Verantwortung, November 2018[[18]](#footnote-19) in addition to applying the criteria for deployment and safeguards adopted by the ECtHR in Big Brother Watch et al. of September 2018.

 IV. The right to privacy: a gender perspective

50. The Human Rights Council[[19]](#footnote-20) and the General Assembly[[20]](#footnote-21) have called on States “to further develop or maintain, in this regard, preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular adverse effects on women, as well as children and persons in vulnerable situations or marginalized groups.”

51. In 1994, the Human Rights Committee in Toonen v. Australia determined a violation of the right to privacy by criminalising consensual same-sex relations between adults. In 2017, the Committee reiterated the right to privacy covers gender identity.[[21]](#footnote-22)

52. While not an absolute right, the right to privacy is essential to the free development of an individual's personality and identity. It is a right that both derives from and conditions the innate dignity of the person, and facilitates the exercise and enjoyment of other human rights.[[22]](#footnote-23) It is a right not restricted to the public sphere.

53. The right to privacy, as a necessary precondition for the protection of fundamental values including liberty, dignity, equality, and freedom from government intrusion, is an essential ingredient for democratic societies, and requires strong protection.[[23]](#footnote-24) The Human Rights Council has adopted resolutions highlighting the interdependent and mutually reinforcing relationship between democracy and human rights.[[24]](#footnote-25)

54. The Special Rapporteur integrates a gender perspective throughout the mandate.[[25]](#footnote-26) Following three successful ‘Privacy, Personality & Information Flows’ regional consultations, an online consultation ‘Gender issues arising in the digital era and their impacts on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics’ was undertaken.

55. Annex 2 is a compilation of submissions received by the mandate of the Special Rapporteur as well as ancillary research and, save for the Recommendations, does not necessarily represent the views of its lead author, Dr Elizabeth Coombs, Chair, UN Special Rapporteur Thematic Action Stream ‘Privacy and Personality’, nor those of the Special Rapporteur, Professor Joseph A. Cannataci. **The full first report is at Annex 2.**

 Thematic Action Stream Privacy and Personality

56. Submissions on this topic received by the Special Rapporteur advocated for an intersectional analysis of economic forces, class, religion, race and gender to identify areas of interest outside the mainstream,[[26]](#footnote-27) and recognition of the interdependency between the right to privacy and democracy.[[27]](#footnote-28)

57. It was reported that individuals’ experience of digital technologies and privacy is affected by their gender, along with factors such as ethnicity, culture, race, age, social origin, wealth, economic self-sufficiency, education, legal and political frameworks.[[28]](#footnote-29) The right to privacy was said to be particularly important for those who face inequality, discrimination or marginalisation based on their gender, sexual orientation, gender identity, sex characteristics or expression. The internet with its reach and relative anonymity has opened new ways for the interaction and mutual support of LGBTQI.

58. Submissions recognized that digital technologies have enormous effect upon privacy by amplifying the experiences of the non-digital world. The benefits of digital technologies were reported as unequally available due to structural inequity and discriminatory gender norms that fall heavily upon women, non-binary gender and cis-normativity individuals, the poor, and minority religious or cultural communities. Cybermisoginy [[29]](#footnote-30) and general cyber-abuse of individuals of non-binary gender are enabled by new technologies[[30]](#footnote-31) with infinitely far greater reach, durability, and impact than previously.

59. Submissions were strongly of the view that this does not need to be the case; digital technology can provide equality in the enjoyment of the right to privacy.

60. Submissions recognised the benefits of smart devices, apps, search engines and social media platforms but also their capacity to breach users’ privacy according to gender. LGBTQI youth for example, use the internet more frequently to engage in social media and networking than non-LGBTQI peers, and are more likely than non-LGBTQI youth to be bullied or harassed online (42% vs. 15%).[[31]](#footnote-32)

61. Despite the benefits of digital technologies,[[32]](#footnote-33) those most at risk were seen as women, girls, children, LGBTQI individuals and communities[[33]](#footnote-34) especially transgender individuals, activists, gay teachers, human rights defenders, sex workers, and women journalists.

62. LGBTQI individuals can experience also specific, unique risks such as ‘outing’, and abuse directly related to their gender identity.[[34]](#footnote-35)

63. It has been found in Canada, that social media, while enabling social connections for women and girls, amplifies societal norms by intensifying commercial surveillance; reinforcing existing societal norms, and increasing surveillance by family members and peers.[[35]](#footnote-36)

64. Fake accounts on LGBTI dating apps and other social media platforms were reported as being used by State and non-State actors to entrap gay men, arrest or subject them to cruel and degrading treatment, or for blackmail.[[36]](#footnote-37)

65. It was reported the media, including new media, publish the personal information of LGBTQI people and of human rights defenders, putting their safety at risk.[[37]](#footnote-38)

66. The internet not only creates contemporary stories but can carry forward in perpetuity those of the pre-digital era, and associated violations of privacy.[[38]](#footnote-39)

67. Some submissions addressed the recognition of gender identity, autonomy and bodily integrity and its expression in relation and expressed their concern for inadequate privacy management in the context of name and gender changes in identity documents.[[39]](#footnote-40) Ordinary, everyday activities requiring identity documents such as travel, banking, medical appointments frequently impose deeply embarrassing and distressing privacy incursions for transgender individuals not experienced by individuals of binary genders.

68. The ECtHR has found States in violation of Article 8 of the ECHR for the gender recognition procedures that violate the right to privacy of transgender people.[[40]](#footnote-41)

69. The online availability of public records, judicial notices and decisions concerning gender identity were a privacy concern particularly in combination with Big Data and search engines capacity.[[41]](#footnote-42)

70. For intersex individuals, privacy intrusions can commence literally from birth with sex reassignment surgery and hormone treatment to assign a certain sex. ‘Normalising’ surgery on intersex infants can impact on human rights, including the right to privacy, as it infringes on the right to personal autonomy/self-determination in relation to medical treatment. Countries were reported to be responding in a variety of ways.[[42]](#footnote-43)

71. Submissions referred to the growing body of international, regional and national research on digital violence based on gender, including that of the Special Rapporteur on violence against women.

72. Digital technology and smart devices provide almost limitless ways to harass and control others.[[43]](#footnote-44) Technologically facilitated violence combines issues of gender inequality, sexualised violence, internet regulation, internet anonymity, and privacy.[[44]](#footnote-45)

73. The phenomenon of 'revenge porn' – the sharing private sexual images and recordings of a person without consent to cause harm –, is widely known as a form of online abuse. Research in Australia has found males and females are equally likely to experience image-based abuse, while people who identified as lesbian, gay or bisexual were more likely to be victims (36%) than heterosexuals (21%).[[45]](#footnote-46)

74. Domestic violence increasingly involves using smart home devices directed at women and dependents[[46]](#footnote-47) which enable new ways to infringe privacy, reduce autonomy and self determination at home,[[47]](#footnote-48) or in communications.[[48]](#footnote-49) Sometimes legal protections are inadequate[[49]](#footnote-50) or there is a lack of police enforcement of breaches.[[50]](#footnote-51)

75. Cybermisogyny has been manifested on digital platforms.[[51]](#footnote-52) Twitter was reported as the main platform for promoting hate campaigns against women and dissemination of sexual content, while Facebook sees most attacks on women who defend their rights.[[52]](#footnote-53)

76. Invasions of privacy and online violence are higher for men who do not conform to conventional masculine stereotypes, and for lesbian, gay, or bisexual people.[[53]](#footnote-54)

77. The gendered experiences of privacy also affect enjoyment of other rights with, for example, women also suffering online censorship and profiling in campaigns targeting female activists and journalists.[[54]](#footnote-55)

 Thematic Action Stream ‘Security and Surveillance’

78. Surveillance, unless undertaken lawfully, proportionately and necessarily represents infringements upon the human right to privacy. Gender, race, class, social origin, religion, opinions and their expression can become factors in determining who is watched in society, and make certain individuals more likely to suffer violations of their right to privacy.[[55]](#footnote-56)

79. In a number of countries, gender bias is evident in the higher degree of surveillance of those who identify as members of the LGBTQI groups.[[56]](#footnote-57) State surveillance of the LGBTQI community has been facilitated in some countries through legislation. An example given was the Anti-Cybercrime Law enacted in Egypt in 2018.[[57]](#footnote-58)

80. While State surveillance is generally presented as targeting males,[[58]](#footnote-59) counter-terrorism measures have been said to disproportionately affect women and transgender asylum-seekers, refugees and immigrants.[[59]](#footnote-60)

81. Women can expect that nearly every detail of their intimate lives will be subject to multiple forms of surveillance by State as well as private actors, from domestic violence to sexual objectification and reproduction.[[60]](#footnote-61)

82. Major platform providers now provide identity management via online identity authentication. Websites, apps and services now require login details, and accept identity credentials as authentic following logon via Facebook or Google accounts.[[61]](#footnote-62) Facebook has 60% of this ‘social log on’ market.[[62]](#footnote-63) This provides access to vast amounts of information to compile profiles, enabling insights in which gender is a variable, into the behaviours of individuals, families, groups and communities.

 Thematic Action Stream ‘Big Data and Open Data’

83. The growth in the collection, storage and manipulation of data has increased the possibilities of privacy breaches, which can have different consequences according to gender.

84. Data processing can embed biases relating to gender roles and identities, particularly as data modelling for social intervention increasingly transcends the individual to focus on groups or communities.[[63]](#footnote-64)

85. Data analytics resulting in inferences being made about individuals or groups according to gender, and which lead to discrimination, are contrary to human rights law.

 Thematic Action Stream ‘Health Data’

86. A particular concern for LGBTQI people is the non-consensual sharing of health data, particularly HIV status.[[64]](#footnote-65) The Grindr app for example, was found to contain trackers and share personal information, including users’ HIV status, with various third parties.[[65]](#footnote-66)

87. Privacy experiences in health care settings have been found to influence health service usage and consequently possess individual and public health impacts.

88. Fears of humiliation or discrimination from loss of privacy can see transgender individuals avoid health services or restrict their use.[[66]](#footnote-67)

89. Violations of women’s right to privacy during childbirth can be a powerful disincentive to seeking care for subsequent deliveries.[[67]](#footnote-68)

90. Technologies such as Google’s Street View, can affect health service usage by women through concerns about being identified using certain health services.[[68]](#footnote-69)

 Thematic Action Stream ‘Use of Personal Data by Corporations’

91. There is growing recognition that the private sector has obligations under human rights law as in the Protect, Respect and Remedy Framework proposed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, in 2008 (A/HRC/8/5).[[69]](#footnote-70)

92. Automated decision-making used by digital platforms can produce outcomes affecting genders differently. Legal action, still ongoing, was reported against Facebook for allegedly allowing landlords and brokers to exclude ads being displayed based on the user’s gender.[[70]](#footnote-71)

93. Concern was expressed at the increased number of social media pages and groups promoting violence against women, sexism, and harmful gender stereotypes, and the amount of community pressure it took to have these pages removed.

94. It was reported that it is unknown how the online platforms make decisions following receipt of online violence complaints, the types and number of cases reported by country, or the actions taken. Amnesty International has found that Twitter failed to adequately investigate reports of violence and abuse, and has repeatedly called on Twitter to release “meaningful information about reports of violence and abuse against women, as well as other groups, on the platform, and how they respond to it.”[[71]](#footnote-72)

95. One submission reported positive action by the app Grindr to reduce misuse aimed at entrapment of gay men.[[72]](#footnote-73) However, the common response of digital platforms (Facebook, Twitter, media, etc.) with respect to victims of online gender-based violence was reported as impunity and opacity, with victims generally feeling abandoned.[[73]](#footnote-74)

96. Reports of harm to individuals arising from gender-based technological infringements of the right to privacy included serious, well-documented effects, from fraud, loss of employment and educational opportunities, restrictions on freedom of movement and freedom of association, to dress as one wishes, interference with parenting abilities, loss of reputation and general confidence, violence even death, imprisonment amongst others.[[74]](#footnote-75)

97. Experiences of privacy breaches are not homogeneous; infringements can result in increased domestic violence for women, and discrimination for LGBTQI people.[[75]](#footnote-76)

98. Invasions of privacy are invasions of the human personality itself and have larger societal impacts. The extreme forms of online abuse and invasions of personal and familial privacy inflicted upon high-profile women, discourage girls and women from participating in public roles thereby undermining women’s right to participate in public affairs and affecting representativeness of democratic institutions.[[76]](#footnote-77)

99. Submissions indicated good practices that protect privacy from a gender perspective range from legislative reform; gender neutral, evidence-based policy frameworks; Courts decisions; participation of civil society organizations and benefitting from their experience; gendered privacy community programs; to educational resources.

100. Good practices to address sexual orientation and gender identity privacy issues were seen to be encapsulated in the Yogyakarta Principles+10.[[77]](#footnote-78)

 Conclusions

101. **The Universal Declaration of Human Rights calls on “every individual and every organ of society” to promote and respect human rights.[[78]](#footnote-79) States, companies, religious bodies, civil society, professional organisations and individuals all have important roles to play.**

102. **The confidence of individuals to share ideas and to assemble is also fundamental to the health of societies and democracy. The loss of privacy can lead to a loss of this confidence including confidence in Government and institutions established to represent the public interests, withdrawal from participation, which can adversely impact and undermine representative democracies.**

103. **While privacy rights are not costless, or free of risks to governments, the challenges are outweighed by our collective interest in democracy. The right to privacy for women, as well as children and individuals of diverse sexual orientations, gender identities, gender expressions and sex characteristics, is critically important for all of the reasons outlined above and reported in submissions.[[79]](#footnote-80)**

104. **Gender based breaches of privacy are a systemic form of denial of human rights; discriminatory in nature and frequently perpetuating unequal social, economic, cultural and political structures.**

105. **Addressing gender based incursions into privacy requires frameworks at international, regional and domestic levels.**

106. **States, in preventing gender based privacy invasions, need to actively protect privacy in policy development, legislative reform, service provision, regulatory action, support to civil society organizations, and educational and employment frameworks, and using the experiences of females, males, transgender women and men, and intersex people, and others who identify as outside the gender binary and cis-normativity.**

107. **The protection of personal information online should be a priority with the adoption of provisions equivalent or superior to the GDPR, for countries that are not party to the Regulation. Gender should be a key consideration for the development and enforcement of privacy protection frameworks.**

108. **Transparency is needed in how private companies use personal data of users,[[80]](#footnote-81) and respond to reports of online harassment. Greater gender diversity among those shaping online experiences is important for making products and platforms safer, more socially-responsible and accountable.**

 Summarised recommendations

109. **United Nations bodies:**

 All relevant special procedures and other mechanisms of the Human Rights Council and human rights treaty bodies should integrate gender and privacy into the implementation of their respective mandates.

110. **Member States:**

(a) Adopt an intersectional approach that recognises the specific benefits, experiences and threats to the right to privacy according to gender, and overarching privacy and human rights principles.

(b) Undertake an assessment of their legal frameworks for prevention and punishment of privacy breaches based on gender, against relevant laws and treaties at global, regional and national levels.

(c) Adopt policies, legal and regulatory frameworks providing comprehensive protection for the use and development of secure digital communications.

(d) Promote meaningful internet access and bridge any digital gender divide.

(e) Take all necessary legislative, administrative and other measures to prevent, investigate and punish breaches of privacy perpetrated on the basis of the gender, sexual orientation or gender identity.

111. **Corporations:**

 Implement the ‘UN Guiding Principles on Business and Human Rights’ and avoid infringing on the human rights of all persons affected by their practices, with effective consideration of the gender-specific impact of their activities.

 V. Privacy and health data

112. Health is the most important fundament of everybody’s life. Changes in health status always imply changes in life, many forever. All of us are, at some point in our lives, patients. Situations arise too where our health status has a decisive impact on our life. We all have therefore, very legitimate interests in our dignity and autonomy being protected by the highest available standards in health-data related scenarios.

113. The relationship between a data subject as a patient and a healthcare professional is highly sensitive: patients are, by definition, in a vulnerable position. The situation can be distressing, dangerous and possessing lifelong consequences. The role of a healthcare professional requires accurate and complete patient information, and processes to use this information in a standardised and transparent manner.

114. The protection of patients (and their genetic relatives) in these moments of existential vulnerability has been subject to legal and ethical considerations and rules for millennia. Principles like medical professional confidentiality, the obligation to establish fully informed consent for treatment, proper documentation of treatment and free choice of treating physician, are some of the fundamental outcomes of centuries of thought on how best to protect the rights of patients.

115. Every medical situation produces personal data. This data is important for treatment purposes and needs to be processed following the highest legal and ethical standards. Digitalisation is producing more and more medical data, which will be increasingly shared between healthcare professionals as they become more and more specialised, and likewise required to collaborate following highest quality standards.

116. Data processed for health purposes is also important for many other stakeholders and for many different purposes outside the possibly life-changing relationship between the healthcare professional and the patient. First, the patient her/himself has a legitimate interest in controlling this data, and can consent to it being shared during and after treatment. Second, other stakeholders such as patients’ relatives, institutions to which the patient has an obligation, for example social security institutions, insurance companies or employers, and other, more indirect stakeholders such as medical researchers and the general public who rely upon an efficient and effective health system, might have an interest to obtain access to that data.

117. The tensions between these different stakeholders interests and needs pose very challenging legal and ethical issues.

 Critical issues:

 Informed consent

118. Generally, patients have the right to agree to treatment after being properly informed about possible risks, side-effects and alternatives of their treatment. The requirements of the consent procedure for medical treatment and medical research are subject to intense, detailed and controversial regulations.

119. Those regulations are not yet harmonized with the requirements on information provided to data subjects and validity criteria of informed consent as a legal basis for data processing. Criteria for informed consent are often vague and contradictory.

120. Data subjects can feel overwhelmed with different consent procedures at a time when the protection of their data is not their immediate concern. Nor are they always willing and able to understand fully all implications of the different consents they give. Consent for tests, for treatment, for medical research and for data processing are not clearly distinguished and often have different and possibly conflicting scopes of regulation and different supervisory authorities. This puts patients and their relatives under serious stress, undermining their capacity to freely provide an informed consent.

 Secondary use for medical research

121. Personal data needs to be collected and processed as a basis for medical treatment. It is then stored for reasons of documentation of treatment, sometimes for decades. This data can often also serve as an important source for medical research. There are important arguments that there is an ethical justification (or even necessity) to further use this data for research in the interest of better outcomes of future patient generations.

122. Research has a different purpose than treatment, requiring a different legal basis for the data processing. The requirements of this second legal basis are very diverse and unclear, as many underlying ethical questions are not clearly described and analysed. In particular, questions include whether this secondary use needs (again) an informed consent of the patient and/or a clearance by a competent ethics committee and/or by supervisory authorities. The issues include personal autonomy arising from bodily privacy and responsibility to the ‘collective good’.

123. If such consent were replaced by another legal basis, further steps need to be taken to protect the data subject’s fundamental rights. Lack of international legislation on the matter leads to situations in which treating physicians need or believe they need an additional informed consent from affected patients – consent which in some cases can no longer be achieved for technical and/or ethical reasons.

 Secondary use for other purposes

124. Medical data is of high value also for other purposes, in particular social security, public health, labour and business. National laws are often silent on data processing for these purposes and it is unclear whether these purposes are ethically and legally justifiable, and which of these secondary uses shall be based either on informed consent or another legitimate legal basis. The purpose binding principle, requiring that secondary use of personal data may only be undertaken for a purpose compatible with the primary purpose is therefore often either ignored or violated.

125. Differences in legislation in this matter lead to a ‘race to the bottom’ in which public services or even businesses reliant on personal health related information are best served by operating in areas with low levels of data protection.

126. The protection of the data subject’s rights – in particular their right to transparency, including information and access – is very difficult as these secondary uses are undertaken by controllers not known to the data subject, and frequently, for unknown purposes.

 Data property as competing means of protection

127. A consequence of the situations described above is that some legal scholars (and even legislators) have started to argue for a data property right, similar to an intellectual property right, that should alleviate sharing of personal and non-personal data. These concepts stand in a very problematic relation to existing fundaments of data protection and require clear reasoning and justification based on evidence-based predictions of the consequences. Currently, the underlying evidentiary and factual matrix is lacking.

 Unclear distribution of responsibilities

128. Medical treatment and research are supervised by regulatory bodies, in particular ethics committees, consisting of different experts and stakeholders, many of them non-lawyers with no specific expertise in data protection.

129. Many of the requirements formulated by these bodies on data processing for treatment and research, however, are data-protection related, such as specific (and often conflicting) requirements on consent procedures, information to be provided to the patient/data subject, the patients’ right to know and not to know, consequences of withdrawal of consent, etc.

130. The regulations proposed by those bodies may conflict with data protection rules, and their supervision may interfere with supervision undertaken by the data protection supervisors and authorities who are exclusively competent for monitoring compliance with data protection, such as independent data protection officers and data protection authorities.

 Unclear scope of applicability: personal, pseudonymized and anonymous data

131. The basic assumption that data protection laws only apply when data is personal, attributed to a particular individual, is very hard to apply in medical scenarios as medical data rarely can be (fully) anonymized. It then remains very unclear which anonymization measure is “good enough” to keep data outside the scope of data protection legislation.

132. This problem is especially difficult when considering if medical data should become part of open access/open data initiatives that require release of (non-personal) data to the public. Data controllers may on the *one* hand be obliged to keep data under their control for protecting anonymity of the data, on the other hand obliged to make data freely accessible while risking re-identification. The lack of clarity may facilitate a de-facto property protection of medical data by data controllers who can – de facto – decide who gets access to data (anonymized by some method) and under which conditions.

133. The Special Rapporteur stated unequivocally in his 2018 report to the General Assembly,: “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.”[[81]](#footnote-82)

 Lack of data portability and lack of digitalisation

134. A lot of medical data is still collected in an analogue format. Anamneses are often random and incomplete and diagnoses can be based on poor data.

135. Digitalisation of medical data, standardisation of formats and processes, as well as minimum criteria for data quality, can assist both patients and health professionals control and responsibly manage health data.

136. States however, tend to establish their own national e-health systems without the participation of citizens and health professionals, and without standardisation. This can make data portability impossible for patients, and reduce their ability to control their medical data without a standardised instrument enabling secure storage and management of their own health data under their own rules.

 Clouds

137. More and more medical information is stored in clouds (like any other data). The consequences are many, inter alia: transfer of personal data across borders with possibly conflicting jurisdictions, lack of control for the patient, and high-impact security incidents that may affect millions.

138. The corresponding minimum requirements for cloud service providers however are not harmonized, triggering incentives to operate from areas with a low level of data protection.

 Lifestyle products/wearables

139. A lot of health-related data is no longer (directly) disease related and is now collected for purposes very different from treating or preventing health conditions. In particular, lifestyle-related apps and gadgets (“wearables”) collect a lot of health related data with or without the data subjects’ informed consent. They have become more and more popular although the legal basis for the collection and requirements for their further use are not clearly defined, no minimum transparency standards apply and the purpose binding principle is not sufficiently taken into consideration.

 Security and safety

140. Although health related data is highly sensitive, and faults in devices processing health-data can be potentially life-threatening, there are no clear and specific rules on minimum security and safety standards. The consequence is a series of security and safety incidents with heavy impacts for the data subjects affected.

 Data breach notification, lack of transparency

141. Although data breaches affecting medical data occur on a regular basis, there are no standards on when and how data the subjects concerned, as well as the general public, need to be informed on these incidents. This situation lacks transparency and fails to meet the accountability expected by the public.

 Access to justice

142. Non-compliance with data protection legislation can have life-threatening impact on data subjects. However, data protection legislation has lacked effective instruments for enforcement from its inception. Unclear rules on competence between data protection authorities, courts, ombudspersons, data protection officers and medical supervisory authorities; uneven distribution of information and knowledge; complexity of the regulatory framework; etc. make it very hard for the data subject affected to enforce their rights.

143. This lack of enforcements leads to a lack of trust in the medical system and, in particular, the relationship between patient and health-care professional, which can have a detrimental effect every patient. Minimum standards formulated on an UN-level are therefore of utmost and strategic importance.

 Next Steps

144. The Special Rapporteur intends to provide guidance for regulating health-related data in order to promote the protection of the right to privacy and to the protection of personal data provided for in Article 12 of the Universal Declaration of Human Rights and article 17 of the ICCPR.

145. Annex 3 contains a Draft guidance enumerating guiding principles concerning data processing of health-related data and which emphasises the importance of a legitimate basis of data processing of health-related data, covering the issues described above. The purpose of the guidance is to, first, serve as a common international baseline for minimum data protection standards for health related data for its implementation at the domestic level. Second, to be a reference point for the ongoing debate on how the right to privacy can be protected in the context of health data, further developed in conjunction with other human rights (such as freedom of speech, to a fair trial and protection of property) in a context where medical data is processed and shared globally.

146. The text, currently before Taskforce experts in the draft version attached (Annex 3), is open to public consultation as a draft for written comments by 11th May 2019, followed by a public stakeholder meeting in Strasbourg on 11-12 June 2019. Member States wishing to participate in this meeting should register their interest by 11 May.

147. A final recommendation of the drafting group, using stakeholders’ input, will be provided to the Special Rapporteur and incorporated in his 2019 Annual Report to the General Assembly in late 2019.

 VI. Privacy metrics

148. The Special Rapporteur is also consulting on “Metrics For Privacy”, and a first draft is appended to this report (Annex 4). Individuals, civil society and governments are invited to send their comments and suggestions by 30th June 2019. The intention would be to use such metrics as a standard investigation tool during country visits, both official and non-official.

 Acknowledgements

149. The Special Rapporteur acknowledges the support of the Office of the High Commissioner for Human Rights in Geneva. The assistance of UN staff is gratefully acknowledged

150. The Special Rapporteur has sourced extra-mural funding and volunteer assistance from the Department of Information Policy and Governance, University of Malta, and the Security, Technology & e-Privacy Research Group, University of Groningen, Netherlands, and from Australia, UNSW Sydney; the Optus Macquarie University Cyber Security Hub; University of Technology; Allens Hub UNSW Sydney; Melbourne University; La Trobe University and Edith Cowan University.

151. The Special Rapporteur would like to particularly recognise the efforts and support of non-governmental organizations, small and large, local, national and international. The mandate could not be undertaken successfully without their assistance around the world.

152. The Special Rapporteur would like to thank the many Government agencies, regulatory and professional bodies who have assisted his mandate, and the Taskforce Chairs, Taskforce members, and voluntary secretariat support.

 Annexes

 I. International keynote addresses

The annex is available on the following link:
<https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex1_Keynotes.pdf>

 II. The human right to privacy: a gender perspective – report on submissions received

The annex is available on the following link:
<https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf>

 III. Privacy and health data – draft guidance opened for consultation

The annex is available on the following link:
<https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf>

 IV. Privacy metrics – consultation draft

The annex is available on the following link:
<https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf>

 V. Good practices on bulk powers

Wetzling, T. and Vieth, K., Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations, Heinich-Böll-Stiftung 2018

The annex is available on the following link:
<https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf>

1. \* Submitted after the deadline in order to reflect the most recent information. [↑](#footnote-ref-2)
2. 18 letters and 6 press releases were jointly issued with other Special Rapporteurs. [↑](#footnote-ref-3)
3. Sieghart P., Privacy and Computers, Latimer, London, 1976 p.24 [↑](#footnote-ref-4)
4. Cannataci Joseph A., Privacy & Data Protection Law, Norwegian University Press, 1987, p60. [↑](#footnote-ref-5)
5. (A/HRC/RES/34/7, par. 2, adopted by consensus on 23 March 2017, 34th Session of the Human Rights Council. [↑](#footnote-ref-6)
6. CCPR /C/USA/CO/4, para. 22. [↑](#footnote-ref-7)
7. Wafa Ben Hassine and Dima Samaro, Restricting cybersecurity, violating human rights: cybercrime laws in MENA region, 10 January 2019, OpenGlobalRights,, last accessed on 10 February 2019 at <https://www.openglobalrights.org/restricting-cybersecurity-violating-human-rights/> [↑](#footnote-ref-8)
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (OJ L 119, 4.5.2016, p. 1) [↑](#footnote-ref-9)
9. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. [↑](#footnote-ref-10)
10. The EU lacks competence in the field of national security, therefore cannot adequately extend privacy protection to activities in this field, including oversight of intelligence activities for the purpose of national security. [↑](#footnote-ref-11)
11. The Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108). [↑](#footnote-ref-12)
12. <https://english.ctivd.nl/documents/publications/2018/11/14/index> [↑](#footnote-ref-13)
13. Submission by the Special Rapporteur to the Australian Joint Parliamentary Committee Intelligence and Security, No. 81. 2018, https://www.aph.gov.au/Parliamentary\_Business/Committees/Joint/Intelligence\_and\_Security/TelcoAmendmentBill2018/Report\_1/section?id=committees%2freportjnt%2f024247%2f26914 [↑](#footnote-ref-14)
14. <https://www.ipco.org.uk/docs/IPCO%20Statement%20re%205%20oversight%20bodies.docx> [↑](#footnote-ref-15)
15. <https://edpb.europa.eu/news/news_en> [↑](#footnote-ref-16)
16. <https://hudoc.echr.coe.int/eng#{"itemid":["001-186048"]}> [↑](#footnote-ref-17)
17. Personal data is exchanged between intelligence agencies located in different states on a regular basis, but it is not necessarily subject to oversight by the independent oversight agencies located in either the state. Moreover, certain legislations effectively prevent such oversight or even consultation about the matter between the independent oversight authorities in the sending and receiving states. States are encouraged to amend their laws to empower their independent oversight authorities to consult with other independent oversight authorities in other states, and follow up on all cases of data exchanged with another state, irrespective of whether they are located in the receiving or sending state, including both raw unprocessed personal data or personal data which is contained in analysis typified by intelligence product. Both types of personal data are exchanged by intelligence agencies and LEAS and both should be subject to independent oversight in both the sending and the receiving state. [↑](#footnote-ref-18)
18. <https://www.stiftung-nv.de/en/publication/upping-ante-bulk-surveillance-international-compendium-good-legal-safeguards-and> [↑](#footnote-ref-19)
19. HRC resolution 34/7 [↑](#footnote-ref-20)
20. UNGA (2014). Right to privacy in the digital age, A/RES/71/199 [↑](#footnote-ref-21)
21. Communication No. 2172/2012 2 December 2011, 17 March 2017, CCPR/C119/D/2172/2012, par. 7.2 [↑](#footnote-ref-22)
22. The General Assembly, the UN High Commissioner for Human Rights and special procedure mandate holders have recognised privacy as a gateway to the enjoyment of other rights (UNGA resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8). [↑](#footnote-ref-23)
23. Canadian Privacy Commissioner, Submission to Innovation, Science and Economic Development Canada in the context of its National Digital and Data Consultations, November 23, 2018: <https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ised_181123/> [↑](#footnote-ref-24)
24. Resolutions 19/36 and 28/14 on “Human rights, democracy and the rule of law” at http://www.un.org/en/sections/issues-depth/democracy/index.html#DHR [↑](#footnote-ref-25)
25. https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx [↑](#footnote-ref-26)
26. For example, APC Submission 2018. [↑](#footnote-ref-27)
27. For example, Privacy Commissioner of Canada, Submission 2018 [↑](#footnote-ref-28)
28. Privacy Commissioner of Canada, 2018, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por\_2016\_12/ [↑](#footnote-ref-29)
29. LEAF 2014, http://www.westcoastleaf.org/our-publications/cybermisogyny/ [↑](#footnote-ref-30)
30. Eastern European Coalition for LGBT+ Equality’s submission, *‘*Gender Perspectives on Privacy in Eastern Partnership Countries and Russia’, 2018; UCL and Privacy International, ‘Gender and IoT’, <https://www.ucl.ac.uk/steapp/research/themes/digital-policy-laboratory/gender-and-iot> [↑](#footnote-ref-31)
31. Holt, D. B., ‘LGBTIQ Teens Plugged in and Unfiltered: How Internet Filtering Impairs Construction of Online Communities, Identity Formation, and Access to Health Information, Santa Clara Digital Commons Law Library Collections, 2009. [↑](#footnote-ref-32)
32. Name withheld Submission 2018 referencing Horres, V. “Online and Enabled: Ways the Internet Benefits and Empowers Women [↑](#footnote-ref-33)
33. Kazakhstan Feminist Initiative “Feminita”, ODRI Intersectional rights, “Stimul” LGBT Group and Transgender Legal Defense Project (Russia), Richard Lusimbo, MPact Global Action for Gay Men’s Health and Rights, Transgender Europe TGEU, Federatie van nederlandse verenigingen tot integratie van homoseksualiteit - COC Nederland, and the International Lesbian, Gay, Bisexual, Trans and Intersex Association ILGA Submission 2018. [↑](#footnote-ref-34)
34. Gender Perspectives on Privacy in Eastern Partnership Countries and Russia by the Eastern European Coalition for LGBT+ Equality [↑](#footnote-ref-35)
35. Steeves, V., and Bailey, J., (2014). Living in the Mirror: Understanding Young Women’s Experiences with Online Social Networking. In Emily van de Muelen (Ed.), *Expanding the Gaze: Gender, Public Space and Surveillance.*Toronto: University of Toronto Press. <https://egirlsproject.ca/>; <http://www.equalityproject.ca/> [↑](#footnote-ref-36)
36. Op cit Kazakhstan Feminist Initiative etal Submission 2018. [↑](#footnote-ref-37)
37. Ibid. [↑](#footnote-ref-38)
38. Osgoode School of Law, confidential submission December 2018. [↑](#footnote-ref-39)
39. Eastern European Coalition for LGBT+ Equality Submission, 2018. [↑](#footnote-ref-40)
40. L. v Lithuania; A.P. (2008), Garcon and Nicot v France (2017) [↑](#footnote-ref-41)
41. Joint submission of Kazakhstan Feminist Initiative et al, 2018. [↑](#footnote-ref-42)
42. https://www.usatoday.com/story/news/nation/2018/08/28/intersex-surgeries-children-california-first-state-condemn/1126185002/ [↑](#footnote-ref-43)
43. Dejusticia Submission September 2018. [↑](#footnote-ref-44)
44. *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, A/HRC/38/47. 2018 [↑](#footnote-ref-45)
45. RMIT University, [*Not Just ‘Revenge Pornography: Australians’ Experience of Image-Based Abuse*](https://www.rmit.edu.au/content/dam/rmit/documents/college-of-design-and-social-context/schools/global-urban-and-social-studies/revenge_porn_report_2017.pdf), May 2017. [↑](#footnote-ref-46)
46. 'Stalked within your own home': Woman says abusive ex used smart home technology against her, CBC, Nov 1, 2018 <https://www.cbc.ca/news/technology/tech-abuse-domestic-abuse-technology-marketplace-1.4864443>; Nellie Bowles “Thermostats, Locks and Lights: Digital Tools of Domestic Abuse” New York Times, June 23, 2018 <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html?smid=tw-nytimes&smtyp=cur>. [↑](#footnote-ref-47)
47. Bowles, N. (2018, 23 June). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. New York Times. www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html [↑](#footnote-ref-48)
48. Mason, C. and Magnet, S., Surveillance Studies and ViolenceAgainst Women, Surveillance & Society 10(2) 2012; APC p13 [↑](#footnote-ref-49)
49. Bowles, Nellie Thermostats, Locks and Lights: Digital Tools of Domestic Abuse, 2018 New York Times <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html> [↑](#footnote-ref-50)
50. Hadeel Al-Alosi, Cyber-Violence:Digital Abuse in the Context of Domestic Violence, UNSW Law Journal 40(4) 2017. [↑](#footnote-ref-51)
51. Op cit LEAF [↑](#footnote-ref-52)
52. Women's Institute of Mexico City; APC Submission 2018. [↑](#footnote-ref-53)
53. Irish Civil Liberties Council [↑](#footnote-ref-54)
54. de Justicia Submission 2018 [↑](#footnote-ref-55)
55. Franks, M.A., Democratic Surveillance, *Harvard Journal of Law & Technology,* Volume 30, Number 2 Spring 2017  [↑](#footnote-ref-56)
56. APC Submission, 2018. [↑](#footnote-ref-57)
57. Joint International Submission, 2018; http://www.loc.gov/law/foreign-news/article/egypt-president-ratifies-anti-cybercrime-law/ [↑](#footnote-ref-58)
58. Privacy International 2017 [↑](#footnote-ref-59)
59. Scheinin, M. 2010 [↑](#footnote-ref-60)
60. Franks, M.A., Democratic Surveillance, *Harvard Journal of Law & Technology,* Volume 30, Number 2 Spring 2017; APC Submission, 2018.  [↑](#footnote-ref-61)
61. The Economist Essay, Christmas Edition, December 2018 [↑](#footnote-ref-62)
62. Ibid. [↑](#footnote-ref-63)
63. Bridges, K.M., The Poverty of Privacy Rights, Stanford University Press, 2017 and Lyon, D. (ed) Surveillance as Social Sorting, Privacy, Risk and Social Organisation, 2003:1 http://www.felfel.is/sites/default/files/2016/Lyon,\_D.\_(2003).\_Surveillance\_and\_social\_sorting%26\_computer\_codes\_and\_mobile\_bodies%20(1).pdf. [↑](#footnote-ref-64)
64. Op cit Kazakhstan Feminist Initiative “Feminita”, et al. [↑](#footnote-ref-65)
65. APC Submission, 2018. [↑](#footnote-ref-66)
66. Malta Times, Saturday April 7, 2018 ‘New Health care clinic for transgender people in pipeline’, p5. [↑](#footnote-ref-67)
67. The Universal Rights of Childbearing Women Charter and M. A. Bohren, J.P. Vogel, E.C. Hunter, O. Lutsiv, S.K. Makh, J.P. Souza, C. Aguiar, F.S. Coneglian, A. Luíz, A. Diniz, Ö. Tunçalp, D. Javadi, O.T. Oladapo, R. Khosla, M.J. Hindin, A.M. Gülmezoglu, ‘The Mistreatment of Women during Childbirth in Health Facilities Globally: A Mixed-Methods Systematic Review’, PLOS Medicine | DOI:10.1371/journal.pmed.1001847 June 30, 2015. Dejusticia; APC [↑](#footnote-ref-68)
68. C. Wahlquist, Protect us from anti-abortion protesters, say women's clinics in WA, The Guardian International Edition, 25 January, 2018. [↑](#footnote-ref-69)
69. The Charter of Human Rights and Principles for the Internet,Internet Rights and Principles Dynamic Coalition UN, Internet Governance Forum, 2014; APC Submission, 2018. [↑](#footnote-ref-70)
70. CPRC Submission citing ‘Money’ CNN News in March 2018. [↑](#footnote-ref-71)
71. https://decoders.amnesty.org/projects/troll-patrol/findings [↑](#footnote-ref-72)
72. Op cit Kazakhstan Feminist Initiative “Feminita”, et all. Submission 2018. [↑](#footnote-ref-73)
73. Electronic Media cited in Dejusticia Submission, 2018 [↑](#footnote-ref-74)
74. APC Submission, 2018, Pushkarn, N. and Ren,MM, Submission 2018, “*Online Reputation, What are they saying about me****?*”, a Discussion Paper, Office of the Privacy Commissioner of Canada,**  **January 2016:** [**https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or\_201601/**](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/); Case submissions to TGEU; and European Union Agency for Fundamental Rights, Violence against Women: an EU-wide survey. Main Results. 2015. [↑](#footnote-ref-75)
75. GLSEN (2013), [Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet](https://www.glsen.org/article/experiences-lgbt-youth-online). In Joint International Submission 2018. [↑](#footnote-ref-76)
76. AWAVA Submission, 2018. [↑](#footnote-ref-77)
77. Joint CSO Submission 2018; AccessNow The gender of surveillance: how the world can work together for a safer internet, February, 2018 <https://www.accessnow.org/gender-surveillance-world-can-work-together-safer-internet/> [↑](#footnote-ref-78)
78. Preamble, https://www.ohchr.org/EN/UDHR/Documents/UDHR\_Translations/eng.pdf [↑](#footnote-ref-79)
79. https://www.ohchr.org/en/issues/discrimination/pages/bornfreeequalbooklet.aspx [↑](#footnote-ref-80)
80. Australian Competition and Consumer Commission, ‘Preliminary Report of Inquiry into Digital Platforms’, 2018. [↑](#footnote-ref-81)
81. Special Rapporteur on the right to privacy, 2018 Annual Report to the UN General Assembly, Recommendation at 117(k), p21, A/73/45712. [↑](#footnote-ref-82)